МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. ЯКОВЛЕВА»

«Утверждено»
Решением Ученого Совета УрГЮУ
имени В.Ф. Яковлева
от «26» июня 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Предупреждение, выявление и расследование правонарушений в сфере телекоммуникаций и медиатехнологий»
Основная профессиональная образовательная программа высшего образования – программа магистратуры по направлению подготовки 40.04.01 Юриспруденция
(профиль (магистерская программа): Юрист в сфере телекоммуникаций и медиатехнологий)

РАЗРАБОТЧИК	
КАФЕДРА:	**криминалистики**
АВТОР (Ы):	**Бахтеев Дмитрий Валерьевич, доцент, к. ю. н., доцент**

Целью освоения учебной дисциплины является подготовка высококвалифицированных юристов с широким междисциплинарным кругозором, готовых к профессиональной деятельности в сфере медиатехнологий в научных и образовательных учреждениях, способных не допускать совершение правонарушений, связанных с обработкой, хранением и распространением цифровой информации, осуществлять проверку по таким инцидентам.

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений.

ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Темы учебной дисциплины	Виды учебной деятельности и трудоемкость (в часах)			Всего часов
		Лекции	Практические занятия	Самостоятельная работа	
1.	Тема 1. Понятие и классификация правонарушений в сфере телекоммуникаций и медиатехнологий	2	2	6	10
2.	Тема 2. Предотвращение правонарушений в сфере телекоммуникаций и медиатехнологий	4	4	12	20
3.	Тема 3. Личная и корпоративная информационная безопасность участника правоотношений в сфере телекоммуникаций и медиатехнологий	4	4	12	20
4.	Тема 4. Взаимодействие участника правоотношений в сфере телекоммуникаций и медиатехнологий с должностными лицами правоохранительных органов и адвокатами	2	2	10	14
5.	Тема 5. OSINT и HUMINT технологии в сфере телекоммуникаций и медиатехнологий	6	6	18	30
6.	Тема 6. Использование специальных знаний при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий	2	2	10	14
	ВСЕГО:	20	20	68	108

РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ:

Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Код компетенции	Содержание профессиональной компетенции	Код индикатора	Содержание индикатора	Результаты обучения
правоприменительный	правовое сопровождение деятельности физических и юридических лиц	ПК-4	Способен обеспечивать юридическое сопровождение деятельности субъектов распространения массовой информации и иных организаций и физических лиц в сфере телекоммуникаций и медиатехнологий.	ИПК-4.4	Выявляет и учитывает особенности правонарушений и преступлений в информационной сфере.	**Знания:** - форм охраняемой законом информации; - видов правонарушений в информационной среде; - методов совершения правонарушений в информационной среде. **Умения:** - квалифицировать правонарушения в информационной среде; - определять направление использования специальных знаний при расследовании преступлений в информационной сфере. **Навыки:** - выявления информационных правонарушений, принятия первичных мер по фиксации доказательственной информации, - использования методов OSINT и HUMINT при расследовании информационных правонарушений.
				ИПК-4.6	Аргументирует в суде позицию по делу, связанному со сферой телекоммуникаций и	**Умения:** - изучения механизма информационного правонарушения, визуализации метода правонарушения; - представлять в суде позицию по делу в сфере телекоммуникаций и

					медиатехнологий.	медиатехнологий.
экспертно-аналитический	правовой анализ	ПК-5	Способен осуществлять анализ деятельности субъектов распространения массовой информации и иных организаций и физических лиц на предмет выявления условий способствующих совершению правонарушений в сфере телекоммуникаций и медиатехнологий.	ИПК-5.1	Анализирует организацию и деятельность средств массовой информации на предмет выявления условий способствующих совершению правонарушений	**Знания:** - правил журналистской этики; - правил информационной безопасности при осуществлении деятельности СМИ. **Умения:** - выявлять информационные правонарушения при осуществлении деятельности СМИ. **Навыки:** - действий при выявлении угрозы личной или корпоративной безопасности СМИ, - обеспечения взаимодействия с правоохранительными органами и носителями специальных знаний при информационных инцидентах, - проведения журналистского расследования информационного инцидента.
				ИПК-5.2	Анализирует деятельность субъектов распространяющих массовую информацию без использования средств массовой информации на предмет	**Знания:** - правил информационной безопасности при осуществлении деятельности субъектов распространяющих массовую информацию без использования средств массовой информации. **Навыки:** - действий при выявлении угрозы личной или корпоративной безопасности субъектов распространяющих массовую информацию без использования средств

					выявления условий способствующих совершению правонарушений	массовой информации.
				ИПК-5.3	Анализирует деятельность субъектов в медиапространстве на предмет выявления условий способствующих совершению правонарушений в сфере телекоммуникаций и медиатехнологий.	**Знания:** - правил информационной безопасности при осуществлении деятельности субъектов в медиапространстве. **Умения:** - выявлять информационные правонарушения при осуществлении деятельности субъектов в медиапространстве. **Навыки:** - действий при выявлении угрозы личной или корпоративной безопасности субъектов в медиапространстве.
				ИПК-5.4	Анализирует деятельность государственных и муниципальных органов на предмет выявления условий способствующих совершению	**Знания:** - правил информационной безопасности при осуществлении деятельности государственных и муниципальных органов. **Умения:** - выявлять информационные правонарушения при осуществлении деятельности государственных и муниципальных органов. **Навыки:**

					правонарушений в сфере телекоммуникаций и медиатехнологий.	- действий при выявлении угрозы личной или корпоративной безопасности государственных и муниципальных органов.
		ПК-6	Способен подготавливать экспертные заключения в области права по вопросам, связанным с созданием, получением, распространением информации.	ИПК-6.4	Подготавливает экспертные заключения по содержанию информационной продукции на предмет соответствия её законодательству.	**Навыки:** - описания события правонарушения в информационной сфере - составления проектов процессуальных и непроцессуальных документов, фиксирующих правонарушение, связанное с нарушением информационной безопасности.
организационно-управленческий	организация деятельности физических и юридических лиц	ПК-8	Способен организовывать правовое сопровождение деятельности хозяйствующих субъектов, редакций, журналистов.	ИПК-8.6	Организует деятельность по недопущению совершения правонарушений и преступлений в информационной сфере.	**Знания:** - технических и тактических методов недопущения совершения правонарушений и преступлений в информационной сфере **Навыки:** - организации режимов информационной тишины и мониторинга источника информации.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема I. Понятие и классификация правонарушений в сфере телекоммуникаций и медиатехнологий

1. Административные правонарушения и уголовно-наказуемые деяния в сфере телекоммуникаций и медиатехнологий.
2. Внутренние и внешние факторы формирования правонарушений в сфере телекоммуникаций и медиатехнологий.
3. Социальные, технические и экономические последствия правонарушений в сфере телекоммуникаций и медиатехнологий.

Оценочные средства по теме № 1: Понятие и классификация правонарушений в сфере телекоммуникаций и медиатехнологий

Вопросы для самоконтроля

1. Структура правовых норм, устанавливающих ответственность за административные правонарушения и уголовно-наказуемые деяния в сфере телекоммуникаций и медиатехнологий.
2. Формы бездействия, являющегося объективной стороной правонарушений в сфере телекоммуникаций и медиатехнологий.
3. Формы и виды информации, являющейся предметом посягательства в сфере телекоммуникаций и медиатехнологий.
4. Принципы распределения ответственности за правонарушения в сфере телекоммуникаций и медиатехнологий.
5. Формы охраняемой законом информации.

2. Примеры дискуссионных вопросов:

1. Приведите примеры внешних факторов формирования правонарушений в сфере телекоммуникаций и медиатехнологий.
2. Приведите примеры внутренних факторов формирования правонарушений в сфере телекоммуникаций и медиатехнологий.
3. Охарактеризуйте возможные последствия похищения ноутбука журналиста.
4. Охарактеризуйте возможные последствия проникновения со взломом в редакцию СМИ.
5. Охарактеризуйте возможные последствия хакерской атаки на веб-сайт СМИ.

Тема II. Предотвращение правонарушений в сфере телекоммуникаций и медиатехнологий

1. Технические средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.

2. Правовые средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.

3. Этические средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.

Оценочные средства по теме № 2: Предотвращение правонарушений в сфере телекоммуникаций и медиатехнологий

Вопросы для самоконтроля

1. Программные средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.
2. Программно-аппаратные средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.
3. Законы и подзаконные акты, регламентирующие безопасность телекоммуникаций и медиатехнологий.
4. Этические кодексы в сфере телекоммуникаций.

1. Примеры дискуссионных вопросов:

1. Нужна ли этика интернет-сообществам? Должна ли она носить внешний характер?
2. Взаимодействие журналиста (блогера) и государства.
3. Дипфейки в медиапространстве.

Тема III. Личная и корпоративная информационная безопасность участника правоотношений в сфере телекоммуникаций и медиатехнологий

1. Личная информационная безопасность участника правоотношений в сфере телекоммуникаций и медиатехнологий

2. Корпоративная информационная безопасность участника правоотношений в сфере телекоммуникаций и медиатехнологий

Оценочные средства по теме № 3: Личная и корпоративная информационная безопасность участника правоотношений в сфере телекоммуникаций и медиатехнологий

Вопросы для самоконтроля

1. Правила безопасности при общении в соцсетях.
2. Правила безопасности при общении в мессенджерах.
3. Правила безопасности при общении в электронной почте.
4. Правила безопасности при общении по телефону.
5. Правила безопасности при работе с файлами-контейнерами.
6. Межсетевые экраны.
7. Антивирусы
8. Системы обнаружения сетевых атак.
9. Пен-тесты корпоративной безопасности.

1. Примерные темы контрольных работ:

1. Действия при обнаружении заражённого файла.
2. Отражение фишинговой атаки на организацию.

Тема IV. Взаимодействие участника правоотношений в сфере телекоммуникаций и медиатехнологий с должностными лицами правоохранительных органов и адвокатами

1. Ситуации и способы подачи заявления об информационном правонарушении в полицию, СК и ФСБ России.
2. Взаимодействие со следователем при расследовании информационных инцидентов. Взаимодействие с адвокатом при расследовании информационных инцидентов.

Оценочные средства по теме № 4: Взаимодействие участника правоотношений в сфере телекоммуникаций и медиатехнологий с должностными лицами правоохранительных органов и адвокатами

Вопросы и задания для самоконтроля

1. Основания возбуждения уголовного дела по заявлению субъекта правоотношений в сфере телекоммуникаций и медиатехнологий
2. Основы методики расследования информационных инцидентов
3. Адвокат в журналистском расследовании.

1. Примерные темы контрольных работ:

1. Составьте план действий при утечке журналистской тайны.
2. Составьте план действий при взломе учётной записи компании в социальной сети.
3. Составьте план действий при взломе электронной почты редакции СМИ.

Тема V. OSINT и HUMINT технологии в сфере телекоммуникаций и медиатехнологий

1. Источники OSINT
2. Программные средства OSINT
3. Нарушения обработки персональных данных при использовании методов OSINT
4. Установление психологического контакта.
5. Анализ вербальной информации.
6. Использование невербальной аналитики.
7. Использование инструментальных средств профилирования.

Оценочные средства по теме № 5: OSINT и HUMINT технологии в сфере телекоммуникаций и медиатехнологий

Вопросы и задания для самоконтроля

1. Боты и веб-сайты как методы OSINT
2. Вербальная и невербальная информация.
3. Полиграф в медиатехнологиях.
4. Доксинг.

1. Примерные темы контрольных работ:

1. Составьте аналитический разбор текстового сообщения.
2. Составьте аналитический разбор устной речи по видеозаписи.

Тема VI. Использование специальных знаний при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий

1. Поиск информации в интернете.
2. Использование консультантов и специалистов при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий.

Оценочные средства по теме № 6: Использование специальных знаний при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий

Вопросы и задания для самоконтроля

1. Использование поисковых операторов и дорков.
2. Виды и формы использования специальных знаний при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий

РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины осуществляется в форме учебных занятий под руководством профессорско-преподавательского состава кафедры и самостоятельной подготовки обучающихся. Основными видами учебных занятий по изучению данной дисциплины являются лекционные и практические занятия. При проведении учебных занятий используются элементы классических и современных педагогических технологий.
Предусматриваются следующие формы работы обучающихся:
– прослушивание лекционного курса;
– чтение и конспектирование рекомендуемой литературы;
– анализ рекомендуемых преподавателем практических ситуаций;
– участие в практических занятиях в качестве докладчика, содокладчика, а также в качестве оппонента;
– подготовка письменных рефератов;
– участие в письменных контрольных работах.

Наиболее эффективное, качественное усвоение учебного материала обеспечивается тщательным изучением, анализом, сравнением и обобщением рекомендуемых источников.

Контроль знаний проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся (текущая аттестация) проводится в ходе семестра с целью определения уровня усвоения обучающимися знаний, сформированности у них умений и навыков.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:
– на практических занятиях (доклады, ответы на вопросы преподавателя);
– по результатам проведения аудиторных контрольных работ;
– в процессе выполнения заданий по анализу практических ситуаций;
– по результатам проверки письменных рефератов (для студентов заочной формы).

Контроль за выполнением обучающимися каждого вида работ может осуществляться поэтапно и служит основанием для предварительной и промежуточной аттестации по дисциплине.

Промежуточная аттестация студентов проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков обучающихся по дисциплине требованиям стандарта.

ТЕКУЩИЙ КОНТРОЛЬ

Система оценивания по дисциплине:

№	Наименование (тема) и форма контрольного мероприятия	Учебная неделя, на которой проводится, иное указание на срок/период выполнения	Балловая стоимость контрольного мероприятия (максимальное значение)
1	Внеаудиторная контрольная работа № 1	Практическое занятие № 3	10
2	Внеаудиторная контрольная	Практическое занятие № 5	10

	работа № 2		
3	Внеаудиторная контрольная работа № 3	Практическое занятие № 9	15
4	Активность на практических занятиях	Весь курс	10
5	Написание эссе	Весь курс	15

Описание контрольных мероприятий:

Внеаудиторная контрольная работа №1. Анализ практического примера нарушения информационной безопасности

- Найти в интернете случай критического нарушения безопасности информационной системы. Указать факторы обеспечения информационной безопасности системы, механизм правонарушения, привести способы предотвращения подобных инцидентов.

Мероприятие проводится *внеаудиторно.*

Критерии оценивания:

12-15 баллов: Описание использует корректный терминологический аппарат, содержит правильно оформленные ссылки на нормативные и иные документы, содержит описание механизма информационного нарушения, подробный список методов по его предотвращению.

8-11 баллов: Описание использует в целом корректный терминологический аппарат, содержит ссылки на нормативные и иные документы, содержит описание механизма информационного нарушения.

4-7 баллов: Описание содержит описание механизма информационного нарушения.

1-3 балла: Работа содержит критические упущения или противоречия.

0 баллов: Работа не выполнена.

Внеаудиторная контрольная работа №2. Составление памятки по информационной безопасности участника правоотношений в медиапространстве

- Составить памятку по информационной безопасности участника правоотношений в медиапространстве с учётом деятельности в интернете, мессенджерах, при разговорах по телефону.

Мероприятие проводится *внеаудиторно.*

Критерии оценивания:

12-15 баллов: Описание использует корректный терминологический аппарат, содержит правильно оформленные ссылки на нормативные и иные документы, содержит подробные рекомендации по обеспечению информационной безопасности.

8-11 баллов: Описание использует в целом корректный терминологический аппарат, содержит ссылки на нормативные и иные документы, содержит обрывочное описание механизма информационного нарушения.

4-7 баллов: Описание содержит обрывочное описание механизма информационного нарушения.

1-3 балла: Работа содержит критические упущения или противоречия.

0 баллов: Работа не выполнена.

Внеаудиторная контрольная работа №3. Использование OSINT методов

- С использование открытых программных методов OSINT найти в интернете информацию о себе, составить профиль собственной цифровой личности.

Мероприятие проводится *внеаудиторно.*

Критерии оценивания:
12-15 баллов: Описание использует корректный терминологический аппарат, содержит результат использования 3 и более методов OSINT.
4-11 баллов: Описание использует в целом корректный терминологический аппарат, содержит результат использования менее 3 методов OSINT.
1-3 балла: Работа содержит критические упущения или противоречия.
0 баллов: Работа не выполнена.

Контрольное эссе.
Примерные темы эссе:

1. Утечки данных из облачных хранилищ.
2. Утечки данных из корпоративных серверных хранилищ.
3. Нарушения журналистской этики.
4. Уголовная ответственность журналиста за деяния, связанные с профессиональной деятельностью.
5. Уголовная ответственность блогера за деяния, связанные с профессиональной деятельностью.
6. Административная ответственность журналиста за деяния, связанные с профессиональной деятельностью.
7. Административная ответственность блогера за деяния, связанные с профессиональной деятельностью.
8. Этические системы интернета эпохи web 1.0.
9. Этические системы интернета эпохи web 2.0.
10. Этические системы интернета эпохи web 3.0.
11. Методы OSINT в медиатехнологиях.
12. Методы HUMINT в медиатехнологиях.
13. Методы поиска информации в сети Интернет.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Форма промежуточной аттестации	*Экзамен*
Формат проведения мероприятий промежуточной аттестации	по билетам/собеседование
Структура мероприятий и балловая стоимость элементов	*Ответ на теоретических 2 вопроса: 20 баллов* *Решение практического задания: 20 баллов.*

Теоретические задания

1. Нормативно-правовые акты, регламентирующие безопасность в сфере телекоммуникаций и медиатехнологий.
2. Административные правонарушения в сфере телекоммуникаций и медиатехнологий.
3. Преступления, совершаемы в сфере телекоммуникаций и медиатехнологий.
4. Этические правонарушения в медиасфере. Доксинг.
5. Технические средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.
6. Этические средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.
7. Организационные средства предотвращения правонарушений в сфере телекоммуникаций и медиатехнологий.
8. Обеспечение личной информационной безопасности при общении в соцсетях и мессенджерах.

9. Обеспечение корпоративной информационной безопасности при общении в соцсетях и мессенджерах.

10. Обеспечение личной и корпоративной информационной безопасности при размещении информации на веб-сайтах.

11. Обеспечение личной информационной безопасности при общении через электронную почту.

12. Обеспечение корпоративной информационной безопасности при общении через электронную почту.

13. Пен-тесты как фактор обеспечения корпоративной безопасности.

14. Инициация уголовного расследования инцидента в сфере информационной безопасности.

15. Методика расследования информационных инцидентов.

16. Адвокат в журналистском расследовании.

17. Методы OSINT: общая характеристика.

18. Методы HUMINT: общая характеристика.

19. Поиск информации в интернете.

20. Использование консультантов и специалистов при расследовании правонарушений в сфере телекоммуникаций и медиатехнологий.

Практические задания:

1. Документ с грифом «Конфиденциально» был разослан в корпоративной сети электронной почты на 2000 пользователей через кнопку «ответить всем». Каковы возможные последствия этого инцидента? Существуют ли способы минимизации таких последствий?

2. Сотрудник, впервые вышедший на работу, скопировал на флеш-карту базу данных из общей сети. Каковы возможные последствия этого инцидента? Существуют ли способы минимизации таких последствий?

3. Составьте план журналистского расследования факта некачественного оказания услуг или продажи товаров ненадлежащего качества.

4. Сотрудник редакции скачал присланный по электронной почте файл формата .pdf. Каковые возможные последствия действий с этим файлом?

5. Сотрудник редакции скачал с интернет-сайта файл формата .apk. Каковые возможные последствия действий с этим файлом?

6. Составьте заявление в полицию о взломе компьютерной системы.

7. Ноутбук при включении циклично перезагружается. Чем это может быть объяснено? Какие нарушения информационной безопасности могли к этому привести?

8. Составьте запрос о консультации IT-специалиста.

9. Составьте план пен-теста редакции СМИ.

10. Составьте гугл-дорк по названной преподавателем задаче.

Критерии оценивания:

Критерии оценивания теоретического вопроса (максимально 10 баллов)

0 баллов – ответ отсутствует

1-4 балла – студент дает ответ, однако в нем содержатся грубые ошибки в использованных терминах.

5-7 баллов – студент даёт ответ, допускает в определении понятий и категорий отдельные ошибки, однако при называет наиболее существенные признаки описываемых категорий, их практическое значение, указывает на наличие взаимосвязей технических, тактических, этических и организационных средств и ситуаций, в которых они применяются.

8-10 баллов – студент дает полный ответ на поставленный вопрос, при определении понятий и категорий указывает на их существенные признаки, характеризует их

практическое значение, а также взаимосвязи применяемых технических, тактических, этических и организационных средств с ситуациями, при этом обосновывает свой ответ.

Критерии оценивания практического задания (максимально 20 баллов за 1 задание)
0 баллов – ответ отсутствует
1-4 балла – при ответе на вопрос задания студент испытывает трудности при оценке конкретной ситуации, оценивает ее неверно, не может обосновать свой ответ, не отвечает или не понимает сущности дополнительных вопросов преподавателя. Называет неверные методы разрешения конкретной ситуации задания., однако при помощи дополнительных вопросов называет отдельные методы, которые могут быть использованы в практических ситуациях
5-8 баллов – студент оценивает конкретную ситуацию с существенными ошибками, корректирует ответ за счет дополнительных вопросов преподавателя, называя отдельные признаки конкретной ситуации и методы её разрешения.
9-12 баллов – студент оценивает конкретную ситуацию с незначительными ошибками, называет наиболее эффективные методы её разрешения, уверенно обосновывает свой ответ, однако испытывает некоторые затруднения в оценке прогнозов развития сложных ситуаций
13-20 баллов – студент даёт полный ответ на вопрос задания, верно оценивает характер конкретной ситуации, называет наиболее эффективные методы её разрешения, прогнозирует развитие сложных ситуаций

БИБЛИОГРАФИЯ ПО ДИСЦИПЛИНЕ

1. IT-справочник следователя / Коллектив авторов. Под ред. С. В. Зуева. М.: Юрлитинформ, 2019. 232 с.
2. Основы теории электронных доказательств: монография / Коллектив авторов. Под ред. С. В. Зуева. М.: Юрлитинформ, 2019. 400 с.
3. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование).
4. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2021. — 417 с. — (Высшее образование).
5. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев. — Москва : Издательство Юрайт, 2021. — 193 с. — (Высшее образование).
6. Электронные носители информации в криминалистике: монография / Коллектив авторов. Под ред. О. С. Кучина. М.: Юрлитинформ, 2017. 304 с.

Перечень электронных учебных изданий

1. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование). — ISBN 978-5-534-13898-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467208
2. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2021. — 417 с. — (Высшее образование). — ISBN 978-5-534-14600-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477984

3. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев. — Москва : Издательство Юрайт, 2021. — 193 с. — (Высшее образование). — ISBN 978-5-534-13286-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477037

Электронные учебные издания доступны для зарегистрированных в Электронной информационно-образовательной среде университета пользователей.

Оснащение помещений для учебных занятий

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, экран проекционный, проектор, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, видеонаблюдение
Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, моноблок, интерактивная доска
Помещение для самостоятельной работы	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации, проектор, экран, многофункциональное устройство

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Microsoft WINEDUperDVC ALNG UpgrdSAPk OLV E 1Y AcdmemicEdition Enterprise;
2. Linux (Альт, Астра);

3. Kaspersky Endpoint Security 11 для Windows;
4. Libre Office (свободно распространяемое программное обеспечение).

Перечень электронно-библиотечных систем:

1. «Электронно-библиотечная система ZNANIUM»;
2. «Образовательная платформа ЮРАЙТ»;
3. Электронно-библиотечная система «BOOK.ru»;
4. Электронно-библиотечная система «ЛАНЬ»;
5. Электронно-библиотечная система Издательства «Проспект».

Перечень современных профессиональных баз данных

1. Электронная библиотека диссертаций (ЭБД);
2. Единая межведомственная информационно – статистическая система (ЕМИСС) - Режим доступа: https://fedstat.ru/;
3. База данных показателей муниципальных образований - Режим доступа: https://rosstat.gov.ru/storage/mediabank/Munst.htm;
4. ПРЕДОСТАВЛЕНИЕ СВЕДЕНИЙ ИЗ ЕГРЮЛ/ЕГРИП В ЭЛЕКТРОННОМ ВИДЕ - Режим доступа: https://egrul.nalog.ru/index.html;
5. Государственная автоматизированная система Российской Федерации «Правосудие» - Режим доступа: https://bsr.sudrf.ru/bigs/portal.html;
6. Банк решений арбитражных судов - Режим доступа: https://ras.arbitr.ru/;
7. База данных судебных актов - Режим доступа: http://bdsa.minjust.ru/;
8. База решений и правовых актов Федеральной антимонопольной службы - Режим доступа: https://br.fas.gov.ru/;
9. Банк решений Конституционного Суда Российской Федерации - Режим доступа: http://www.ksrf.ru/ru/Decision/Pages/default.aspx;
10. Государственная система правовой информации – Режим доступа: http://www.pravo.gov.ru/;
11. Федеральный портал проектов нормативных актов - Режим доступа: https://regulation.gov.ru/;
12. Система обеспечения законодательной деятельности - Режим доступа: https://sozd.duma.gov.ru/.

Перечень информационных справочных систем

1. Информационно-правовой портал «Система Гарант»;
2. Справочная правовая система «КонсультантПлюс»;
3. Информационно-правовая система «Кодекс»;
4. Информационно-правовая система (ИПС) «Законодательство стран СНГ».