

Содержание:

image not found or type unknown



Введение

На современном этапе развития науки информационный подход является одним из доминирующих методов получения и использования знаний. Юриспруденция не является исключением. В этой связи особую значимость приобретают специальные технологии, направленные на получение, обработку, передачу и хранение информации, определяемые как информационные технологии (ИТ-технологии).

Так, например, в уголовном процессе влияние информационного подхода проявляется в частности на таком ключевом понятии как доказательство. В ст. 74 УПК РФ доказательства определяются как «любые сведения», то есть по сути информация. Более того, можно отметить, что процессуальная наука в значительной степени заинтересована в эффективных методах обработки информации. Так как речь идет о ее сборе, накоплении, оценке, передаче и хранении, важным является недопущение искажения информации в процессе обработки. Можно предположить, что эффективное развитие процессуальной науки невозможно без применения существующих ИТ-технологий и, к сожалению, следует отметить, что эти технологии внедряются в процессуальную сферу крайне медленно.

Министерство внутренних дел РФ является федеральным органом, подчиненным Президенту Российской Федерации и Правительству Российской Федерации; оно возглавляет систему органов внутренних дел и несет ответственность за выполнение возложенных законодательством на органы внутренних дел задач и обязанностей. Деятельность органов внутренних дел включает несколько самостоятельных направлений: охрана общественного порядка; охрана собственности; охрана прав и законных интересов граждан от преступных посягательств; предупреждение и пресечение правонарушений; раскрытие и расследование преступлений; соблюдение разрешительной системы; обеспечение безопасности дорожного движения и пожарной безопасности.

Все эти виды деятельности нуждаются в информационно-аналитическом обеспечении. Рассмотрим основные, используемые в настоящее время, в юридической деятельности, ИТ-технологии.

Справочно-правовые системы (СПС)

Самым первым и наиболее значимым достижением информационных технологий, облегчившим жизнь каждого юриста, является создание справочно-правовой системы. К 60–70-м годам прошлого столетия был накоплен значительный по своим объемам бумажный массив информации, касающийся документов внутреннего, а также международного права и многих других. С течением времени все сложнее и сложнее становилась систематизация этих бумажных носителей.

В этот же период началось развитие информационных технологий, что и побудило юристов обратиться к специалистам в компьютерной области, которые успешно выполнили свою задачу. Уже в 1967 г. программа по компьютерному поиску юридической информации появилась в Европе. В нашей стране первую СПС внедрили в 1975 г., но на начальном этапе доступ к ее информации был ограничен. Лишь в 80–90-х годах прошлого столетия ситуация коренным образом изменилась. Появились многочисленные правовые системы, предназначенные для широкого круга пользователей. С 2011 г. стали внедрять и мобильные СПС. Работа с ними возможна с КПК и мобильных устройств.

На рынке справочно-правовых систем в России наиболее известны следующие продукты таких фирм (поданным АО "Консультант Плюс"):

- "Консультант Плюс" (АО "Консультант Плюс");
- "ГАРАНТ" (НПП "Гарант-Сервис");
- "Кодекс" (Центр компьютерных разработок).

Системы, созданные государственными предприятиями для обеспечения потребностей в правовой информации государственных ведомств:

- "Эталон" (НЦПИ при Министерстве юстиции РФ);
- "Система" (НТЦ "Система" при ФАПСИ).

Автоматизированные информационные системы (АИС)

Информационные технологии в юридической деятельности получили свое дальнейшее развитие с внедрением автоматизированных информационных систем. Опыт практического применения АИС показал, что наиболее точной, соответствующей самому назначению АИС следует считать классификацию по степени сложности технической, вычислительной, аналитической и логической обработки используемой информации. При таком подходе к классификации можно наиболее тесно связать АИС и соответствующие информационные технологии.

Можно выделить следующие виды АИС:

- автоматизированные системы обработки данных (АСОД);
- автоматизированные информационно-поисковые системы (АИПС);
- автоматизированные информационно-справочные системы (АИСС);
- автоматизированные информационно-логические системы (АИЛС);
- автоматизированные рабочие места (АРМ);
- автоматизированные системы управления (АСУ);
- автоматизированные системы информационного обеспечения (АСИО);
- экспертные системы (ЭС) и системы поддержки принятия решений.

В компьютеризации юридической деятельности можно условно выделить три группы систем:

1) автоматизированные информационные системы о нормативных актах, включающие в себя банки законодательных, правительственных и ведомственных актов, решения Конституционного Суда, постановления Пленума Верховного Суда, материалы судебной и арбитражной практики;

2) автоматизированные информационные системы, обеспечивающие оперативно-розыскную деятельность, расследование преступлений, охрану общественного порядка, где отражены банки данных криминального учета лиц - владельцев оружия и автотранспорта, лиц, разыскиваемых и без вести пропавших и единиц разыскиваемого оружия и т. д.;

3) автоматизированные информационные системы регистрации и учета преступлений, лиц, их совершивших, осужденных, заключенных, иной статистической информации о деятельности правоохранительных органов, судов, других юридических учреждений.

Для удобства использования АИС с 2005 года в правоохранительных органах широко стали распространяться автоматизированные рабочие места (АРМ). Это

позволило уже к концу 2006 г. далеко продвинуться в создании Единой информационно-телекоммуникационной системы МВД РФ. С ее помощью стала возможной комплексная автоматизация деятельности следователей и руководителей следственных органов. Внедренное программное обеспечение, используемое в качестве средства информационных технологий, призвано оказать поддержку сотрудников любого уровня при расследовании преступлений.

Единая система информационно-аналитического обеспечения деятельности МВД РФ (ИСОД МВД)

В марте 2012 года МВД утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России в 2012-2014 гг. Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства.

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) МВД, который велся с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений МВД с другими правоохранительными органами и госорганами различных уровней.

Основной причиной принятия решения о создании ИСОД в материалах структур МВД называется отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем в ведомстве.

В процессе создания ИСОД решены задачи автоматизации основных видов деятельности подразделений МВД, организации централизованного хранения и обработки данных. По задумке МВД, система должна стать единым источником информации для всех сотрудников подразделений МВД, служить для организации электронного взаимодействия между ними, обеспечения разграниченного доступа к информационным ресурсам.

Электронный документооборот

Еще одним достижением ИТ-технологий, изменившие жизнь юридической общественности стали электронный документ (ЭД), электронный документооборот (ЭДО) и электронная подпись (ЭП). ЭД, ЭДО и ЭП были разработаны, апробированы и внедрены в общественную жизнь нашей страны благодаря Федеральной целевой программе «Электронная Россия (2002 – 2010 годы)», утвержденной Постановлением Правительства РФ от 28.01.2002 № 65 (ред. от 09.06.2010).

На сегодняшний день ЭДО постоянно совершенствуется, трансформируясь в электронные доказательства и систему их оценки. Это допускается такими нормативными документами, как ГПК, УПК, а также АПК России. Электронный документооборот в юридической сфере выступает в форме: электронных доказательств; электронной системы, оценивающей эти доказательства. Электронными доказательствами являются аудио- и видеозаписи, электронные переписки, SMS-сообщения и т. д. К рассмотрению они принимаются в том случае, когда несут на себе следы каких-либо правонарушений. Это могут быть письма с угрозами, SMS-мошенничество и т. д.

Электронная подпись

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Информация в электронной форме, подписанная простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны устанавливать:

- 1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;
- 2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

- 1) простая электронная подпись содержится в самом электронном документе;
- 2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Не допускается использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну.

Техническое обеспечение **усиленной** (неквалифицированной и квалифицированной) **электронной подписи** основано на использовании методов криптографии.

Любой документ можно рассматривать как уникальную последовательность символов. Изменение хотя бы одного символа в последовательности будет означать, что в результате получится уже совсем другой документ, отличный от исходного.

Безопасность электронных документов

На сегодняшний день любая ПЭВМ, подключенная к ИСОД МВД России, может использоваться для реализации угроз информационной безопасности, которые могут быть направлены не только на конкретную автоматизированную систему, но и на функционирование ИСОД МВД России в целом. Поэтому для обеспечения конфиденциальности, целостности и доступности информации, циркулирующей в ИСОД МВД России, а также для стабильного функционирования органов внутренних дел в целом, необходимо обеспечить состояние защищенности всех клиентских ПЭВМ в ИСОД МВД России. Согласно исследованиям ЗАО «Позитив Текнолоджиз», проведенных в 2016 году, практически в половине случаев (45%) при реализации компьютерных атак злоумышленники использовали вредоносное

программное обеспечение. А с учетом особенностей организации ИСОД МВД России, где отсутствуют подключения к сетям общего пользования, данный тип атак, как менее затратный, становится еще более актуальным. Поэтому задача противодействия вредоносному программному обеспечению является одной из основных для подсистемы обеспечения информационной безопасности в ИСОД МВД России. Для борьбы с вредоносным программным обеспечением существует специализированное программное обеспечение. Первые такие средства появились сразу после появления первых компьютерных вирусов.

В настоящее время развитие антивирусных средств привело к признанию их в качестве полноценных средств защиты информации в системах сертификации ФСБ России и ФСТЭК России. Приказом ФСТЭК России от 20 марта 2012 года № 28 утверждены «Требования к средствам антивирусной защиты». В первую очередь данные требования предназначены для организаций, осуществляющих работы по созданию средств защиты информации, заявителей на осуществление сертификации продукции, а также для испытательных лабораторий и органов по сертификации средств защиты информации.

Определены 6 классов защиты антивирусных средств. Самый низкий класс — 6, самый высокий — 1. Антивирусные средства с 6 по 4 класс защиты применяются в информационных системах персональных данных, государственных информационных системах, информационных системах общего пользования, в которых не содержится сведений, составляющих государственную тайну. Антивирусные средства с 3 по 1 класс защиты применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну. Также выделяют 4 типа средств антивирусной защиты: «А», «Б», «В», и «Г». Конкретные требования к функциям безопасности, а также взаимосвязи этих требований для каждого класса и типа средств антивирусной защиты, приводятся в соответствующих профилях защиты, утвержденных ФСТЭК России 14 июня 2012 года. В пункте 8 статьи 14 Федерального Закона Российской Федерации от 27.07.2016 № 149 (в редакции от 19.12.2016) «Об информации, информационных технологиях и защите информации» определено, что «...Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании». В Специальных требованиях по защите конфиденциальной информации (СТР-К), утвержденных в ФСТЭК России, также

сказано, что «Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации средства защиты информации...». Таким образом, в государственных органах могут использоваться только антивирусные средства, прошедшие оценку соответствия в системе сертификации средств защиты информации.

ЭДО и ЭП представляют собой элементы, создающие защитное обеспечение информационных технологий. Это позволяют сделать кодовые замки и антивирусные программы, система логинов и паролей и т. д.

Технические устройства

Трудно спорить с тем, что технические устройства изменили юридическую жизнь в плане добывания, фиксации и исследования доказательств. Другой разговор, что подразумевать под техническими устройствами. В первую очередь это технические средства, применяемые в разведывательной работе (средства аудио, видеозаписи и т. д.), которые органы госбезопасности активно применяют с момента их создания.

Далее идут современные средства, такие как мобильные устройства коммуникации (мультимедийные смартфоны iPhone, iPad, планшетные ПК), мобильные средства защиты свидетеля. Начиная с 2011 года стали появляться так называемые мобильные СПС, мобильные версии правовых порталов. В настоящее время получить любую правовую информацию, включая информацию о судебных делах, оперативные сводки возможно не только с помощью компьютера, но и с помощью, например, мультимедийных смартфонов iPhone. Так, по адресу www.arbitr.ru/ejustice2/ikad находится бесплатное приложение «Мобильная картотека». Ее основная функция: экспресс-получение информации о движении практически любого арбитражного дела. Еще одно новейшее средство – это мобильное средство защиты свидетеля. Последнее представляет собой комплекс технических решений, в который

входят следующие элементы: плазменная панель, web-камера, микрофон, колонки, устройство по изменению речи свидетеля. Само мобильное средство располагается в смежной от зала судебного заседания комнате. Можно думать, что следующий положительный шаг со стороны правоохранительных органов будет заключаться в организации подобных специально оборудованных помещений вне мест проведения судебных заседаний

Видеоконференцсвязь (ВКС)

Данный вид ИТ-технологий юристам известен давно. В настоящее время ВКС обеспечивает проведение судебных заседаний в режиме удаленного участия осужденных, свидетелей и потерпевших в судах общей юрисдикции и между участвующими сторонами в арбитражных судах. Эффект от ВКС очевиден – экономия средств, времени и сил. В самом деле, нецелесообразно этапировать (что предполагает задействование внутренних войск, спецвагонов, других спецсредств, колоссальная трата времени) подсудимого из другого города ради уточнения некоторых обстоятельств дела. Ближайшая эволюция ВКС, по крайней мере, в арбитражных судах, проведение ВКС в режиме on-line и off-line. То есть трансляция судебного заседания в режиме реального времени либо просмотр архивных видео-файлов.

Интересно отметить сходство в технике проведения и техническом оснащении ВКС и мобильных средств защиты (МСЗ). Однако имеются и принципиальные различия:

- 1) ВКС – это всегда двусторонняя связь, тогда как МСЗ предполагает одностороннюю связь;
- 2) в МСЗ есть устройство, изменяющее голос свидетеля, во всех остальных технических средствах ВКС и МСЗ совпадают;
- 3) различные цели применения.

Для ВКС это установление удаленного диалога, для МСЗ – обеспечение физической безопасности свидетеля.

Правовые порталы

На сегодняшний день насчитывается несколько наиболее востребованных интернет-сайтов, содержащих информацию юридического плана. Ценность таких порталов заключена в наличии на них автоматизированных систем оперативной информации (сводок), судебных актов и т. д. В западноевропейских странах реализуется специальная программа, находящаяся на правовых государственных порталах. Она позволяет подавать документы в арбитражный суд юридическим и физическим лицам.

1. Официальный интернет-портал правовой информации	(http://pravo.gov.ru)	Официальный интернет-источник правовой информации
2. Портал ВАС РФ	(http://arbitr.ru)	Размещаются интегрированные системы, такие как картотека арбитражных дел; календарь судебных заседаний; решения арбитражных судов; бесплатное приложение «Мобильная картотека»
3. Портал правоохранительных органов	(http://112.ru)	Размещение таких сервисов, как «найденные дети»; «участковые»; «проверка автотранспортного средства»; «розыск»
4. Портал Государственной автоматизированной системы Российской Федерации «Правосудие»	(http://sudrf.ru)	Содержит такие подсистемы, как «банк судебных решений (судебной практики)»; «видеоконференцсвязь»; «документооборот»; «обращения граждан»

5. Портал
Правительства
Российской Федерации

(<http://правительство.рф>)

Содержит ссылки на сайты исполнительной власти, президента РФ, на порталы «Госзакупки», «Госуслуги», «Общественных экспертиз законопроектов РФ»;

оснащен интерактивным общением с гражданами.

6. Портал «Почта
России»

(<http://почта-россии.рф>)

Снабжен поиском отделений почтовой связи, сервисом по отслеживанию почтовых отправлений.

7. Информационный
нотариальный портал

(<http://notary.ru>)

Содержит базы данных о нотариальных палатах и частнопрактикующих нотариусах России, судебную практику нотариусов и Нотариальных палат.

Спутниковая навигационно-мониторинговая система ГЛОНАСС в системе МВД России

Развитие навигационно-мониторинговых систем на базе передовых технологий ГЛОНАСС является важной составляющей совершенствования технической оснащённости органов внутренних дел МВД России, повышения эффективности их деятельности. До последнего времени вопросы внедрения спутниковых технологий ГЛОНАСС для организации контроля подвижных объектов системы МВД России регламентировались утвержденными приказом МВД России от 31 декабря 2008 г. № 1197 общими тактико-техническими требованиями к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России. Применение указанных ОТТТ позволило прийти к определенной стандартизации используемого бортового навигационного оборудования и применяемых навигационно-мониторинговых систем. Однако

с момента разработки ОТТТ технологии ГЛОНАСС и тесно связанные с ними технологии беспроводной связи шагнули далеко вперед, что дает основу усовершенствования концептуальных подходов к дальнейшему развитию навигационно-мониторинговых систем МВД России.

В этой связи необходимо, в частности, отметить следующие важные обстоятельства:

- появились комплектующие изделия, в том числе и отечественного производства, и технологии, расширяющие функциональные возможности навигационно-мониторинговых систем и существенно улучшающие отдельные технические характеристики НАП;
- в системе МВД России внедряются новые стандарты цифровой беспроводной связи, которая также должна использоваться и в качестве транспортной среды для передачи навигационной информации;
- в системе МВД России развернута и развивается единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД), с которой должны сопрягаться создаваемые центры мониторинга, накоплен определенный опыт в сфере взаимодействия навигационных сервисов и сервисов автоматизации служебной деятельности подразделений в рамках единых автоматизированных информационных систем;
- при формировании мероприятий МВД России в рамках Федеральной целевой программы «Поддержание, развитие и использование системы ГЛОНАСС на 2012 – 2020 годы» был расширен круг специальных потребителей из различных служб МВД России, в том числе тех, которые в силу специфики выполняемых ими оперативно-служебных задач не могут использовать в своих интересах территориальные центры мониторинга (например, подразделения — субъекты оперативно-розыскной деятельности, охранно-конвойные подразделения и т. д.). Поставлена задача создания в их интересах прикладных навигационно-мониторинговых систем с дополнительными возможностями информационного обеспечения;
- в территориальных подразделениях органов внутренних дел по-прежнему эксплуатируются порядка 10 разнородных навигационно-мониторинговых систем, причем, как правило, они не могут взаимодействовать друг с другом из-за использования различных протоколов информационного обмена, различных типов электронных карт и различных типов навигационной аппаратуры

потребителей (НАЛ);

- быстрыми темпами проходит внедрение навигационных технологий в Национальной гвардии РФ. При этом в силу ряда объективных причин подразделения Росгвардии используют навигационно-мониторинговые системы ГЛОНАСС, по своим тактико-техническим характеристикам, а прежде всего по применяемому специальному программному обеспечению, заметно отличающиеся от систем, используемых подразделениями органов внутренних дел. Отсюда вытекает задача обеспечения информационного сопряжения этих систем между собой при проведении совместных мероприятий;

- отдельно необходимо отметить тот факт, что на сегодняшний день еще не вполне решенными остаются вопросы защиты навигационной информации;

- в результате проведения МВД России ряда НИОКР выработаны дополнительные требования к системам контроля и управления подвижными объектами, а также к показателям назначения, функциональным возможностям и конструктивным особенностям НАП. Развитие навигационно-мониторинговых систем на базе передовых технологий ГЛОНАСС является важной составляющей совершенствования технической оснащенности органов внутренних дел МВД России, повышения эффективности их деятельности. До последнего времени вопросы внедрения спутниковых технологий ГЛОНАСС для организации контроля подвижных объектов системы МВД России регламентировались утвержденными приказом МВД России от 31 декабря 2008 г. № 1197 общими тактико-техническими требованиями к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России. Применение указанных ОТТТ позволило прийти к определенной стандартизации используемого бортового навигационного оборудования и применяемых навигационно-мониторинговых систем. Однако с момента разработки ОТТТ технологии ГЛОНАСС и тесно связанные с ними технологии беспроводной связи шагнули далеко вперед, что дает основу усовершенствования концептуальных подходов к дальнейшему развитию навигационно-мониторинговых систем МВД России. К числу проведенных НИОКР относятся такие работы, как «Центр НМС», «Протокол КС», «Протокол ГЛОНАСС», «Диафон», «Система МВД», «ГЛОНАСС-МВД», а также осуществляемая в настоящее время ОКР «Элемент». Результаты этих НИОКР, включая промежуточные, позволяют, в частности, сформулировать ряд принципов и положений, которые могут лечь в основу новых подходов к развитию спутниковых навигационно-мониторинговых систем ГЛОНАСС.

Государственные услуги в электронном виде

МВД России предоставляет населению наиболее востребованные услуги — от выдачи водительских удостоверений до решения вопросов, связанных с получением гражданства. При столь широком спектре услуг ведомству необходимо постоянно работать над их качеством, а также решать ряд неизбежно возникающих проблем информационно-технического характера. Так, в связи с прошедшей в 2016 году реорганизацией МВД России, в ходе которой в состав Министерства вошла упраздненная ФМС России и были исключены подразделения лицензионно разрешительной работы, возникла необходимость проведения работ по интеграции и дезинтеграции их информационных систем. МВД России стало одним из первых ведомств, подключившихся к системе мониторинга качества предоставления госуслуг. Возможность оценить качество оказания услуг подразделениями МВД России граждане получили в 2014 году. Как показывает статистика сайта «Ваш контроль», госуслуги МВД России являются одними из самых популярных госуслуг среди граждан. Ведомство традиционно лидирует по числу оценок, поступивших от россиян.

За получением многих госуслуг граждане могут обратиться в многофункциональные центры предоставления государственных и муниципальных услуг (МФЦ) или же получить их через Единый портал государственных и муниципальных услуг (ЕПГУ), даже не выходя из дома. За несколько лет в России создана и успешно работает система межведомственного электронного взаимодействия. Теперь гражданину нужно посетить государственное учреждение не более двух раз — в момент подачи документов и для получения конечного результата услуги. Результат оказания части госуслуг предоставляется в электронном виде и доступен в личном кабинете граждан на ЕПГУ или направляется на адрес электронной почты заявителя.

Список используемой литературы

- Васильев Д. Компьютер вместо юрисконсульта // Наука и жизнь — 2001.
- Введение в правовую информатику. Справочно-правовые системы КонсультантПлюс: учебник для вузов / под. общ. ред. Д. Б. Новикова, В. Л. Камынина. – М.: КонсультантПлюс – Новые Технологии, 2009.
- Амелин, Р. В. Автоматизированная информационная система как источник права / Р. В. Амелин,

- С. Е. Чаннов // Информационное право. – 2008.
- Информационные технологии, связь и защита информации МВД России -2017
<https://media.mvd.ru/files/embed/1163358>
- [http://www.tadviser.ru/index.php/Проект:Единая_система_информационно-аналитического_обеспечения_деятельности_МВД_РФ_\(ИСОД_МВД\)](http://www.tadviser.ru/index.php/Проект:Единая_система_информационно-аналитического_обеспечения_деятельности_МВД_РФ_(ИСОД_МВД))
- <http://fb.ru/article/188730/informatsionnyie-tehnologii-v-yuridicheskoy-deyatelnosti-primeryi-informatsionnyih-tehnologiy>
- <https://studfiles.net/preview/6058633/page:6/>