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
«Методы цифровой криминалистики в расследовании преступлений»

Основная профессиональная образовательная программа высшего образования – программа специалитета по специальности
40.05.01 Правовое обеспечение национальной безопасности
Государственно-правовая специализация

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

Целью освоения учебной дисциплины является изучение обучающимися современных способов совершения преступлений в сфере информационно-коммуникационных технологий и методов их выявления и расследования. В курсе исследуются механизмы формирования, обнаружения, фиксации и изъятия цифровых следов преступлений, программные, программно-аппаратные и тактические средства, особенности назначения и производства компьютерно-технических исследований и привлечения к расследованию специалистов в сфере компьютерной информации.

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	Общие положения цифровой криминалистики	2	4	6	12
2	Механизм формирования цифровых следов.	2	4	8	14
3	Способы совершения киберпреступлений.	2	4	8	14
4	Программные и программно-аппаратные средства цифровой криминалистики	2	4	10	16
5	Обнаружение и визуализация цифровых следов	2	4	10	16
6	Особенности производства следственных действий в отношении компьютерно-технических объектов	4	8	10	22
7	Назначение и производство компьютерно-технических исследований	2	4	8	14
	ВСЕГО:	16	32	60	108

РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ:

Наименование категории (группы) универсальных/общепрофессиональных компетенций	Код универсальной/ общепрофессиональной компетенции	Содержание универсальной/ общепрофессиональной компетенции	Код индикатора	Содержание индикатора	Результаты обучения
Системное и критическое мышление	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК 1.1	Анализирует достоверность и достаточность имеющейся информации для разрешения проблемной ситуации; выявляет все факты и обстоятельства, подлежащие оценке, для целей разрешения проблемной ситуации.	**Знания:** основной терминологический инструментарий из областей компьютерной техники и сетевых технологий. **Умения:** определяет типовые цифровые следы и их носители при анализе следственных ситуаций; описывает механизм следообразования цифровых следов в различных криминальных ситуациях. **Навыки**: классифицирует цифровые следы и носители цифровой доказательственной информации; квалифицирует факты, события и обстоятельства, связанные с компьютерными инцидентами; оценивает информационное значение следов преступлений в целях их расследования; на основе анализа проблемной ситуации определяет и реализовывает тактические

					приемы производства следственных действий.
			ИУК 1.2	Формулирует собственные суждения на основе анализа и оценки проблемной ситуации; отличает факты от мнений, интерпретаций, оценок; формулирует стратегию действий по разрешению проблемной ситуации. Демонстрирует интеллектуальную автономию.	**Умения:** оценивает корректность применения специальных знаний при проведении служебных и иных документальных проверок по фактам совершения компьютерных инцидентов; изучает факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных; выявляет и анализирует следственные ошибки при работе с цифровыми объектами; предлагает способы выявления фактов сокрытия цифровых следов.
			ИУК 1.3	Выстраивает систему аргументации собственных выводов по результатам анализа проблемной ситуации, а также обоснованно аргументирует выбор стратегии действий по разрешению ситуации, указывая на преимущества предложенной стратегии по сравнению с альтернативными. Применяет теорию	**Знания**: основы функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений; требования нормативно-правовых актов в области информационной безопасности и защиты информации. **Умения:** умеет подготавливать проекты процессуальных документов в связи с компьютерными инцидентами.

				аргументации при обосновании своих решений и оценке их последствий.	

Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Код профессиональной компетенции	Содержание профессиональной компетенции	Код индикатора	Содержание индикатора	Результаты обучения
правоохранительный	защита национальных интересов Российской Федерации от внешних и внутренних угроз	ПК-5	Способен защищать национальные интересы Российской Федерации от внешних и внутренних угроз.	ИПК-5.7	Использует в целях установления объективной истины по конкретным делам технико-криминалистические методы и средства, федеральные и иные банки данных криминалистической информации, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования	**Знает:** требования к проведению осмотра компьютерных объектов. **Умеет:** работать с большими объёмами цифровой информации; производить осмотр компьютерных объектов. **Навыки**: исследует соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

					отдельных видов и групп преступлений.	
				ИПК-5.8	Соблюдает установленные законодательством правила изъятия, хранения и передачи вещественных доказательств и в установленные сроки исполняет приговоры судов по уголовным делам в части принятых решений по вещественным доказательствам.	**Умения:** оценивает результаты компьютерно-технической экспертизы. **Навыки**: обнаруживает и сохраняет цифровые следы, осуществляет их предварительное исследование.
экспертно-консультационный (консультационный	цифровая трансформация государственных органов	ПК-8	Способен принимать участие в цифровой трансформации государственных органов обеспечения национальной безопасности.	ИПК-8.3.	Оптимизирует профессиональную деятельность, используя современные информационные системы и информационно-коммуникационные технологии.	**Навыки**: осуществляет мануальный и полуавтоматический поиск в телекоммуникационных сетях; использует открытые источники информации о способах совершения киберпреступлений; подготавливает проекты запросов операторам сотовой связи и провайдерам.
профилактический	профилактика и предупреждение правонарушений и преступлений	ПК-9	Способен осуществлять профилактику, предупреждение правонарушений и	ИПК-9.3.	Использует современные информационно-коммуникационные технологии в целях	**Навыки:** выделяет следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной

			преступлений, угрожающих интересам национальной безопасности, выявлять и устранять причины и условия, способствующие их совершению, в том числе с использованием современных информационно-коммуникационных технологий.		предупреждения и выявления правонарушений и преступлений.	информации; разделяет способы сокрытия цифровой информации.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Общие положения цифровой криминалистики
Изучаемые вопросы:

1. Понятие, объект и предмет цифровой криминалистики.
2. Структура цифровой криминалистики.
3. Место цифровой криминалистики в юридической науке.

Изучаемые нормативно-правовые акты:

- "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ
- Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
- Постановление Правительства РФ от 09.12.2014 N 1342 (ред. от 18.01.2021) "О порядке оказания услуг телефонной связи"

Тема 2. Механизм формирования цифровых следов.
Изучаемые вопросы:

1. Классификация цифровых следов.
2. Локальные и удалённые источники формирования цифровых следов.
3. Криптографические и стеганографические способы сокрытия цифровых следов.

Задание:

Составить сравнительную таблицу криптографических и стеганографических способов сокрытия цифровых следов. Сформулировать по одному примеру для каждого способа.

Тема 3. Способы совершения киберпреступлений.
Изучаемые вопросы:

1. Правовая характеристика способов совершения киберпреступлений.
2. Техническая характеристика способов совершения киберпреступлений. Система MITTRE ATT&CK

Задание:

1. Изучить систему MITTRE ATT&CK, выписать 3 способа, которые были использованы при совершении преступлений в России.
2. Написать аналитическое эссе с описанием связи между способом совершения киберпреступления и личностью преступника.

Тема 4. Программные и программно-аппаратные средства цифровой криминалистики
Изучаемые вопросы:

1. Криминалистические программные и программно-аппаратные средства, используемые для анализа информации в сети Интернет.
2. Криминалистические программные и программно-аппаратные средства, используемые для анализа информации на персональных компьютерах и серверах.
3. Криминалистические программные и программно-аппаратные средства, используемые для анализа информации на мобильных устройствах.

4. Криминалистическое исследование информации базовых станций сотовой связи.

Задание:
1. С помощью открытого программного обеспечения нанести на карту расположение 5 базовых станций.
2. Составить сравнительную таблицу возможностей криминалистических программных средств изучения информации на мобильных устройствах.
3. Описать не менее 8 операторов для полуавтоматического поиска информации в сети Интернет.
4. Изучить возможности сервера whois.

Тема 5. Обнаружение и визуализация цифровых следов
Изучаемые вопросы:
1. Общая характеристика способов обнаружения цифровых следов.
2. Формирование доказательств из цифровых следов. Системы визуализации и анализа цифровых массивов.

Задание:
1. Зафиксировать и изучить с помощью программных средств переписку или архив фотографий. Составить фрагмент протокола осмотра носителя цифровой информации.
2. С помощью открытых источников изучить содержимое сайта crimlib.info в марте 2015 года.

Тема 6. Особенности производства следственных действий в отношении компьютерно-технических объектов
Изучаемые вопросы:
1. Особенности производства осмотра компьютерных объектов.
2. Особенности производства обыска по ст. 164.1 УПК Российской Федерации.
3. Особенности производства следственного эксперимента в отношении объектов, содержащих цифровую доказательственную информацию.
4. Особенности производства получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Задание:
1. Составить план следственного эксперимента по установлению факта подключения устройства абонента к базовой станции.
2. Составить протокол осмотра веб-сайта.
3. Составить запрос оператору сотовой связи.

Тема 7. Назначение и производство компьютерно-технических исследований
Изучаемые вопросы:
1. Привлечение специалиста в области информационно-коммуникационных технологий к расследованию преступлений.
2. Задачи и классификация компьютерно-технических исследований.
3. Назначение компьютерно-технической экспертизы.
4. Общая характеристика методов компьютерно-технической экспертизы
5. Оценка и использование результатов компьютерно-технической экспертизы.

Задание:
Составить постановление о назначении КТЭ.

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	Аудиторная контрольная работа №1	Практическое занятие № 3	10
2	Аудиторная контрольная работа №2	Практическое занятие № 10	10
3	Аудиторная контрольная работа №3	Практическое занятие № 14	10
4	Активность на практических занятиях	Весь курс	20

Описание контрольных мероприятий:

Аудиторная контрольная работа №1. Способы и механизмы совершения киберпреступлений

Изучить российский опыт борьбы с киберпреступлениями. Описать один случай использования вредоносного программного обеспечения с указанием характеристик этого способа в системе MITTRE ATT&CK. Указать факторы, способствовавшие совершению преступления и возможные меры по противодействию этому способу.
Мероприятие предполагает доступ обучающихся к сети Интернет, проводится аудиторно.

Критерии оценивания:

8-10 баллов: Использован реальный пример, приведена ссылка на судебную или следственную практику, детально описан способ совершения преступления, указаны меры по противодействию преступлению, выражено собственное мнение обучающегося.

5-7 баллов: Использован реальный пример, приведена ссылка на материалы СМИ, детально описан способ совершения преступления, указаны меры по противодействию преступлению.

3-4 баллов: Приведена ссылка СМИ, приведено противоречивое описание способа совершения преступления, указаны отдельные меры по противодействию преступлению.

1-2 балла: Работа содержит критические упущения или противоречия.

0 баллов: Работа не выполнена.

Аудиторная контрольная работа №2. Составление протокола осмотра веб-сайта.

Составить протокол осмотра произвольного веб-сайта. В процессе выполнения задания использовать сервис whois.
Мероприятие предполагает доступ обучающихся к сети Интернет, проводится аудиторно.

Критерии оценивания:

8-10 баллов: Протокол составлен с соблюдением процессуальных требований, содержит детальное описание структуры и содержания веб-сайта. В протоколе приведены сведения из сервиса whois. К протоколу приложена иллюстрационная таблица, исходный код веб-сайта.

5-7 баллов: Протокол составлен с соблюдением процессуальных требований, содержит общее описание структуры и содержания веб-сайта. В протоколе приведены сведения из сервиса whois. К протоколу приложена иллюстрационная таблица.

3-4 баллов: Протокол составлен с незначительными нарушениями процессуальных требований, содержит общее описание структуры веб-сайта. В протоколе приведены сведения из сервиса whois.

1-2 балла: Работа содержит критические упущения или противоречия.

0 баллов: Работа не выполнена.

Аудиторная контрольная работа №3. Способы и механизмы совершения киберпреступлений

Составить протокол следственного эксперимента по получению информации базовых станций.

Мероприятие предполагает доступ обучающихся к сети Интернет, наличие смартфона, проводится аудиторно.

Критерии оценивания:

8-10 баллов: Протокол составлен с соблюдением процессуальных требований, содержит детальное описание произведённых операций. К протоколу приложена иллюстрационная таблица, скриншоты.

5-7 баллов: Протокол составлен с соблюдением процессуальных требований, содержит общее описание произведённых операций. К протоколу приложена иллюстрационная таблица.

3-4 баллов: Протокол составлен с незначительными нарушениями процессуальных требований, содержит общее описание произведённых операций.

1-2 балла: Работа содержит критические упущения или противоречия.

0 баллов: Работа не выполнена.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Форма промежуточной аттестации	*зачет*
Формат проведения мероприятий промежуточной аттестации	*Устно* *по билетам/собеседование*
Структура мероприятий и балловая стоимость элементов	*2 теоретических задания – максимально по 15 баллов* *1 практическое задание – максимально 20 баллов*

Примерные задания для мероприятий промежуточной аттестации:

Теоретические задания

1. Понятие, структура цифровой криминалистики
2. Задачи, объект и предмет цифровой криминалистики
3. Понятие, свойства цифровой информации.

4. Элементы механизма формирования цифровых следов преступления.
5. Классификация способов совершения киберпреступлений.
6. Способы сокрытия цифровой информации.
7. База данных MITTRE ATT&CK как источник информации для раскрытия киберпреступлений
8. Программно-аппаратные средства цифровой криминалистики.
9. Программные средства цифровой криминалистики.
10. Процессуальные основания использования программных и программно-аппаратных средств цифровой криминалистики.
11. Обнаружение и фиксация цифровых следов.
12. Изъятие и копирование цифровой информации.
13. Обеспечение сохранности цифровой информации и её носителей.
14. Мониторинг сети интернет в следственной деятельности.
15. Осмотр смартфона.
16. Осмотр веб-сайта.
17. Осмотр персонального компьютера.
18. Осмотр локального сервера.
19. Осмотр содержимого облачных хранилищ.
20. Криминалистическое исследование информации базовых станций сотовой связи.
21. Особенности обыска в отношении компьютерно-технических объектов.
22. Особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами.
23. Особенности производства следственного эксперимента в отношении цифровых объектов.
24. Получение судебного разрешения на доступ к цифровым сведениям.
25. Направление запросов операторам сотовой связи и провайдерам сети Интернет.
26. Основные ошибки при работе с цифровыми следами и объектами.
27. Привлечение специалиста в области информационно-коммуникационных технологий к расследованию преступлений.
28. Понятие, задачи и направления компьютерно-технических исследований.
29. Назначение компьютерно-технической экспертизы.
30. Оценка заключения эксперта компьютерно-технической экспертизы.

Практические задания:

1. Составьте протокол следственного осмотра смартфона.
2. Составьте протокол следственного осмотра ноутбука.
3. Составьте протокол следственного осмотра веб-сайта.
4. Составьте протокол осмотра содержимого облачного хранилища.
5. Составьте протокол осмотра носителя цифровой информации.
6. Составьте запрос оператору сотовой связи о предоставлении сведений биллинга
7. Составьте протокол выемки носителя цифровой информации.
8. Составьте план следственного эксперимента по проверке биллинговой информации.
9. Составьте постановление о назначении программной компьютерно-технической экспертизы.
10. Составьте постановление о назначении аппаратной компьютерно-технической экспертизы.
11. Составьте план расследования незаконного доступа к компьютерной информации.

Критерии оценивания

Критерии оценивания теоретических вопросов:

7-10 баллов: логически грамотно изложенный, содержательный и аргументированный ответ, подкрепленный знанием основной и дополнительной литературы по теме вопроса, точное соблюдение криминалистической терминологии, умение отвечать на дополнительно заданные вопросы по темам дисциплины;

4-6 баллов: незначительное нарушение логики изложения материала, периодическое использование разговорной лексики, допущение не более одной ошибки в содержании ответа на вопрос, а также не более одной неточности при аргументации своей позиции, неполные или недостаточно точные ответы на дополнительно заданные вопросы;

1-3 балла: существенное нарушение логики изложения материала, систематическое использование разговорной лексики, допущение ошибок в содержании ответа на вопрос, а также неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы;

0 баллов: отказ от ответа.

Критерии оценивания практических заданий:

15-20 баллов: при решении задания обучающийся правильно оперирует криминалистической терминологией, даёт полный, грамотно и последовательно изложенный ответ, аргументирует свою позицию ссылками на основную и дополнительную литературу. Студент уверенно владеет измерительными приборами и криминалистической техникой;

10-15 баллов: при решении задания обучающийся оперирует криминалистической терминологией, допускает незначительные ошибки в использовании терминов, даёт полный, грамотно и последовательно изложенный ответ, но допускает ошибки при проведении измерений объектов;

5-10 баллов: при решении задания обучающийся использует разговорную лексику, допускает ошибки в использовании терминов, даёт неполный, либо непоследовательный ответ, допускает грубую ошибку при проведении измерений объектов;

1-5 баллов: обучающийся демонстрирует незнание криминалистической терминологии, при ответе допускает большое количество ошибок, нарушает последовательность ответа, не владеет методикой проведения измерений с помощью криминалистических измерительных приборов;

0 баллов: обучающийся отказывается от ответа.

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**
Специализированная аудитория, оборудованная для проведения занятий по криминалистике. Криминалистический полигон для отработки навыков служебной деятельности	Видеокамера (регистратор) дистанционного наблюдения, видеокамера JVC, дактилопленка темного цвета, дактилоскопическая кисть-флейц, дактилоскопическая пленка прозрачная, дактилоскопическая пленка светлого цвета, дактилоскопический магнитный порошок белый, дактилоскопический магнитный порошок темный, дактилоскопический набор "дакто", дактилоскопический не магнитный порошок белый, дактилоскопический не магнитный порошок темный, кисть магнитная, комплект дактилоскопических порошков, комплект образцов резинового оружия, комплект принадлежности для 3d-

	съемки, комплект, лупа просмотровая, микроскоп портативный цифровой, микроскоп цифровой 200-кратный, микроскоп цифровой с регулируемой подсветкой, набор д/макросъемки для фотоаппарата, натуральная коллекция "образцы гранат", натуральная коллекция "образцы огнестрельного оружия", натуральная коллекция "образцы холодного оружия", объектив canon, переносной дисковый накопитель, слепочный материал, слепочный набор, учебный комплект "следы выстрелов на пулях и гильзах", фотоаппарат canon digital, фотоаппарат canon eos 650 d, фотоаппарат Canon Power Shot G11 10Mpix 5*2,8"SD/SDHC , фотовспышка Canon Macro Ring Lite MR-14EX, Фотоаппарат Canon Digital IXUS 120IS, Фотовспышка Canon Speedlite 600EX-RT
Помещение для хранения и профилактического обслуживания учебного оборудования	Учебное оборудование
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».