



**Арина Сергеевна
СЕЛЮК,**

ассистент кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА)
arina_selyuk@mail.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Защита персональных данных в цифровом пространстве

Аннотация. Защита персональных данных представляет собой одну из наиболее важных задач на современном этапе развития государства. Эта необходимость определяется цифровизацией, переходом большинства видов деятельности человека в цифровое пространство, а также увеличением численности кибератак и утечек персональных данных в цифровой среде. Цель исследования заключалась в анализе причин и условий повышенных рисков в отношении персональных данных, анализе действующего законодательства РФ в части системы защиты персональных данных в цифровой среде, анализе соответствующего опыта зарубежных стран. В статье определены основные проблемы защиты персональных данных в цифровом пространстве, а также основные направления, требующие совершенствования для обеспечения защиты персональных данных. **Ключевые слова:** персональные данные, цифровая среда, Интернет, цифровизация, киберпреступность, фишинг.

DOI: 10.17803/2311-5998.2023.102.2.110-119

ARINA S. SELYUK,

Assistant of the Department of information law
and digital technologies
of the Kutafin Moscow State Law University (MSAL)
arina_selyuk@mail.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Protection of Personal Data in the Digital Space

Abstract. The protection of personal data is one of the most important tasks at the present stage of the development of states. This need is determined by digitalization, the transition of most human activities into the digital space, as well as an increase in the number of cyber-attacks and leaks of personal data in the digital environment. The purpose of the study was to analyze the causes and conditions of increased risks in relation to personal data, to analyze the current legislation of the Russian Federation regarding the system of personal data protection in the digital environment, to analyze the experience of foreign countries in relation to this issue. The article draws conclusions about the main problems of personal data protection in the digital space, and also identifies the main areas that require improvement to ensure the protection of personal data.

Keywords: personal data, digital environment, Internet, digitalization, cybercrime, phishing.

Права человека — ценностный ориентир для большинства демократических государств, в том числе и для России. Сегодня понятие личных прав, которые должны быть гарантированы государством и защищены соответствующими государственными институтами, значительно расширен. Конституция РФ в ст. 23 устанавливает, что каждому гарантируется право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей части и доброго имени¹.

Какие-либо произвольные ограничения указанных прав недопустимы, за исключением установленных законодательством случаев. Понятие права на неприкосновенность частной и личной жизни включает в себя и возможность пользоваться и распоряжаться своими персональными данными². С переходом к цифровой экономике, расширением сети Интернет, цифровизации общества вопросы охраны и защиты персональных данных, в частности их защита в цифровой среде, становятся все более актуальными, что обусловлено сложностями самой цифровой среды, под которой все чаще понимается информационно-телекоммуникационная сеть Интернет.

Понятие персональных данных закреплено в Федеральном законе «О персональных данных» № 152-ФЗ от 27.07.2006 (далее — Закон о персональных данных): «персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»³. При этом доктринальные источники определяют персональные данные как особый институт охраны права на неприкосновенность частной жизни, как информационный ресурс ограниченного доступа⁴.

Закон о персональных данных определяет персональные данные как конфиденциальную информацию, что следует из положений о доступе к такой информации, особенностей ее распространения. Закон устанавливает обязанности операторов персональных данных по соблюдению требований к их сбору, обработке и распространению, а также закрепляет необходимость формирования системы защиты персональных данных в Российской Федерации.

Однако заложенная российским законодателем система защиты и оборота персональных данных в условиях цифровизации сталкивается с проблемами самой цифровой среды — сети Интернет.

Сегодня, как отмечают многие исследователи, происходит цифровая трансформация (цифровая революция), реализуемая в трех основных этапах:

- IOT (интернет вещей);
- Big Data (большие данные);
- AI (искусственный интеллект)⁵.

¹ Конституция Российской Федерации // URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102027595&ysclid=ld7mdb65j8554953653#l0 (дата обращения: 17.01.2023).

² Сычева М. И. Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. 2022. № 10–3 (73). С. 175.

³ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165.

⁴ Бачило И. Л. Информационное право : учебник для магистров 3-е изд., перераб. и доп. М. : Юрайт, 2015.

⁵ Сибел Т. Цифровая трансформация. Как выжить и преуспеть в новую эпоху. М. : Манн, Иванов и Фербер, 2021. С. 5—15.



На современном этапе развития можно однозначно сказать о применимости трех уровней, так как в большинстве стран мира модернизируется законодательство, а также рассматриваются статус и положение искусственного интеллекта, особенности его применения в финансовых услугах и цифровом пространстве.

Цифровая среда представляет собой информационное пространство, в котором информация может распространяться неограниченно, предполагается простота копирования информации, возможность хранения информации без материального носителя. И основная сложность — невозможность наложить какие-либо юрисдикционные границы на цифровую среду. Соответственно, наиболее важным аспектом данной проблемы выступает необходимость согласованного международного подхода к регулированию оборота персональных данных в цифровой среде.

Эти вопросы в доктрине нередко поднимаются исследователями. Справедливой и обоснованной представляется позиция, согласно которой в современных реалиях цифровое пространство нерегулируемо расширяется, что ведет к господству «цифровой» эры, где право на защиту персональных данных должно быть приравнено к фундаментальным правам и свободам человека⁶.

В последние годы нарастает тенденция к фиксированию случаев утечек персональных данных граждан в сеть Интернет, когда любой злоумышленник может воспользоваться конкретной информацией о гражданине. При этом не имеет значения — были ли использованы данные гражданина для совершения противоправных действий (например, кражи денежных средств со счета по составам мошенничества) либо же была совершена кража персональных данных без их последующего использования. Чаще всего такие данные собираются в специальную базу данных и впоследствии хранятся с целью их возможной будущей перепродажи.

Кража данных представляет собой незаконную передачу или хранение личной, конфиденциальной и финансовой информации⁷.

В 2022 г. фиксировалось рекордное количество утечек персональных данных из крупнейших компаний, осуществляющих свою деятельность в удаленном формате («Яндекс.Еда», Delivery Club, «Гемотест», СДЭК)⁸. Базы персональных данных содержали в себе информацию о пользователях, адресе их проживания, телефонных номерах, а также некоторую банковскую информацию. Данные Роскомнадзора также подтверждают, что с сентября 2022 г. было получено порядка 100 уведомлений от компаний об утечках персональных данных пользователей⁹.

Увеличение случаев утечек персональных данных по большей части неразрывно связано с тенденциями к построению информационного общества,

⁶ Абрамова А. Г. Международно-правовая защита персональных данных в сети Интернет: общие положения // Регион и мир. 2020. Т. 11. № 5. С. 52.

⁷ Что такое кража данных и как ее избежать? // URL: <https://www.kaspersky.ru/resource-center/threats/data-theft?ysclid=ld7atap1ar727360244> (дата обращения: 17.01.2023).

⁸ 14 компаний, откуда утекли данные пользователей в 2022 году // URL: <https://www.sravni.ru/text/14-kompanij-otkuda-utekli-dannye-polzovatelej-v-2022-godu/> (дата обращения: 18.01.2023).

⁹ В Роскомнадзор с сентября поступило порядка 100 уведомлений от компаний об утечках данных // URL: <https://tass.ru/ekonomika/16838265> (дата обращения: 19.01.2023).

повсеместной цифровизацией, а также распространением финансовых технологий, что получило еще более ускоренное развитие в результате пандемии и перехода компаний на предоставление услуг в онлайн-формате. Конечно, переход к предоставлению услуг онлайн дает немало преимуществ для потребителей и компаний — простоту получения услуг для одних, капитализацию и расширение масштабов бизнеса для других.

Однако широкие возможности в рамках предоставления удаленно услуг и товаров неуклонно ведут к коммерциализации персональных данных, а также их краже. При этом законодательство не успевает за развитием способов кражи персональных данных, что позволяет говорить о наличии пробелов в регулировании защиты персональных данных. Это также подтверждается данными о состоянии преступности в Российской Федерации за январь — ноябрь 2022 г.

Так, согласно данным МВД России, было зарегистрировано более 470 тысяч преступлений с использованием информационных технологий, при этом раскрыто менее 130 тысяч¹⁰. Соответственно, наблюдается низкая степень раскрываемости преступлений в сфере использования информационных технологий. Оборот персональных данных в сети Интернет позволяет относить посягательства на целостность такой информации к категории преступлений, совершенных посредством использования информационных технологий.

Поэтому справедливым будет указать и тот факт, что подобные преступления, а равно противоправные действия в отношении персональных данных (т.е. их кража), обладают высокой степенью латентности.

Таким образом, можно выделить следующие тенденции противоправной деятельности в отношении персональных данных:

- потерпевшие (лица, чьи персональные данные были украдены, распространены без получения соответствующего согласия) зачастую могут не знать о факте краже их персональных данных. К примеру, без должного освещения СМИ случаев утечки персональных данных крупных фирм граждане не смогут узнать о том, что их персональные данные утекли в Сеть;
- низкая степень раскрываемости киберпреступлений в отношении персональных данных, так как для органов следствия наиболее сложными и проблемными являются методы расследования таких преступлений, а также поиск виновного лица. Данные обстоятельства осложняются тем, что если кража персональных данных выступает в качестве основной задачи для преступников, то чаще формируются преступные группы или сообщества, а также используются технические средства для сокрытия цифровых следов;
- фиксация и анализ цифровых следов, которые могут обнаружить органы следствия;
- отсутствие необходимой нормативной базы для эффективного обеспечения защиты персональных данных в цифровой среде.

В рамках национального правового поля все чаще выдвигаются инициативы по установлению штрафов для компаний за утечку персональных данных. Подобная

¹⁰ Краткая характеристика состояния преступности в Российской Федерации за январь — ноябрь 2022 года // URL: <https://мвд.рф/reports/item/34307225/> (дата обращения: 18.01.2023).



инициативы высказало в декабре 2022 г. Минцифры России, однако законопроект не нашел одобрения среди субъектов бизнеса, так как штрафные санкции, предлагаемые государством, являются для них несоразмерными¹¹.

В значительной степени сложности таких инициатив связаны с критерием повторности утечек персональных данных, за которые, согласно предложениям Минцифры, предусматривается более жесткая юридическая ответственность, так как уже после первой утечки персональных данных информация о пользователях будет храниться в цифровой среде, что не позволяет корректно определить, был ли факт повторной утечки или же распространение персональных данных основано на первой зафиксированной утечке.

Однако все же российское законодательство модернизируется с учетом современных реалий. В Федеральном законе от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон “О персональных данных”» закреплены положения о необходимости получения согласия на обработку персональных данных отдельно от иных согласий, которые могут запрашиваться со стороны компании, а также необходимость указания в данном согласии пункта о том, что лицо, соглашаясь с условиями, также согласно на распространение персональных данных. Без такого условия оператор персональных данных не обладает правом на распространение персональных данных¹².

Основная проблема данного нововведения заключается в том, что указанные положения не имеют обратной силы, соответственно, даже при условии отзыва согласия на обработку и распространение персональных данных полученные ранее оператором персональные данные уже находятся в базе, а следовательно, могут выступать предметом преступных посягательств. Также отсутствуют и сам механизм, и требования для отзыва согласия на прекращение использования и распространения персональных данных.

Помимо этого, в сентябре 2022 г. также вступили в силу поправки, которые направлены на усиление системы защиты персональных данных путем закрепления обязанности оператора персональных данных сообщать уполномоченным органам об утечках персональных данных в течение суток, а в течение трех суток — о результатах внутренней проверки факта утечки персональных данных.

В современных условиях повышенных киберрисков национальное законодательство также пытается на них реагировать. Так, было принято постановление Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан»¹³. Данный акт устанавливает следующие ситуации запрета трансграничной передачи персональных данных:

¹¹ Минцифры задумало ввести штрафы за утечки данных до 500 млн рублей // URL: https://www.rbc.ru/technology_and_media/26/12/2022/63a8f2999a79471e4e7c3968?ysclid=ld7atg60px644919802 (дата обращения: 19.01.2023).

¹² Российская газета. 11.01.2021. № 1.

¹³ URL: <http://publication.pravo.gov.ru/document/view/0001202301170011> (дата обращения: 20.01.2023).

- если органами власти иной юрисдикции не принимаются меры по защите передаваемых персональных данных;
- юридическое лицо, которое относится к иной юрисдикции, входит в список запрещенных на территории России организаций;
- юридическое лицо иной юрисдикции относится к категории нежелательных организаций на территории России;
- трансграничная передача персональных данных не соответствует целям их сбора.

Что касается цифрового пространства, то в Российской Федерации имеется соответствующая нормативная основа для обеспечения защиты персональных данных в сети Интернет. Так, защита лиц от мошеннических действий в Интернете реализуется в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ (далее — Закон об информации)¹⁴. Данный акт не только раскрывает понятие информационно-телекоммуникационной сети (т.е. сети Интернет), но и регулирует вопросы системы сертификации, разработки программ по защите информации, а также внедрения усовершенствованных систем аутентификации пользователей на различных сервисах.

Однако указанные акты — Закон о персональных данных и Закон об информации не формируют необходимой и совершенной системы защиты, которая отвечала бы требованиям развития самих информационных технологий (в том числе в контексте развития средств и способов воздействия со стороны злоумышленников на персональные данные), а также требованиям полной информационной безопасности каждого пользователя. В этой связи справедливым является мнение, согласно которому разработка инновационных методов защиты — это наиболее приоритетное направление развития для всего мира¹⁵.

В современных условиях существует несколько моделей реализации умысла по краже персональных данных:

- 1) социальная инженерия. Чаще всего социальная инженерия реализуется в форме фишинга, когда злоумышленник представляется доверенным лицом и путем обмана (в том числе создания поддельных сайтов, рассылки) осуществляет кражу данных непосредственно у лица (субъекта персональных данных). Наиболее распространена в составах мошенничества;
- 2) использование ненадежных способов защиты персональных данных. В данном случае можно говорить не только о фактах пробелов в системе информационной безопасности компании, но и об использовании ненадежных способов защиты самим клиентом (например, использование простых паролей и др.), что может быть обусловлено низким качеством информационно-просветительской работы по вопросам защиты персональных данных;

¹⁴ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Российская газета. 29.07.2006. № 165.

¹⁵ Шарыпова Т. Н., Пунга К. В. Интернет-мошенничество: защита персональных данных от фишинга // Modern Science. 2022. № 5–3. С. 216.



- 3) использование для обработки персональных данных технологий искусственного интеллекта¹⁶. Это позволяет быстрее и эффективнее осуществлять обработку персональных данных, но при этом искусственный интеллект также создает повышенную уязвимость системы;
- 4) кадровые риски. Данная модель реализуется посредством использования должностным лицом своих полномочий по доступу к базе персональных данных и их последующей кражи.

Относительно последней модели реализации умысла по краже персональных данных необходимо отметить, что в практике российских судов нередко встречаются споры, касающиеся того, что должностное лицо информационной компании или компании по предоставлению связи, имея, согласно своим должностным полномочиям, доступ к персональным данным пользователей, осуществляет воздействие на эти данные, кражу или же использует эти данные без получения соответствующего согласия со стороны граждан¹⁷.

Соответственно, формирование системы защиты персональных данных в первую очередь должно обеспечиваться посредством внутренних механизмов защиты (например, использования высокотехнологичного программного обеспечения, создания внутренних должностных инструкций, стандартов). Такие внутренние меры по защите персональных данных должны коррелироваться с правовыми основами, которые также закрепляют стандарты для обеспечения эффективной защиты персональных данных в цифровой среде.

В контексте формирования в России эффективной правовой среды для защиты персональных данных, а также учета сущностных характеристик цифрового пространства (трансграничность и отсутствие возможности для установления юрисдикции в отношении сети Интернет), интересно рассмотрение зарубежного опыта защиты персональных данных. На данном уровне регулирования имеются достаточно интересные практики по защите персональных данных в Европейском союзе во взаимосвязи с Международным союзом электросвязи (МСЭ).

В ЕС был принят регламент GDPR, целью которого является укрепление прав субъектов персональных данных¹⁸. Данный акт предполагает установление ответственности за несоблюдение правил хранения и обработки персональных данных, раскрывает терминологическую основу — понятия персональных данных, обработки персональных данных, ограничения персональных данных, контроллера, процессора персональных данных.

¹⁶ Минбалеев А. В., Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. Серия : Право. 2020. Т. 20. № 3. С. 89.

¹⁷ См., например: приговоры Советского районного суда г. Владивостока № 1-277/2020 от 30.07.2020 по делу № 1-277/2020 // URL: <https://sudact.ru/regular/doc/4AyuDmz7J9oX/?ysclid=Id7r658k9780709119> ; Октябрьского городского суда № 1-243/2020 от 29.07.2020 по делу № 1-243/2020 // URL: <https://sudact.ru/regular/doc/eLKpELsMEF5w/?ysclid=Id7r7grw9p48969269> ; Шиманского районного суда № 1-2/2019 1-2/2020 1-30/2018 от 05.11.2020 по делу № 1-2/2019 // URL: <https://sudact.ru/regular/doc/r4h59Cvexoln/?ysclid=Id7r88hq5t802523738> (дата обращения: 20.01.2023).

¹⁸ URL: <https://gdpr.eu> (дата обращения: 20.01.2023).

Сравнивая данные положения с национальным законодательством, хочется отметить, что законодательство ЕС более детально раскрывает субъектный состав при обороте персональных данных. Более того, регламент GDPR закрепляет такие основополагающие принципы для сферы обработки персональных данных, как законность, справедливость и прозрачность, сбор и обработка для законных целей, адекватность и релевантность персональных данных целям обработки, хранение персональных данных в соответствующей форме.

Принципы, закрепленные GDPR, не являются абстрактными, а приближены к реальным и практическим условиям. Интересным подходом ЕС является установление такой правовой категории, как «право на забвение», т.е. возможность удаления данных пользователя из поисковой выдачи по требованию субъекта персональных данных, в том числе путем отзыва согласия на обработку персональных данных.

В рамках ЕС различаются понятия сбора и использования персональных данных. Если обращаться к практике МСЭ, то можно отметить, что в первую очередь организация ориентируется на стандартизацию и выдачу рекомендаций относительно защиты персональных данных, а также применения законодательства, в том числе GDPR.

В зарубежных странах защита персональных данных в значительной степени реализуется на внутреннем уровне — посредством предоставления пользователям пользовательских соглашений, в которых указываются права и обязанности сторон¹⁹. Более того, на многих интернет-платформах (в том числе в социальных сетях) реализуются собственные программы по защите пользователей от кражи персональных данных (Facebook, YouTube, различные поисковые системы и браузеры). Представляется, что некоторая степень саморегулирования в контексте защиты персональных данных пользователей имеет место, так как основная задача информационных порталов и платформ — это предоставление защищенной системы, которая функционирует на законодательных стандартах обеспечения безопасности пользовательских данных.

Логичным является вопрос определения правовой и функциональной возможности создания условий для «абсолютной» защиты персональных данных. Теоретически эта возможность может быть реализована только при условии, что существуют технические способы такой защиты²⁰. Однако представляется, что все же невозможно реализовать эффективную и постоянную систему защиты — и техническим организациям (разработчикам софта, ПО), и законодателю необходимо будет реагировать на любые технические изменения, в том числе на механизмы и способы воздействия со стороны преступников на информацию. Более того, трансграничность сети Интернет предполагает установление общих международных стандартов для формирования систем защиты персональных данных, что на сегодняшний день труднореализуемо.

¹⁹ Гонтарь Л. О. Защита персональных данных в условиях развития интернет-компаний: международно-правовое регулирование vs саморегулирование // Труды по интеллектуальной собственности. 2021. Т. 37. № 1–2. С. 134.

²⁰ Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3.



Таким образом, подводя итог, можно сказать, что проблема защиты персональных данных является одной из наиболее актуальных в современных условиях. Для России ее актуальность связана с увеличением количества преступных воздействий на персональные данные, отсутствием необходимого уровня технологической независимости, что неоднократно отмечалось на протяжении 2022 г. Центральным банком РФ, а также со сложностями в разработке отечественного программного обеспечения и технологий после ухода с российского рынка большинства иностранных компаний, в том числе информационных и технологических.

Предполагается, что формирование системы защиты персональных данных в цифровой среде должно осуществляться на двух уровнях: государственном (путем принятия нормативных правовых актов) и на уровне организаций. При этом его должен сопровождать следующий комплекс мер:

- 1) реализация государством просветительской функции в части защиты персональных данных²¹ в целях ознакомления граждан с положениями законодательства, основными рисками утечки персональных данных и способами самостоятельной защиты своих персональных данных;
- 2) развитие частных инициатив по защите персональных данных, что прямо коррелируется с необходимостью построения независимой экономики и технологической независимости в России. Это также предполагает и применение дополнительных мер — налоговых, административных для снижения давления на субъекты, занимающиеся разработкой программного обеспечения и информационных систем для защиты персональных данных пользователей;
- 3) формирование внутренних должностных инструкций и стандартов, а также проведение просветительских мероприятий относительно юридической ответственности за нарушения уголовного и административного законодательства в отношении персональных данных с использованием своего должностного положения;
- 4) формирование способов и механизмов внесудебной защиты персональных данных в случае обнаружения утечек;
- 5) уведомление граждан о факте утечек, что дополняло бы обязанность операторов персональных данных сообщать уполномоченным органам о факте утечки персональных данных;
- 6) формирование системы внешнего расследования случаев утечки персональных данных.

²¹ Герасимова Н. А. Проблемы защиты персональных данных в сети Интернет // Актуальные проблемы науки и практики : Гатчинские чтения — 2020 : сборник научных трудов по материалам VII Международной научно-практической конференции. Гатчина, 22 мая 2020 г. Гатчина : Государственный институт экономики, финансов, права и технологий, 2020. Т. 2. С. 80.

БИБЛИОГРАФИЯ

1. *Абрамова А. Г.* Международно-правовая защита персональных данных в сети Интернет: общие положения // Регион и мир. — 2020. — Т. 11. — № 5. — С. 51—58.
2. *Бачило И. Л.* Информационное право : учебник для магистров. — 3-е изд., перераб. и доп. — М. : Юрайт, 2015. — 564 с.
3. *Герасимова Н. А.* Проблемы защиты персональных данных в сети Интернет // Актуальные проблемы науки и практики : Гатчинские чтения — 2020 : сборник научных трудов по материалам VII Международной научно-практической конференции. Гатчина, 22 мая 2020 г. — Гатчина : Государственный институт экономики, финансов, права и технологий, 2020. — Т. 2. — С. 78—80.
4. *Гонтарь Л. О.* Защита персональных данных в условиях развития интернет-компаний: международно-правовое регулирование vs саморегулирование // Труды по интеллектуальной собственности. — 2021. — Т. 37. — № 1–2. — С. 116—140.
5. *Дмитриева Е. Г.* Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. — 2021. — № 3.
6. *Минбалева А. В., Филоненкова В. А.* Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2020. — Т. 20. — № 3. — С. 89—94.
7. *Сибел Т.* Цифровая трансформация. Как выжить и преуспеть в новую эпоху. — М. : Манн, Иванов и Фербер, 2021.
8. *Сычева М. И.* Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. — 2022. — № 10–3 (73). — С. 175—178.
9. *Шарыпова Т. Н., Пунга К. В.* Интернет-мошенничество: защита персональных данных от фишинга // Modern Science. — 2022. — № 5–3.

