

*Веренчиков И. Р., Серода А. Е.*

## **СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРАВОВОЙ ОХРАНЫ ИЗОБРАЖЕНИЯ ЛИЦА В КНР И РЕСПУБЛИКЕ БЕЛАРУСЬ В КОНТЕКСТЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ**

Белорусский государственный университет,  
пр. Независимости, 4, 220030, г. Минск, Беларусь, *lawcrim@bsu.by*

В статье рассматривается законодательный аспект правовой охраны изображения лиц в КНР и Республике Беларусь. Авторы осуществляют сравнительный анализ выявленных правовых особенностей и предлагают некоторые пути решения обозначенных проблем. Установлено, что отсутствуют программы обучения и критерии квалификации специалистов в области систем автоматического распознавания лиц. Акцентируется возможность разработки в Республике Беларусь стандартов применения, обеспечения безопасности персональных данных и подготовки специалистов в области распознавания лиц.

**Ключевые слова:** распознавание лиц; технологии; идентификация; верификация; персональные данные; информационная безопасность; искусственный интеллект.

В эпоху быстрого расширения технологических горизонтов научной мысли, биометрическая технология распознавания, идентифицирующая и верифицирующая личность человека по его лицу, становится ярким объектом внимания общественности, представляя собой некий рупор прогресса, неизменнодвигающегося по возрастающей в области компьютеризации и цифровизации современного бытия человека. Будущее технологий, как и людей, неразрывно связано с организационно-правовым обеспечением данных изобретений, разработанных и предложенных для имплементации в духе соблюдения чести и достоинства индивида в правовом государстве, а также в соответствии с этическими принципами ценности свободы и творческой мысли человека.

Процессы глобализации и мировой мобильности позволяют в значительной степени ускорить международный обмен знаниями, опытом и технологиями, в некоторой степени открывая двери для взаимного проникновения культур; таким образом зародившееся более 50 лет назад направление компьютерного зрения и статистического анализа образов внешности человека приобрело значимое присутствие во всем цивилизованном мире. По состоянию на 2024 год, значительный вклад в дальнейшее развитие и распространение технологии был внесен Китайской Народной Республикой (далее – КНР), где в промышленных масштабах осуществляется производство, а также реализация данных

технологий для нужд частного и государственного секторов соответственно.

Китайский сектор информатики демонстрирует впечатляющий рост и развитие, с множеством частных компаний, занимающихся разработкой технологий в этой области: китайская индустрия распознавания лиц находится в эпицентре этого «цифрового шторма». Известные на международном уровне компании, осуществляющие разработку и реализацию систем автоматического распознавания лиц, включают следующие: «Huawei», «Hikvision», «Dahua Technology», «ZTE» и др. [1, с. 65] Среди наиболее значимых достижений КНР в области распознавания лиц, а также многообещающих примеров научных исследований и успешной имплементации продукции, следует указать такие как:

1) система социального кредита, получившая широкую огласку и которая предполагает интеграцию технологий распознавания лиц с другими методами сбора данных для создания всеобъемлющей базы учета активности граждан. Технология распознавания лиц является ключевым элементом данной системы, поскольку она обеспечивает идентификацию индивидуумов в общественных местах и позволяет собирать данные о их действиях [1, с. 140];

2) разработка систем автоматического распознавания эмоций: внедрение технологий распознавания лиц становится все более распространенным явлением. Например, компания «Canon» в КНР установили камеры видеонаблюдения с функцией «распознавания улыбок», что позволяет фиксировать эмоциональное состояние сотрудников [1, с. 92];

3) разработка систем, устанавливающих намерения человека: одна из китайских компаний утверждает, что ей удалось создать систему, способную анализировать выражения лиц потенциальных заемщиков с целью определения их намерений относительно погашения кредита [1, с. 152];

4) системы для анализа жестов и обнаружения особенностей скелета: одним из ведущих компаний является китайское предприятие «MEGVII» с ее продуктом «Face++», охватывающим различные уровни сложности и точности: стандартные алгоритмы используют 106 точек на лице для базовой идентификации, тогда как продвинутые версии могут использовать до 1000. «MEGVII» развивает технологии распознавания человеческого тела, включая системы для анализа жестов и скелета человека [1, с. 66];

5) исследование возможности распознавания в области сельского хозяйства: «Huawei» занимает ведущие позиции в разработке коммерческого внедрения распознавания лиц в сельском хозяйстве – включая мониторинг и идентификацию отдельных животных [1, с. 66].

Известные мировой общественности примеры имплементации распознавания лиц в КНР включают:

- использование распознавания лиц для поиска пропавших без вести людей. В рамках первого пробного применения обозначенных технологий для этой цели были найдены и идентифицированы более 6500 людей в результате сканирования около 200000 лиц без определенного места жительства [1, с. 81];

- для поддержания общественного порядка используется система распознавания лиц «Dragonfly Eye». В первые три месяца задействия данной технологии в городе Шанхай правоохранители задержали 567 нарушителей, и уровень карманных краж в городах, где она была имплементирована, упал практически на треть. Полиция города Чжэнчжоу, например, используют очки с системой распознавания лиц, выдающие имя и адрес человека за 2-3 минуты [2, с. 734];

- силовые структуры в ряде крупных городов Западного Китая используют распознавание лиц для идентификации этнической принадлежности человека – в данном случае распознавание лиц применяется как инструмент для систематического наблюдения, что включает в себя сбор биометрических данных и отслеживание местоположения [1, с. 116];

- использование в исправительных учреждениях камер видеонаблюдения и системы распознавания лиц для постоянного мониторинга заключенных не только с целью идентификации лиц, но и анализа поведения для выявления подозрительных действий [1, с. 116];

- розничные компании в Китае, такие как «Jack & Jones» и «Vero Moda», внедряют технологии распознавания лиц для замещения стандартных процедур процесса оплаты (банковские карты, наличные деньги). Участники сообщества в мессенджере «WeChat» (аналог «Viber» в Беларуси) «AI Club WeChat» могут оплачивать покупки посредством распознавания лиц [1, с. 87];

- в условиях пандемии COVID-19 технологии распознавания лиц стали активно разрабатываться для выявления и идентификации граждан, которые не носят маски (а также тех, кто их носит для сокрытия личности), что позволяет реагировать на потенциальные угрозы общественному здоровью [1, с. 143].

Таким образом, явным становятся направления развития и имплементации технологий распознавания лиц в общественной жизни КНР. Законодательство в данной области также имеет свои характерные особенности – например, в настоящее время правовые нормы, касающиеся защиты персональных данных в виде изображений лиц граждан в рамках распознавания лиц в КНР, характеризуются неоднозначностью; кроме того, наблюдается отсутствие специализированного правового регулирования охраны персональных данных в области распознавания лиц. С целью

обоснования вышесказанного следует обратиться к нижеперечисленным нормативным правовым актам [3, с. 273]:

1. Закон КНР от 20 августа 2021 г. «О защите персональных данных». Согласно ст. 26, «установка оборудования для сбора изображения лица и идентификации личности в общественных местах должна быть необходима для поддержания общественной безопасности, соответствовать соответствующим государственным нормам и устанавливать заметные предупреждающие знаки».

2. Закон КНР от 31.10.1993 г. № 11 «О защите прав потребителей» закрепляет права и обязанности операторов по сбору, обработке и использованию персональных данных потребителей. Поскольку информация о изображении лица относится к «чувствительным персональным данным», её сбор, обработка и использование должны осуществляться с согласия субъекта.

3. Закон КНР от 07.11.2016 г. № 53 «О сетевой безопасности» включает персональные данные в качестве объекта защиты, а также устанавливает в ст. 40-50 принципы сбора персональных данных: порядок сбора, хранения и использования персональных данных, право пользователя на распоряжение персональными данными и обязанности оператора по сбору и обработке персональных данных.

4. Гражданский кодекс КНР от 28.05.2020 г. (далее – ГК КНР) содержит положения о защите персональных данных в разделе «личные права» (ст. 1034-1039), включая биометрические данные как вид персональных данных. В ГК КНР также уточнены принципы законности, необходимости и обоснованности, принципы информированного согласия и принципы ограничения передачи при обработке персональных данных, что создает базу механизма гражданской правовой защиты персональных данных.

Поправки к Уголовному кодексу КНР от 28.02.2009 впервые квалифицировали незаконное приобретение, продажу и предоставление персональных данных граждан как преступление, установив, однако, субъектом только сотрудников государственных органов или специальных подразделений. Последующие поправки от 29.08.2015, введя ст. 253-1, расширили субъектный состав до общего субъекта, при этом специальный статус стал отягчающим обстоятельством для совершения данного преступления [3, с. 275].

1 июня 2017 г. Судебный комитет Верховного народного суда и Прокурорский комитет Верховной народной прокуратуры КНР опубликовали Разъяснение, касающееся применения законодательства при рассмотрении уголовных дел, связанных с нарушением персональных данных граждан. Документ состоит из десяти статей, которые определяют [3, с. 275]: объем персональных данных граждан, подлежащих уголовно-правовой защите; критерии для осуждения за преступления с

персональными данными граждан; обстоятельства, смягчающие или отягчающие ответственность; вопросы конкуренции составов преступлений, связанных с нарушением персональных данных.

Исходя из этого, данное Разъяснение устанавливает основные параметры уголовно-правовой охраны персональных данных, определяя ее пределы, условия наступления ответственности и влияние квалифицирующих признаков. Это способствует единообразному применению законодательства судами и органами прокуратуры в данной сфере.

В 2021 г. судебный комитет Верховного народного суда КНР опубликовал Разъяснение, касающееся применения законодательства в контексте гражданских дел, связанных с использованием технологий распознавания лиц при обработке персональных данных:

- ст. 14 устанавливает правовые аспекты подачи гражданских исков, касающихся информации о изображении лица;

- ст. 5 устанавливает случаи, когда обработчик информации освобождается от гражданской ответственности. В частности, это касается ситуаций, когда обработка данных о лицах осуществляется в целях реагирования на чрезвычайные ситуации в области здравоохранения или для защиты жизни, здоровья и имущества граждан в условиях кризиса [3, с. 274];

- ст. 2 определяет несколько типов действий, которые нарушают права физических лиц, включая использование технологии распознавания лиц для идентификации в общественных местах, таких как гостиницы и торговые центры, без надлежащего согласия.

С 2012 г. в КНР государственные органы начали активно заниматься стандартизацией в области защиты персональных данных. Национальный технический комитет по стандартизации информационной безопасности разработал и опубликовал «Руководство по государственному стандарту № GB/Z 28828-2012», которое посвящено защите персональных данных в информационных системах государственных и коммерческих служб с использованием технологий информационной безопасности – это руководство стало первым Национальным стандартом в данной области [3, с. 276].

В 2020 г. была опубликована обновленная версия Руководства по государственному стандарту № GB/T 35273-2020 «Технология информационной безопасности – спецификации безопасности персональных данных» (далее – Руководство № GB/T 35273-2020), касающаяся технологий информационной безопасности и спецификаций безопасности персональных данных [3, с. 278]. Данный стандарт устанавливает принципы и требования безопасности, которые должны соблюдаться при обработке персональных данных. Он применяется к

различным организациям и регулирует их деятельность в области обработки персональных данных, включая надзор и оценку со стороны компетентных органов. Руководство № GB/T 35273-2020 впервые различает «персональные данные» и «чувствительные персональные данные» – информация, обработка которой может представлять повышенный риск для безопасности личности или имущества, а также может негативно сказаться на репутации, психическом и физическом здоровье и др.

На основании вышеперечисленного следует сделать вывод, что в настоящее время нормы о защите информации распознавания лиц в Китае относительно разрозненны. Они существуют в законах, постановлениях, ведомственных инструкциях, судебных толкованиях и иных нормативных документах. Отсутствует соответствующее специальное регулирование, нет четко детерминированных положений в законодательстве. Подобный исход законодательного развития в области охраны персональных данных требует исправления ситуации разработки правовых норм для защиты биометрической информации и унификации стандартов правоприменения в сфере защиты персональных данных в распознавании лиц граждан [3, с. 276].

В данной связи, перенимая технологии и ассимилируя новаторские идеи в отношении многочисленных проектов в области биометрии, законодателю в Республике Беларусь нужно также обращать внимание и на проблемные аспекты организационно-правового регулирования данной области у более технологически развитого партнера: с целью внесения конструктивных предложений и обоснованных замечаний, следует осуществить детальное исследование аспектов генезиса и становления правовой охраны изображения лица человека (т.е. персональных данных) в Республике Беларусь.

Представляет интерес тот факт, что первоначально данная сфера не была предметом специального правового регулирования – такой вывод позволяет сделать ретроспективное исследование нормативно-правовых актов, регулирующих общественные отношения, связанные с обработкой персональных данных в Республике Беларусь. Т.е. правовое регулирование в Беларуси осуществлялось нормативными правовыми актами, которые устанавливали общие принципы и нормы, применимые к более широкому кругу общественных отношений, нежели складывающиеся по поводу обработки персональных данных. К ним следует относить Конституцию Республики Беларусь, Закон Республики Беларусь от 10 ноября 2008 г. №455-3 «Об информации, информатизации и защите информации», Закон Республики Беларусь от 21 июля 2008 г. №418-Э «О регистре населения», Закон Республики Беларусь от 15 июля 2015 г. №307-3 «Об оперативно-розыскной деятельности», Уголовный Кодекс Республики Беларусь

(далее – УК), Кодекс об административных правонарушениях Республики Беларусь (далее – КоАП) и др.

В частности, согласно ст. 28 Конституции Республики Беларусь, каждый гражданин имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. В соответствии со ст. 18 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с письменного согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь.

В Законе Республики Беларусь от 21 июля 2008 г. №418-З «О регистре населения» впервые появилось понятие «персональные данные». Персональные данные физических лиц определялись как совокупность основных и дополнительных персональных данных, а также данных о реквизитах документов, подтверждающих основные и дополнительные персональные данные конкретных физических лиц. Среди прочего, к персональным данным обозначенный Закон относил и цифровой фотопортрет. Из этого следует, что различные образы, с которыми работали системы распознавания лиц в Республике Беларусь следовало первоначально обозначать как «информация о личной жизни человека» [4].

В 2010-х гг. широкое внедрение биометрических систем, рост Интернет-технологий и появление искусственного интеллекта на международной арене значительно увеличили потребность в упорядочивании законодательства, касающегося общественных отношений, возникающих в результате сбора, обработки и хранения идентифицирующей информации о человеке. Эти изменения обусловили необходимость адаптации правовых норм к новым вызовам, связанным с защитой персональных данных и обеспечением прав граждан в условиях активного использования биометрических технологий.

Следующим шагом стало то, что в Закон «Об информации, информатизации и защите информации» 4 января 2014 г. было включено дополнение, в котором впервые предпринята попытка дать универсальное определение персональных данных. Под персональными данными было предложено понимать основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. В 2018 г. статья 22.13 КоАП претерпела изменения, в соответствии с которыми установлена ответственность за умышленное незаконное разглашение персональных данных лицом,

которому персональные данные известны в связи с его профессиональной или служебной деятельностью [4].

Нельзя не обратить внимание и на положения УК и КоАП. КоАП, принятый в 2021 г., предусмотрел самостоятельную статью (ст. 23.7), устанавливающую ответственность за нарушение законодательства о персональных данных. В 2021 г. УК дополнен двумя самостоятельными составами, предусматривающими ответственность за незаконные действия в отношении персональных данных и за несоблюдение мер обеспечения их защиты.

Постепенное «насыщение» законодательства отдельными нормами о персональных данных, а также разрозненный характер имеющегося регулирования привели к необходимости упорядочения получившегося «нормативного массива», что привело к принятию Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных». Действительно, определение достаточно четко и однозначно охватывало суть персональных данных: «под персональными данными следует понимать «любую информацию, относящуюся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано» [4].

Дифференциация понятий «персональные данные» и «информация о личной жизни человека» внесла значительный вклад в правовое обеспечение работы биометрических систем. Не в последнюю очередь это связано с тем, что понятие «персональные данные» имеет составной характер своей конструкции – Закон от 7 мая 2021 г. № 99-З «О защите персональных данных» выделяет такие понятия как «биометрические персональные данные», «специальные персональные данные» и др., что позволяет учитывать их различия в фиксации, обработке, хранению и использованию [4].

Помимо законодательно закрепленных процедур сбора, обработки и хранения персональных данных, правовое регулирование систем автоматического распознавания лиц включает формирование и правовое обеспечение функционирования Республиканской системы мониторинга общественной безопасности (далее – РСМОБ): на основании ретроспективного анализа соответствующих нормативных правовых актов, можно утверждать, что в Республике Беларусь с 2012 г. велась работа по созданию единой системы видеонаблюдения, а с 2013 г. началось ее испытательное внедрение. Высокое значение для ее имплементации в Республике Беларусь следует отнести: 1) Постановлению Совета Министров Республики Беларусь от 11 декабря 2012 г. № 1135 «Об утверждении Положения о применении систем безопасности и телевизионных систем наблюдения»; 2) Указу Президента Республики Беларусь от 28 ноября 2013 г. № 527 «О вопросах создания и применения

системы видеонаблюдения в интересах обеспечения общественного порядка» и др. [5, с. 254]. В названном Постановлении от 11 декабря 2012 г. № 1135 впервые были закреплены термины «система безопасности», «телевизионная система видеонаблюдения», «обеспечение общественной безопасности», «общественная безопасность» и даны их определения [6, с. 6].

Значительным шагом к правовому регулированию систем видеонаблюдения и, впоследствии, распознавания лиц, стали следующие Постановления Совета Министров Республики Беларусь: Постановление Совета Министров Республики Беларусь от 30 декабря 2013 г. № 1163 «Об утверждении Положения о порядке предоставления информации, зафиксированной системой видеонаблюдения за состоянием общественной безопасности, и определения размера платы за ее предоставление»; Постановление Совета Министров Республики Беларусь от 31 января 2014 г. № 89 «Об утверждении перечня мест массового пребывания граждан в г. Минске, подлежащих оборудованию средствами системы видеонаблюдения за состоянием общественной безопасности».

Внедрение видеонаблюдения в остальных административно-территориальных единицах потребовало дальнейшего совершенствования нормативного правового регулирования. Важным событием для становления РСМОБ послужило принятие Указа Президента Республики Беларусь от 25 мая 2017 г. №187 «О Республиканской системе мониторинга общественной безопасности», согласно которому, для повышения уровня общественной безопасности вводится система видеонаблюдения, оснащенная каналами связи единой сети передачи данных. В свою очередь на основании этого нормативного правового акта, впоследствии Постановлением Совета Министров Республики Беларусь от 10 ноября 2017 г. № 841 было разработано и утверждено Положение «О Республиканской системе мониторинга общественной безопасности и порядке подключения к ней» [5, с. 255].

Указ Президента Республики Беларусь от 25 мая 2017 г. № 187 включил в себя закрепленные в ранее принятых нормативных правовых актах подходы к обеспечению общественной безопасности с использованием видеонаблюдения. В нем определены правовые основы функционирования РСМОБ, а также порядок подключения к ней, как в обязательном порядке, так и по желанию различных субъектов права. Кроме этого, расширен и детализирован перечень задач, решаемых РСМОБ.

Согласно ч. 12 Постановления Министерства внутренних дел Республики Беларусь от 2 июля 2019 г. №181 «О единых технических требованиях к программному обеспечению видеоаналитики», в части функциональных возможностей технического решения применяемой системы обеспечения общественной безопасности указывается: 1) поиск

похожих людей как по фотографии из базы данных, так и по фотографии, полученной с камеры видеонаблюдения; 2) настройку порога степени схожести изображения распознанных лиц с эталонными фотографиями из базы данных; 3) импорт фотографий в базу данных и экспорт фотографий распознанных лиц во внешние базы данных; 4) интеграцию со сторонними информационными системами и базами данных, содержащими фотографии людей и др.

В соответствии с Решением Минского городского исполнительного комитета от 29 июля 2021 г. №2268 «О перечне объектов, подлежащих обязательному оборудованию средствами системы видеонаблюдения», обязательному оборудованию подлежат с 2021 г. 1090 объектов. Указом Президента Республики Беларусь от 25 февраля 2022 г. №69 «О развитии Республиканской системы мониторинга общественной безопасности» предусмотрено интегрирование в РСМОБ специальных технических средств, работающих в автоматическом режиме, предназначенных для фиксации в том числе административных правонарушений [5, с. 257].

Немаловажное значение для работы с персональными данными в Республике Беларусь имеет Указ Президента Республики Беларусь от 28 октября 2021 г. №422 «О мерах по совершенствованию защиты персональных данных», в соответствии с которым был создан Национальный центр защиты персональных данных Республики Беларусь, учредителем которого является Оперативно-аналитический центр при Президенте Республики Беларусь. К основным задачам Национального центра относятся: 1) принятие мер по защите прав субъектов персональных данных при обработке персональных данных; 2) организация обучения по вопросам защиты персональных данных. К основным его функциям, согласно Положению, относится осуществление контроля за обработкой персональных данных операторами (т.е. уполномоченными лицами) [5, с. 258].

Таким образом, следует отметить, что в КНР, как и в Республике Беларусь, отсутствует специализированное законодательство, регулирующее защиту информации, связанной с распознаванием лиц, что потенциально приводит к разрозненности норм, содержащихся в различных законах, постановлениях и нормативных актах (как было представлено на примере КНР). Исходя из этого, следует поставить вопрос о необходимости разработки специального нормативного правового акта, регулирующего применение систем автоматического распознавания лиц в Республике Беларусь, что будет являться значительным шагом в области организационно-правового обеспечения распознавания лиц при расследовании преступлений: данный нормативный правовой акт должен предусматривать определение понятий, связанных с системами автоматического распознавания лиц, указывать условия их применения, а

также меры, принимаемые для обработки персональных данных в условиях соблюдения белорусского законодательства.

В значительной степени интерес вызывают процессы стандартизации безопасности применения технологий, работающих в сфере биометрических персональных данных – как в случае с Руководства по государственному стандарту № GB/T 35273-2020 «Технология информационной безопасности – Спецификации безопасности персональных данных» в КНР. В данной связи, представляется что разработка в Республике Беларусь специальных стандартов в области: 1) применения; 2) обеспечения безопасности данных; 3) подготовки специалистов для работы с системами биометрической идентификации заметно систематизирует и регламентирует работу систем распознавания лиц и обработку персональных данных в работе с ними.

Практически полностью отсутствуют требования к квалификации сотрудников, работающим с системами автоматического распознавания лиц, что, на наш взгляд, является значительным упущением ввиду характерных особенностей применения обозначенных технологий. Ввиду многогранности и многоуровневости аппаратно-программных аспектов работы систем распознавания лиц, а также обширного рода ситуаций, возникающих в процессе их функционирования, следует обозначить минимальные критерии понимания принципов работы подобных технологий и обучать будущих специалистов в соответствии с разработанными для этой цели квалификационными программами.

В заключение следует отметить, что в результате проведенного анализа было выявлено как преимущественное положение развития Республики Беларусь по отношению к КНР в области распознавания лиц, так и недостающие элементы нашего законодательства. В большинстве же своем, законодательство Республики Беларусь характеризуется большей четкостью формулировок и направлено на обеспечение контроля со стороны государства за деятельностью операторов персональных данных.

### **Библиографический список**

1. Andrejevic, M. Facial Recognition / M. Andrejevic, N. Selwyn. – Polity Press, Cambridge, 2022. – 217 p.

2. Веренчиков, И. Р. Особенности криминалистического распознавания лиц: проблемы и перспективы / И. Р. Веренчиков, А. Е. Середа // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: Н.А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2022. – Вып.17. – С. 733-742.

3. Цзя, Ш. Правовая защита гражданина на изображение лица при применении технологии распознавания лиц в законодательстве Китая / Ш. Цзя, Ц. Чжан // Правоведение, 2024. – №2. – С.271–283.

4. Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» [Электронный ресурс]. – Режим доступа: <https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/>. – Дата доступа: 18.09.2024.

5. Луговский, С. Г. Правовое регулирование Республиканской системы мониторинга общественной безопасности в условиях цифровой трансформации Республики Беларусь / С. Г. Луговский // Актуальные проблемы достижения целей устойчивого развития в условиях цифровой трансформации государства и права в Республике Беларусь : материалы Республиканской науч.-практ. конференции, Минск, 18–19 ноября 2022 г. / БГУ, Юридический фак. Каф. конституционного права ; [редкол.: Г. А. Василевич (отв. ред.) и др.]. – Минск : БГУ, 2022. – С. 253-258.

6. Гиммельрейх, О. В. Республиканская система мониторинга общественной безопасности в системе организационных средств охраны общественного порядка и безопасности / О. В. Гиммельрейх // Вестник Академии МВД Республики Беларусь. – 2020. – № 1. – С. 5-11.