Тип работы: Дипломная работа

Предмет: Информационные системы и процессы

1.2. Нормативно правовое обеспечение регламентирующее защиту персональных данных
Ст. 23 Конституции Российской Федерации подтверждает право граждан на неприкосновенность личной жизни и защиту чести и достоинства [1]. А ст.24 предусматривает, что сбор, обработка и передача персональных данных без согласия гражданина являются незаконными. Всемирная декларация и Международный пакт о гражданских и политических правах защищают людей от несанкционированного вмешательства в частную жизнь и разглашения информации из личных сообщений. Важно знать, что такое персональные данные, как предотвратить незаконное использование и что ответственность за такие действия предусмотрена законом.
В соответствии с законодательством Российской Федерации существует 4 категории персональных данных, подлежащих правовой защите:
1. Общедоступные персональные данные означают информацию, которая не подпадает под понятие конфиденциальности, или которая по соглашению с гражданином доступна широкому кругу лиц (включена в адресную книгу или телефонную книжку), и такие данные могут быть удалены из этих источников по заявлению самого гражданина или по решению суда. решение суда.
2. Особые персональные данные - информация о национальности, расе, состоянии здоровья, философских, религиозных и политических убеждениях. Сбор, хранение и обработка указанных данных допускается только с согласия гражданина, которое осуществляется в письменной форме (оформление нотариально заверенной доверенности не предусмотрено). Исключениями являются сбор и обработка данных в ходе оперативно-розыскных мероприятий, других уголовно-процессуальных мероприятий, а также в случаях, когда гражданин по состоянию здоровья не может дать такое разрешение.
3. Персональные данные, обрабатываемые информационной системой. Такие данные сообщают сами субъекты в социальных сетях, на сайтах знакомств, форумах или блогах. Однако проверить их подлинность трудно.
4. Биометрические данные - это информация личного характера о физиологических особенностях, которые позволяют идентифицировать граждан. К ним относится фото- и видеосъемка граждан. Обработка и распространение персональных данных данной категории подпадает под санкции статьи 11 федерального закона "О персональных данных", которая предусматривает обязательное согласие граждан. Должностные лица Министерства внутренних дел, а также сотрудники тюрем и органов государственной безопасности, выполняющие служебные обязанности, получают право на фото- и видеосъемку без такого разрешения.
Все методы защиты персональных данных условно делятся на 3 типа:
1. Нормы, прописанные в гражданском и трудовом законодательстве, регулируют отношения между гражданами и государственными служащими, наемными работниками и работодателями.
2. Перечень правовых и организационных мер, ограничивающих полномочия работодателей и

государственных служащих.
3. Гарантия права физического лица на безопасность персональных данных.
Для защиты персональных данных законодатель предусматривает:
 неоплачиваемый, открытый доступ к персональным данным физических лиц, предоставление копий информации, включая персональные данные;
 подбор физических или юридических представителей для защиты персональных данных;
 открытость информации об использовании и распространении персональных данных;
 требования к исправлению персональных данных в случае обнаружения ошибок в персональных данных;
 в целях защиты персональных данных компании-работодатели или государственные служащие в случае выявления незаконных действий обращаются с иском в суд.
Статья 150 Гражданского кодекса Российской Федерации относится к нематериальным правам, охраняемым правовой защитой личной неприкосновенности граждан и их жилищ, а также для обеспечения сохранности данных, в том числе личной конфиденциальной информации. Гражданский кодекс также вводит понятие морального ущерба, который является результатом морального или физического проступка, нарушения конфиденциальности персональных данных. Это является основанием для назначения денежной компенсации за причиненный ущерб.
При расчете размера компенсации, в соответствии с положениями Гражданского кодекса Российской Федерации, суд обращает внимание на следующее:
 халатность злоумышленника;
 вред, причиняемый распространением персональных данных;
 личные характеристики лица, пострадавшего от незаконных действий.
Потерпевший имеет право обратиться в суд с заявлением об опровержении данных, которые не соответствуют действительности, подрывают его честь и деловую репутацию, если ответчик не докажет достоверность таких данных. Публикация и использование персональных данных в виде фотографий и видеоизображений граждан допускается только после получения согласия на эти действия.
Материальная ответственность за разглашение персональных данных, подлежащих правовой защите, эквивалентна сумме причиненного ущерба. Эта норма предусмотрена пунктом 7 статьи 243 Трудового кодекса. Данный случай полной компенсации понесенного ущерба является исключением из правил, подтверждающим первостепенную важность защиты персональных данных [4].
Дисциплинарная ответственность включает в себя увольнение других сотрудников организации или сотрудников, которые санкционировали распространение персональных данных клиента. Это положение применяется только в том случае, если раскрытие персональных данных происходит в результате выполнения обязанностей нарушителем. Нести дисциплинарную ответственность за распространение персональных данных - это право, а не обязанность работодателя. При назначении этого наказания учитываются следующие обстоятельства:
 степень вреда, причиненного разглашением персональных данных;
 ситуация при совершении этого преступления.
К сотрудникам, виновным в незаконном распространении персональных данных, применяются следующие дисциплинарные взыскания:
 замечания;
 выговор;
 увольнение.
Административная ответственность за незаконное получение, хранение, обработку и распространение персональных данных граждан предусматривает устные предупреждения или штрафы для физических лиц в размере 300-500 рублей для сотрудников, 500-1000 рублей для предприятий и 5000-10 000 рублей. Эта норма изменена в статье 13.11 Кодекса Российской Федерации об административных правонарушениях. За распространение персональных данных, полученных в результате исполнения служебных обязанностей, налагается административный штраф в размере 500-1000 рублей. Если сотрудник причастен к этому преступлению, размер штрафа увеличивается с 4000 рублей до 5000 рублей. Эта санкция предусмотрена статьей 13.14 Закона об административных правонарушениях.
Уголовная ответственность за нарушения правил защиты персональных данных предусмотрена статьей 137 Уголовного кодекса России. Несанкционированное получение, хранение и передача данных, составляющих семейную и личную тайну, без согласия гражданина, использование этой информации в публичных выступлениях и демонстрациях произведений искусства, публикация таких данных в средствах массовой информации (массмедиа) наказывается уголовным штрафом в размере до 200 000 рублей, общественным

или исправительные работы, или арест на срок до 4 месяцев. Если это деяние совершено должностным лицом, то сумма штрафа увеличится до 300 000 рублей, а срок ареста - до 6 месяцев.
В соответствии с требованиями Федерального закона «О персональных данных» юридические лица обязаны принимать меры по защите персональных данных, но имеют право самостоятельно определять перечень таких мер. Меры, принимаемые для защиты персональных данных, можно разделить на две большие подгруппы: внутренняя защита персональных данных и внешняя защита [12].
Меры, принятые для внутренней защиты персональных данных, включают в себя следующие меры:
 управление ограничением числа работников (с указанием их должностей), которым открыт доступ к персональным данным. Кого может включать в себя этот список? Для всех, кто имеет доступ к личным делам, то есть сотрудников отдела кадров или менеджеров по найму, сотрудников бухгалтерии, офисных секретарей, специалистов, заключающих контракты с физическими лицами, а также инженеров, программистов, юристов;
 назначение ответственного лица, обеспечивающего соблюдение организацией законодательства в соответствующей области. назначение ответственного лица, обеспечивающего соблюдение организацией законодательства в соответствующей области;
 утверждение списка документов, содержащих персональные данные;
 публикация внутренних документов по защите персональных данных, мониторинг их соблюдения;
 знакомить сотрудников с действующими правилами защиты персональных данных и местными нормативными актами; проводить систематические проверки соответствующих знаний сотрудников, обрабатывающих персональные данные, и обеспечивать соблюдение ими правил защиты конфиденциальной информации. Обратите внимание, что всем сотрудникам, имеющим доступ к персональным данным других лиц, необходимо ознакомиться с особенностями законодательства о защите данных;
 рациональное размещение рабочих мест, чтобы исключить несанкционированное использование защищенной информации;
 утверждение списка лиц, имеющих доступ к помещениям, в которых хранятся персональные данные;
 подтверждение утверждения процедуры уничтожения данных;
 выявление и устранение нарушений требований к конфиденциальности;
 проводить профилактическую работу с сотрудниками, чтобы предотвратить раскрытие ими личной информации.
Среди мер внешней защиты персональных данных следует выделить такие, которые:
 недавно был введен режим пропускной способности, порядок, в котором посетители могут быть приняты и зарегистрированы;
 требует внедрения технических средств защиты, программного обеспечения для защиты информации на электронных носителях и т.д.
Хотя законом не установлены конкретные требования к количеству и содержанию локальных актов в Организации по обработке и защите персональных данных, практика реализации этого закона сформировала необходимый минимум документов, которые необходимо разработать на предприятии:
 общий документ, определяющий политику компании в отношении обработки персональных данных, такую как определение персональных данных;
 список лиц, обрабатывающих персональные данные;
 распоряжаться назначением сотрудника, ответственного за организацию обработки персональных данных. Это лицо должно осуществлять внутренний мониторинг соблюдения компанией и ее сотрудниками законов «О персональных данных», включая требования к их защите, информировать персонал о положениях законов «О персональных данных», местных нормативных актах, регулирующих обработку персональных данных, требованиях к защите таких данных, принимать и обрабатывать запросы и организовывать запросы лиц, запрашивающих персональные данные, и (или) контролировать получение и обработку таких запросов и запросов;
 положения, касающиеся правовых, организационных и технических мер по защите персональных данных от неправильного использования или случайного доступа, их уничтожения, изменения, блокировки, копирования, предоставления, распространения и других противоправных действий в отношении персональных данных. В этом положении рекомендуется прописать конкретные меры защиты персональных данных (введение режима пропускной способности, использование программ защиты информации - паролей, антивирусных программ, хранение персональных данных отдельно от другой информации, на отдельных материальных носителях и в специально оборудованных помещениях с

ограниченным доступом и т.д.). В этом положении рекомендуется указать конкретные меры по защите персональных данных (ввод режима пропускной способности, использование программ защиты информации - паролей, антивирусных программ, хранение персональных данных отдельно от другой информации, на отдельных материальных носителях и в специально оборудованных помещениях с ограниченным доступом и т.д.) [20].
Как местный акт, устанавливающий процедуры предотвращения и выявления нарушений законодательства в сфере защиты данных и устранения последствий таких нарушений. Так, компания может разработать план действий по внутреннему контролю за безопасностью персональных данных, Инструкции о порядке проведения служебного расследования по факту нарушения права на защиту персональных данных, протокол антивирусных проверок и контроля работы с персональными данными, протокол обучения, инструктажа и сертификации по защите персональных данных.

1.3. Особенности защиты персональных данных в правоохранительных органах
Защита информации относится к защите права владеть информацией и распоряжаться ею, ограничению ее распространения, устранению или существенному скрытию кражи, конфиденциальной информации и незаконного доступа к ее владельцам. Кроме того, концепция информационной безопасности - это информационная безопасность, которая защищает инфраструктуру от случайных или преднамеренных воздействий естественного или искусственного характера, наносящих ущерб владельцу или пользователю информации и связанной с ней инфраструктуры. Он также поддерживает множество приложений, таких как: современный этап общественного развития характеризуется повышением роли информационной сферы. Информационная сфера - это совокупность новых систем регулирования информации, информационной инфраструктуры, субъектов, которые собирают, формируют, распространяют и используют информацию, а также связей с общественностью. В доктрине под информационной безопасностью Российской Федерации понимается состояние защищенности национальных интересов в информационной сфере, которое определяется совокупностью сбалансированных интересов людей, общества и государства [21].
Национальная политика информационной безопасности России основана на следующих принципах:
1. Соблюдение Конституции Российской Федерации, законов Российской Федерации, общепринятых принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации.
2. Открытость при осуществлении функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и государственных учреждений с учетом ограничений, установленных законодательством Российской Федерации.
3. Юридическое равенство всех участников процесса информационного взаимодействия, независимо от политического, социального и экономического статуса, заключается в праве свободно искать, получать, передавать, производить и распространять информацию законным способом.
4. В целях соблюдения жизненно важных интересов Российской Федерации приоритетное развитие современных информационно-коммуникационных технологий в стране, производство технических и программных средств, способных совершенствовать отечественные телекоммуникационные сети, их подключение к глобальным информационным сетям.
Министерство внутренних дел Российской Федерации является оператором, который организует и осуществляет обработку персональных данных, обязано принимать правовые, организационные и технические меры по защите персональных данных от несанкционированного или случайного доступа от других незаконных действий, связанных с этой информацией.
Закон устанавливает, что перечень мер, направленных на выполнение обязательств, связанных с обработкой персональных данных государственными органами, устанавливается Федеральным правительством России. Состав и содержание конкретных требований к защите персональных данных, организационных и технических мер по обеспечению безопасности при обработке в Информационной системе персональных данных (далее - ISPDn) устанавливаются в пределах своей компетенции ФСБ России и ФСТЭК России [23].
Для обеспечения выполнения требований законодательства Российской Федерации в области защиты персональных данных при обработке в органах внутренних дел необходимо создать соответствующую систему защиты персональных данных (далее - NWPDn). Такая система предназначена для обеспечения конфиденциальности, целостности и доступности персональных данных при их обработке в ISPDn территориального органа МВД России.

NWPDn - это набор объектов защиты информации, а также ассоциаций, исполнителей и используемых ими технологий защиты информации. Она организована и эксплуатируется в соответствии с правилами и предписаниями, установленными соответствующими документами в области защиты информации.
В соответствии с требованиями приказа МВД России, NWPDn включает организационные и технические мероприятия, средства защиты информации и предотвращения несанкционированного доступа, утечки информации по техническим каналам, технического воздействия на технические средства обработки программного обеспечения и персональных данных, а также информационные технологии, используемые в ISPDn.
В то же время существуют некоторые различия в составе элементов системы защиты информации между той, которая определена гостем, и приказом МВД России. Это несоответствие в элементах системы должно быть устранено путем изменения порядка расположения отделов.
Итак, принимая во внимание вышеизложенное, мы можем определить, что система защиты персональных данных органов внутренних дел состоит из следующих элементов:
1. Персональные данные и носители таких данных.
2. Персонал, отделы и служащие, ответственные за организацию и выполнение работы по защите персональных данных.
3. Методы, технологии и средства защиты персональных данных.
4. Меры, принимаемые для защиты персональных данных.
Согласно Федеральному закону, органы внутренних дел имеют право обрабатывать персональные данные в связи с осуществлением общественных или производственных отношений, а также предоставлением государственных услуг и осуществлением государственных функций. Обработка персональных данных органами внутренних дел осуществляется в соответствии с целями и условиями обработки персональных данных, определенными в Законе о персональных данных [7].
Законом о персональных данных и Постановлением Правительства 2011/3/2 № 211 утвержден перечень мер, направленных на обеспечение выполнения обязательств, предусмотренных федеральным законом «О персональных данных», и в соответствии с ним утверждены нормативные правовые акты, принимаемые операторами, органами государственной власти или местного самоуправления.
Для реализации вышеуказанного перечня Министерство внутренних дел Российской Федерации (далее - Министерство), как государственный орган, несет ответственность за обеспечение выполнения обязательств, предусмотренных Законом о персональных данных.
Эти акты включают в себя:
- Приказ МВД России от 29.12.2016 №925 «Об отдельных вопросах обработки персональных данных в Министерстве внутренних дел России»;
- Приказ МВД России от 7.07.17 № 467 «Об утверждении Правил рассмотрения запросов субъектов персональных данных или их представителей в Министерстве внутренних дел Российской Федерации»;
- Приказ МВД России от 14.11.2017 №852 «Об утверждении Правил обращения с неперсонифицированными данными в случае обезличивания персональных данных в Министерстве внутренних дел Российской Федерации»;
- Приказ МВД России № 949 «О конкретных мерах, направленных на обеспечение исполнения обязательств МВД России, предусмотренных ФЗ «О персональных данных».

Обработка персональных данных в системе Министерства внутренних дел России допускается только для целей категории объектов, предусмотренных нормативными правовыми актами Министерства внутренних дел России. Не допускается обработка персональных данных в связи с другими целями и другими категориями субъектов. Система Министерства внутренних дел России обрабатывает только персональные данные, указанные в нормативных правовых актах. Перечень обрабатываемых персональных данных является открытым, поскольку субъект персональных данных имеет право дополнительно предоставить иную информацию о себе. Содержание этих положений непосредственно соответствует понятию «Персональные данные», поскольку другая информация может означать любую информацию, прямо или косвенно относящуюся к конкретному или идентифицируемому физическому лицу (субъекту персональных данных). Стоит отметить, что для каждой цели, для которой обрабатываются персональные данные, определяется содержание обрабатываемых персональных данных и соответствующая категория субъектов.
Обработка персональных данных или доступ к персональным данным в территориальных органах МВД России разрешен всем должностям рядового и начальствующего состава органов внутренних дел и должностям федеральных государственных гражданских служащих, если служебные обязанности сотрудника и должностного лица в обязанности Федеральной государственной гражданской службы

входит обработка персональных данных или доступ к персональным данным.
Министерство предоставляет третьим лицам персональные данные, полученные в ходе осуществления государственных или трудовых отношений, а также в связи с предоставлением государственных услуг и осуществлением государственных функций, в соответствии с законодательством в области персональных данных.
Примерами правового основания для предоставления персональных данных являются органы местного самоуправления, предоставляющие государственные или муниципальные услуги, в ответ на межведомственные запросы государственных органов, предоставляющие информацию о наличии непогашенной или неснятых судимостей у лица, если предоставление такой информации или документов, содержащих такую информацию, является обязательным. предусмотрено для предоставления государственных или муниципальных услуг конкретному государственному или муниципальному учреждению.
Что касается получения Министерством информации, представляющей собой информацию о персональных данных, то этот процесс также регулируется процедурами, установленными законодательством Российской Федерации в области персональных данных.
Полномочия по запросу Министерства информации, включая информацию о персональных данных, регулируются Федеральным законом от 07.02.2011 № 3-Фз «О полиции», полиция имеет право при исполнении своих обязанностей в связи с расследуемыми уголовными делами и расследуемыми административными преступлениями, а также поскольку в связи с проверкой зарегистрировано в установленном порядке сообщение, его разрешение отнесено к возможностям полиции. Запрашивать и получать информацию, справки, документы (их копии) и другую необходимую информацию, включая персональные данные гражданина, бесплатно по обоснованному запросу уполномоченных сотрудников полиции от государственных и муниципальных органов, общественных объединений, организаций, должностных лиц и граждан, за исключением случаев, когда установлены специальные процедуры получения информации по информации федерального закона.
Существует три типа информационных угроз:
1. Опасность нарушения доступности.
2. Угроза нарушения целостности.
3. Угроза вторжения в частную жизнь.
Доступность информации является атрибутом системы (среды, средства и технологии обработки) обращения информации. Его особенность состоит в том, чтобы гарантировать, что субъекты имеют своевременный и беспрепятственный доступ к интересующей их информации, а также в любое время подготовить соответствующие автоматизированные услуги для удовлетворения потребности в обработке запросов на обслуживание, выполняемых субъектами [15].
Нарушение доступности - это создание условий, при которых доступ к услугам или информации будет заблокирован или определенные бизнес-цели могут не быть предоставлены в течение определенного периода времени. Рассмотрим пример: в случае сбоя сервера, на котором находится информация, необходимая для принятия стратегического решения, атрибут доступности информации нарушается. Аналогичный пример: в случае изоляции по какой-либо причине (сбой сервера, сбой коммуникационного соединения и т. д.) почтовый сервер можно говорить о нарушении доступности сервиса «Электронная почта». В частности, следует отметить, что причина нарушения доступности информации или информационных услуг не обязательно должна быть в рамках ответственности владельца услуги или информации. Например, в приведенном выше примере нарушения доступности почтового сервера причина (сбой канала связи) может быть не в области ответственности администратора сервера (например,).
Следует также отметить, что понятие «доступность» субъективно в любое время для каждого субъекта, потребляющего услуги или информацию в данный момент времени. В частности, нарушение работы сотрудника из-за доступности почтового сервера может означать нарушение личных планов и потерю контракта, а также неспособность получать последние новости от другого сотрудника в той же организации.
Целостность информации заключается в том, что информация существует в неискаженной форме (неизменяемой по отношению к некоторым из ее фиксированных состояний). Чаще всего субъект заинтересован в обеспечении более широкого спектра атрибутов-достоверности информации, включая адекватность (полноту и точность) отображения статуса предметной области и полноту прямой информации, то есть она не искажена [22].
Угроза нарушения целостности - это угроза, связанная с вероятностью изменения определенной

информации, хранящейся в информационной системе. Нарушения целостности могут быть вызваны различными факторами, от преднамеренного поведения персонала до отказа оборудования. Воздействие информации (электромагнитное излучение, внедрение деструктивного программного обеспечения в компьютерные системы, духовное влияние на людей и духовное оружие). Угроза нарушения конфиденциальности заключается в том, что информация становится известной людям, у которых нет разрешения на доступ к ней. Это происходит всякий раз, когда доступ к определенной секретной информации, хранящейся в компьютерной системе, получается или передается из одной системы в другую. Иногда из-за угрозы нарушения конфиденциальности используется термин «утечка». Эта угроза может быть вызвана «человеческим фактором» (например, случайным делегированием привилегий другого пользователя тому или иному пользователю), сбоями программного и аппаратного обеспечения. Применение каждой из этих угроз индивидуально или в сочетании приведет к нарушению информационной безопасности. Можно отметить, что все меры информационной безопасности должны основываться на принципе минимизации этих угроз.
Следует также отметить, что в современном обществе Интернет предоставляет множество возможностей государственным органам, иностранным организациям и различным преступным сообществам для осуществления незаконных и других видов деятельности, представляющих опасность для Российской Федерации. Прежде всего, децентрализованная структура и другие технические характеристики превратили Интернет в совершенно новую среду для организации нетрадиционных каналов обмена информацией.

1. Конституция Российской Федерации от 12дскабря 1993 г.: по сост. на 21 июля 2014 г. Н Собрание законодательства Российской Федерации. — 2014. — № 31. — Ст. 4398.
2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. И Собрание законодательства Российской Федерации. — 2014. — № 5. — Ст. 419
3. Конвенция Содружества Независимых Государств о правах и основных свободах человека от 26 мая 1995 г. // Собрание законодательства Российской Федерации. — 1999.- № 13.-Ст. 1489.
4. Трудовой кодекс Российской Федерации от 30 ноября 2001 N 197-ФЗ: по сост. на 1 июня 2019 г.// Собрание законодательства Российской Федерации. — 2002. — № 1. — Ст. 3.
5. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. № 14-ФЗ: по сост. на 1 июня 2019 г. // Собрание законодательства Российской Федерации. — 1996. — № 5. — Ст. 410.
6. Об оперативной и розыскной деятельности: федеральный закон от 12.08.1995 N 144-ФЗ по сост. на 29 нюня 2018 г. // Собрание законодательства Российской Федерации. — 1995. — № 33. — Ст. 3349.
7. Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федеральный закон от 01 апреля 1996 г. № 27-ФЗ по сост. на 1 декабря 2018 г. // Собрание законодательства Российской Федерации. — 1996- № 14. — Ст. 1401.
8. О персональных данных: федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 31 (часть I). — Ст. 3451.
9. Абдулова, Э. Д. Правовое регулирование в сфере защиты персональных данных / Э. Д. Абдулова. — Текст : непосредственный // Молодой ученый. — 2022. — № 5 (400). — С. 151-154.
10. Аверченков, В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2016. - 260 с.
11. Баксалова А.М. Правоохранительные органы: учебно-методический комплекс/под общ. ред. С.Л. Лоня. Новосибирск. Си. унив. изд-во, 2018. - 144 с.
12. Барбакадзе, В.Т. Защита интересов организации в арбитражном суде (+ CD-ROM) / В.Т. Барбакадзе, А.Н. Ермаков, И.Ю. Захарьящева. - М.: Эксмо, 2019. - 368 с.
13. Белоусов М.Г. Технологии связей с общественностью: учебное пособие. Москва: Московский гос. технический ун-т гражданской авиации, 2016. - 107 с.
14. Благоразумный А.А. Организация общественных связей органов внутренних дел. М.: Академия управления МВД РФ, 2014. - 202 с.
15. Бобунова, С. А. Персональные данные и цифровизация / С. А. Бобунова. — Текст : непосредственный // Молодой ученый. — 2022. — № 36 (431). — С. 75-79.
16. Бозров В.М. Правоохранительные органы: учебник для СПО. Научная школа: Уральский государственный юридический университет (г. Екатеринбург), 2018. - 424 с.
17. Болотнов А.В. К вопросу о динамике информационных волн в медиадискурсе // Вестн. Томского гос. пед. ун-та (TSPU Bulletin), 2016. - № 7 (172). - С. 146-150.

18. Волчихин, В.И. Нейросетевая защита персональных биометрических данных / В.И. Волчихин. - М.: Радиотехника, 2018. - 288 с.
19. Ворошилов, В. В. Современная пресс-служба / В.В. Ворошилов. - Москва: ИЛ, 2014. - 224 с.
20. Газетдинов Н.И. Правоохранительные органы Российской Федерации: учебник. Казань: Казанский университет, 2016. - 302 с.
21. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы (СанПин 2.2.2/2.4.1340-03). - М.: ДЕАН, 2019. - 347 с.
22. Зельманов, А. Б. Связи с общественностью в социальной сфере / А.Б. Зельманов. - М.: Издательство Михайлова В. А., 2016. - 128 с.
23. Киселев, А. Г. Теория и практика массовой информации. Общество. СМИ. Власть / А.Г. Киселев. - М.: Юнити-Дана, 2015. - 432 с.
24. Коноваленко, В. А. Основы интегрированных коммуникаций. Учебник и практикум / В.А. Коноваленко, М.Ю. Коноваленко, Н.Г. Швед. - М.: Юрайт, 2015. - 488 с.
25. Корнеева М.П. Особенности организации начальником территориального органа МВД России на районном уровне внешнего взаимодействия органов предварительного следствия с общественными организациями и средствами массовой информации: статья из сборника «Проблемы управления правоохранительной деятельностью» // Академия управления МВД России, 2018. - №1 (45). - С. 79-84
26. Мазитов Р.Р. Информационная открытость органов внутренних дел и ее критерии //Адвокатская практика, 2016. - № 1. - С. 34-37.
27. Марков А.А. Связи с общественностью в защите имиджа от негативной информации СМИ: монография. СПб: РГГМУ, 2019. - 345 с.