М. С. Абламейко
(M. S. Ablameyko)

Р. П. Богуш
(R. P. Bogush)

УДК 340.64:343.982.32

ИНТЕЛЛЕКТУАЛЬНОЕ ВИДЕОНАБЛЮДЕНИЕ В «УМНОМ ГОРОДЕ»: КОНТРОЛЬ И ЗАЩИТА ВИЗУАЛЬНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

(INTELLIGENT VIDEO SURVEILLANCE IN «SMART CITY»: CONTROL AND PROTECTION OF VISUAL PERSONAL DATA)

В статье приводятся результаты использования систем видеонаблюдения, рассматриваются признаки, по которым обнаруживается и распознается человек. Анализируется опыт ряда стран по внедрению систем искусственного интеллекта для укрепления общественной безопасности в существующих «умных городах». Предлагается введение термина «визуальные персональные данные» и определение мер по его применению в существующем правовом поле для защиты персональных данных как со стороны оператора таких систем, так и со стороны гражданина. Излагаются предложения по развитию нормативно-правовой базы в Республике Беларусь в целях защиты прав граждан.

Ключевые слова: «умный город»; интеллектуальное видеонаблюдение; биометрические персональные данные; визуальные персональные данные; распознавание лиц; идентификация человека; информационная безопасность

Введение. Развитие технологий привело к их масштабному применению в различных сферах жизнедеятельности общества и государства. В настоящее время одной из передовых является технология «умного города», которая получила развитие во многих странах мира. «Умный город» призван в первую очередь повысить качество жизни граждан, сделать проживание в городе безопасным и комфортным. Для обеспечения реализации данных критериев используется видеонаблюдение, позволяющее осуществлять мониторинг общественной, экологической безопасности на определенной местности с оперативным реагированием на инциденты.

Некоторые исследователи полагают, что сегодня главным элементом «умного города» является автоматизированная система, основанная на анализе потоков данных от различных источников информации, которая позволяет производить обработку полученных сведений в реальном времени, осуществлять многофакторный анализ и инициировать оперативное реагирование как в режиме поддержки принятия решений с участием человека, так и в полностью автоматическом режиме [1].

Системы интеллектуального видеонаблюдения сегодня стали неотъемлемой частью «умных городов», что обусловлено широким кругом решаемых ими задач. Видеонаблюдение включает в себя обнаружение и распознавание людей, сопровождение их перемещения на видео, повторную идентификацию (реидентификацию) людей в мультикамерных системах видеонаблюдения, определение нехарактерного поведения людей [2].

В динамично развивающемся мире должен соблюдаться баланс интересов человека и государства. С технической точки зрения должна

Абламейко Мария Сергеевна, доцент кафедры конституционного права юридического факультета Белорусского государственного университета (Беларусь, 220030, г. Минск, ул. Ленинградская, 8; e-mail: m.ablameyko@mail.ru; тел./tel.: +375172095576), кандидат юридических наук, доцент

Богуш Рихард Петрович, заведующий кафедрой вычислительных систем и сетей Полоцкого государственного университета им. Евфросинии Полоцкой (Беларусь, 211440, Витебская обл., г. Новополоцк, ул. Блохина, 29; e-mail: bogushr@mail.ru), доктор технических наук, доцент

Maria S. Ablameyko, Belarusian State University (Minsk, Belarus), Ph. D. in law, Associate professor

Richard P. Bogush, Polotsk State University named after Euphrosyne of Polotsk (Novopolotsk, Belarus), Doctor of Technical Sciences, Associate Professor

быть обеспечена безопасность и непрерывность функционирования таких систем. С правовой стороны: человек должен иметь возможность защищать свое право на неприкосновенность частной жизни. Следует учитывать интересы всех сторон и предложить сбалансированные решения, содействующие распространению новых технологий и обеспечивающие их надежность и безопасность.

Технологии интеллектуального видеонаблюдения

Технологии интеллектуального наблюдения стали широко использоваться во многих городах мира. В Москве в рамках программы «Безопасный город» действует одна из крупнейших в мире сетей с распознанием лиц – более 200 тыс. камер видеонаблюдения [3]. По состоянию на 2022 год российскую технологию распознания лиц (NtechLab) признали лучшей в мире по результатам тестирования Национального института стандартов и технологий США [4].

В КНР по примерным подсчетам, на 1,46 млрд жителей страны приходится 540 млн камер видеонаблюдения, или 372,8 шт. (тут и далее – на тысячу человек). В топ-10 локаций с самой большой концентрацией камер вошли города Индаур (62,52), Хайдарабад (41,8), Дели (26,7), Ченнаи, Сингапур, Багдад, Москва (16,85), Санкт-Петербург (12,65), Лондон и Лос-Анджелес. К концу 2021 года в мире было установлено более миллиарда камер видеонаблюдения. 54% из них находятся в Китае [5].

В США используется система распознания лиц FACES, которая основана на алгоритмах, сканирующих более 30 млн изображений фотографий. По состоянию на 2022 год из 24 агентств США 18 использовали технологии распознания лиц, некоторые применяли более одной системы [6].

В Республике Беларусь в соответствии с Указом Президента Республики Беларусь от 25 мая 2017 г. № 187 «О республиканской системе мониторинга общественной безопасности» (далее – РСМОБ) функционирует система мониторинга по единым техническим стандартам, целью которой является повышение уровня общественной безопасности [7]. Она объединяет на одной платформе локальные системы видеонаблюдения, специальные детекторы, каналы связи, центр обработки данных, а также иные системы и информационные ресурсы. При этом обработка и хранение информации в системе мониторинга осуществляются посредством программной платформы и аппаратного комплекса республиканского центра обработки данных.

25 февраля 2022 г. Главой государства подписан Указ № 69 «О развитии республиканской системы мониторинга общественной безопасности», которым РУП «Белтелеком» определено как единый технический оператор, ответственный за создание и функционирование республиканской системы мониторинга общественной безопасности, а также хранение полученной информации.

При практической реализации алгоритмов обработки видео на первом шаге выполняется обнаружение объектов и их локализация или же детектирование областей-кандидатов, которые могут быть отнесены к объектам интереса [8]. Следующий этап требует вычисления признаков выделенных фрагментов (лица), на основе которых выполняется анализ и конечная их классификация.

Технология видеонаблюдения с функциями обнаружения, идентификации, отслеживания и реидентификации людей

Пространственно распределенная система видеонаблюдения состоит из территориально разнесенных IP-камер и организована на основе единого центра обработки данных.

На рисунке 1 показана упрощенная структура пространственно распределенной видеосистемы с функциями обнаружения и отслеживания людей для трех IP-камер.

На каждом кадре F^k k – номер видеокамеры. С помощью детектора выполняются обнаружение всех людей, попадающих в поле зрения камер, формирование ограничительных рамок, которые описывают прямоугольником обнаруженные фигуры для них. Эти изображения людей размещаются в галерее, и для каждого из них с помощью сверточных нейронных сетей (далее – СНС) определяются векторы СНС-признаков (СНС-дескрипторы), формирующие общее пространство СНС-признаков, которое представляется в виде таблицы, где каждая строка является СНС-дескриптором для одного изображения. В каждой обнаруженной области выполняется поиск лица человека и распознавание по признакам лица.

На рисунке 1 объект $P1_{C1}^{Fk}$ покидает область наблюдения IP-камеры 1 (С1) и момент его выхода фиксируется на k-кадре видеопоследовательности, формируемой камерой С1. Данный объект переходит в область наблюдения IP-камеры 3 (С3), следовательно, необходимо применение повторной идентификации по признакам лица или по признакам изображения всей фигуры. Для другого человека $P2_{C2}^{Fk}$ данного примера необхо-

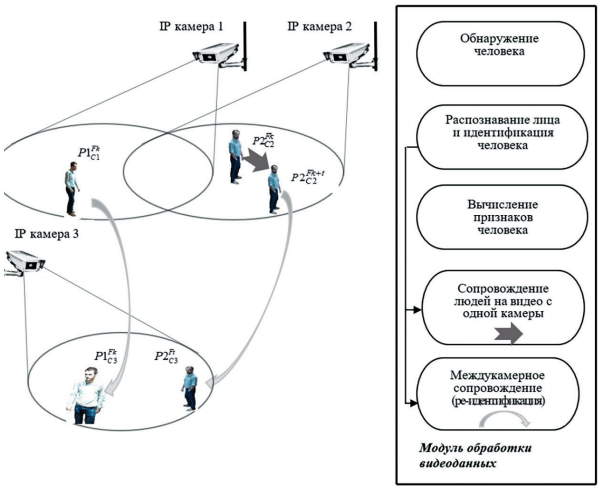

Рисунок 1. Обнаружение и анализ изображений людей в распределенной системе видеонаблюдения

димо его сопровождение в период времени *t* на видеопоследовательности, формируемой IP-камерой 2 (С2), и дальнейшая реидентификация при переходе в область наблюдения IP-камеры 3.

В системах видеонаблюдения для обнаружения и контроля передвижения людей можно выделить следующие основные задачи:

- *обнаружение* человека на видео;
- *распознавание* человека по лицу;
- *сопровождение* передвижения человека на видео, полученного с одной камеры;
- *идентификация* человека с определением всех его персональных данных;
- *повторная идентификация* людей, изображения которых получены с разных камер или с одной, но в различное время.

Первой задачей, которую необходимо решить, является обнаружение людей на изображении или видео. Мы в своих работах рассматривали такие основные методы, которые могут использоваться для обнаружения движущихся людей [9], как: межкадровой разности (frame difference); вычитания фона (background subtraction) и на основе анализа оптического потока (optical flow).

После того как человек обнаружен и выделен на изображении, необходимо выделить и распознать его лицо. Разработано и используется много алгоритмов для выделения лица человека на изображении (face detection) [10].

Распознавание лица человека по цифровому изображению – одна из ключевых задач идентификации человека. Схожей задачей является поиск местоположения человека в пространстве по его цифровой фотографии, а также его сопровождение по набору признаков, который включает, кроме признаков лица, общие признаки человека, позволяющие отследить его движение даже при невозможности распознавания лица, например, когда оно скрыто капюшоном или расположено относительно видеокамеры под значительным углом, который не позволяет выполнить идентификацию по лицу [2].

Далее следует поиск лиц в сопровождаемых областях. Выделение области поиска лица выполняется на основе анализа размеров детектированного фрагмента. Если его ширина меньше его высоты более чем в три раза, то анализируется только верхняя часть этого фрагмента, иначе анализируется вся область, описывающая человека. Для обнаружения областей, содержащих лица, применяется мультизадачная трехкаскадная СНС MTCNN [11]. Признаки лица используются для установления соответствия людей на кадрах. Это позволяет повысить эффективность сопровождения при анализе траекторий движения людей, долговременного скрытия их за объектами фона, высокой схожести внешних признаков людей.

Полученная на предыдущем шаге область кадра, содержащая лицо, поступает для распознавания. Для этого этапа применяется СНС MobileFaceNet, которая характеризуется значительно меньшими вычислительными затратами и обеспечивает при этом высокую точность работы (например, на базе данных LFW точность составляет 99,5%, а для СНС LResNet100E-IR – 99,77%) [12].

Сопровождение людей (одного или нескольких человек) – одна из наиболее актуальных задач для систем видеонаблюдения, однако в настоящее время она не решена в полной мере. На сегодняшний день наиболее результативным является сопровождение через обнаружение. Широкое развитие и применение для обнаружения объектов получили алгоритмы классификации с применением СНС, которые устойчивы к изменениям освещенности, динамическому заднему фону и позволяют осуществлять детектирование даже в случае частичных перекрытий, что повышает качество сопровождения.

Если лицо не распознано с использованием базы данных, то выполняется сравнение признаков обнаруженного лица с соответствующими данными составного дескриптора [9]. Составной дескриптор изображения каждого человека включает признаки лиц, вычисленные на основе СНС, и комплекс признаков изображения человека, что позволяет сопровождать людей даже при дальнейшей невозможности идентификации лиц.

Рисунок 2. Примеры сопровождения множества людей вне помещения

В случаях невозможности обнаружения или распознавания лиц сопровождение выполняется на основе алгоритма, включающего: оценку наличия всей фигуры человека; формирование СНС-признаков для всей области и для верхней ее части и их накопление; формирование пространственных признаков и фильтрацию по расстоянию и размерам; вычисление схожести между всеми сопровождаемыми и обнаруженными на текущем кадре людьми и установление соответствия между ними; индексацию людей; определение их видимости на кадре; выделение рамкой человека при его присутствии в кадре [9].

Тестирование выполнено по методике MOT16 [13]. Результаты показаны на рисунке 2.

Проведенные эксперименты показывают, что разработанная методика дает возможность идентифицировать человека по лицу и затем сопровождать его передвижение при сложной траектории движения.

После того как лицо человека распознано, наступает этап полной идентификации человека с установлением всех его персональных данных. Это выполняется посредством поиска лица по базам данных, имеющим изображения лиц, например, АС «Паспорт».

Биометрические персональные данные

Использование технологий интеллектуального видеонаблюдения предоставляет большие возможности для обеспечения общественной безопасности. Но могут возникнуть риски и угрозы как для человека в частности, так и для общества в целом. Распознавание человека по лицу можно использовать не только как инструмент для идентификации людей и отслеживания местоположения, но и для получения информации об их социальной активности (с кем и где они проводят время) [2]. Полиция города Чжэнчжоу, к примеру, использует очки с системой распознания лиц, выдающие имя и адрес человека за 2-3 минуты [14]. При этом если у человека есть профиль в социальных сетях (база его снимков разного возраста), то точность распознавания повышается в разы.

Проведя анализ использования систем видеонаблюдения в разных странах, можно прийти к выводу, что применять данные технологии пытаются все без исключения, однако многие страны, в частности страны Европейского союза, соотносят использование видеонаблюдения с единым актом в сфере защиты персональных данных General Data Protection Regulation. Следует отметить, что единого подхода к регулированию использования систем видеонаблюдения и распознавания лиц в этих странах не выработано до сих пор. В некоторых городах США существует запрет применения технологии распознавания лиц при видеонаблюдении. Однако в КНР практикуется широкомасштабное использование как видеонаблюдения, так и технологии распознавания лиц с полной идентификацией и даже с правовыми последствиями (штраф, социальный рейтинг и др.).

Мировой опыт внедрения и распространения технологий интеллектуального видеонаблюдения для обеспечения общественной безопасности «умного города» свидетельствует о неоднозначном отношении к нему общества [15]. С одной стороны, применение подобных систем действительно приводит к положительной динамике сокращения преступности, предотвращению крупных аварий и т. д., с другой – далеко не каждое общество отдельно взятой страны готово к тотальному контролю со стороны государства и небезосновательно видит в этом посягательство на тайну частной жизни. Вместе с тем, все большее распространение получает добровольное

согласие на так называемое «отслеживание» путем использования различных приложений, определяющих и использующих геолокацию [2].

В 2021 году в Республике Беларусь вступил в силу Закон № 99-З «О защите персональных данных» (далее – Закон), который вносит определенную ясность в данную сферу [16]. В Законе дается следующее определение: персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Идентификация физического лица – это когда физическое лицо может быть прямо или косвенно определено, например, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности. Преимущество нового определения заключается в том, что оно четко описывает основные признаки персональных данных и позволяет относить к таким данным информацию, косвенно идентифицирующую субъектов персональных данных [17].

Законом, в частности, определяются биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение, голос и другое). Таким образом, биометрических и физиологических данных большое количество, причем далеко не все активно используются с точки зрения сбора и последующей обработки.

Во многих странах осуществляется сбор биометрических данных, таких как распознавание голоса и лица. Применение данных технологий возможно и в рамках электронного правительства при получении электронных услуг. К примеру, в России принят Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…», который регулирует отношения, возникающие при осуществлении идентификации с использованием биометрических персональных данных, что подчеркивает внимание к данной проблеме со стороны государства.

В рамках данного исследования полагаем возможным выделить изображение (фотографию или видеосъемку) человека как визуальные персональные данные, как подвид биометрических персональных данных, так как именно эти данные используются как государством, так и бизнесом. Сбор, обработка, хранение и даже передача этих данных, в том числе трансграничная, осуществляются повсеместно, начиная со сканирования и распознавания лица при использовании смартфона до полной идентификации человека на улице камерами видеонаблюдения. Причем визуальные персональные данные становятся таковыми только после идентификации личности человека. Результаты видеосъемки в общественных местах или на охраняемой территории до установления личности не считаются биометрией. Только после распознавания и идентификации личности человека они становятся визуальными персональными данными [17].

Следует отметить, что использование систем видеонаблюдения возможно и без идентификации человека, в целом это касается общего мониторинга ситуации в городе. В случае выявления определенных отклонений от нормы (скопление людей, девиантное поведение, совершение противоправных действий) применяется технология распознавания лиц.

Контроль и защита визуальных персональных данных

Контроль и защита со стороны оператора персональных данных

Изображение лица человека, распознанное системами видеонаблюдения, может храниться в различных базах данных. При утечке сведений из таких баз в Интернет они становятся доступными для всеобщего пользования. Люди должны быть уверены, что их визуальные персональные данные не будут потом использованы в противоправных целях.

Персональные данные человека должны быть защищены. Такая защита включает целую группу мер. В первую очередь, это меры программного-технического характера (криптографическая защита, регламентация права на доступ и др.). Кроме того, очень важны меры организационно-правового характера: издание документов, определяющих политику оператора в отношении обработки персональных данных, и ознакомление с ними сотрудников оператора, определение порядка доступа, внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные, обучение сотрудников, назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработ-

кой персональных данных, введение режима и охраны помещений, эффективного делопроизводства по электронным документам и т. п. [18].

Обнародовать изображение гражданина – значит впервые сделать изображение доступным для всеобщего сведения (опубликование, публичный показ, размещение в Интернете или любой другой способ). Однако обнародование изображения (в том числе размещение его самим гражданином в Интернете) и его общедоступность не дают иным лицам права его свободно использовать без получения согласия изображенного лица.

Отдельной проблемой является использование баз изображений лиц и людей для обучения нейронных сетей. При использовании существующих наборов данных, имеющихся в Интернете, для обучения СНС приходится сталкиваться с проблемой защиты персональных данных, и некоторые наборы данных являются закрытыми, так как авторы предоставляют для исследований не изображения, а только извлеченные из изображений людей признаки. Некоторые наборы данных можно использовать с ограничениями [19], потому что при публикации исследований оператор просит соблюдать конфиденциальность студентов, изображения которых использовались для создания, при этом распространение этих наборов данных возможно только при согласовании с авторами. Некоторые наборы данных могут быть отозваны. Например, DukeMTMC-ReID [20] был отозван и его использование не рекомендуется из-за нарушений гражданских прав, прав людей и частной жизни студентов университета Duke, изображения которых использовались при формировании набора данных.

Если базу данных, содержащую фото людей, планируется кому-то передать и использовать, то необходимо, чтобы оператор выставил, а принимающая сторона подписала и соблюдала следующие условия:

- база данных не будет публиковаться, копироваться или распространяться каким-либо образом или в какой-либо форме, независимо от того, был изменен набор данных или нет;
- вся база данных будет использоваться только в целях научных исследований;
- изображения из базы данных не могут быть опубликованы или показаны в какой-либо форме для публикации, документа или демонстрации.

Для возможности использования изображений людей в исследовательских целях при формировании базы данных, содержащей их фото, у всех участников необходимо просить разрешения на включение фото в базу. И такое разрешение должно быть в письменном виде. Чтобы запросить и получить базу изображений для исследований, необходимо отправить подписанное соглашение держателям базы [21].

Контроль со стороны гражданина

С точки зрения гражданина важным является вопрос сбора, использования и дальнейшего распространения видео с его участием. Открытым остается вопрос присутствия человека в различных базах данных и возможности от этого отказаться.

Согласие субъекта персональных данных на обработку персональных данных, за исключением специальных персональных данных, не требуется: для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности; для исполнения правосудия, судебных постановлений и иных документов; в целях осуществления контроля (надзора) в соответствии с законодательными актами; для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно [16].

Основное требование законодателя в Беларуси к допустимости видеозаписи и фотосъемки заключается в том, что обе стороны должны быть осведомлены о ее проведении [3]. Однако гражданин не знает, каким образом будет использована видеосъемка в последующем и будет ли произведена идентификация личностей. В связи с этим критики системы видеонаблюдения и распознания лиц Kipod, используемой в Республике Беларусь, считают, что она либо уже интегрирована, либо будет в будущем, с АС «Паспорт», АИС «ГАИ-Центр», и рассматривают это как нарушение прав и свобод граждан [3].

В рамках Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, а также Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, информационная безопасность определена как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Таким образом, информационная безопасность личности является составной частью информационной безопасности.

В связи этим необходимо соблюдать баланс интересов государства с точки зрения обеспечения общественной безопасности с использованием видеонаблюдения и последующей видеоаналитики и интересов человека, так как затрагиваются вопросы неприкосновенности частной жизни и персональных данных.

В соответствии с Законом любой человек вправе отозвать согласие, а оператор обязан прекратить обработку и удалить информацию. Но данное право может быть реализовано только если этому предшествовало само согласие. Человек может требовать удаления своих данных, если их собрали или обработали без законных оснований. Остается открытым вопрос реализации данного права в части определения оператора. Если видео размещено в сети Интернет, то найти автора или первоисточник практически невозможно для простого пользователя. Если в результате опубликования фотографий или видеозаписи возникает реальная угроза жизни и здоровью гражданина либо ему наносятся моральные страдания, то на основании его мотивированного обращения распространение (демонстрация) данной информации должно быть прекращено. Однако существует необходимость в разработке подзаконных актов, строго регламентирующих данную процедуру.

На основании анализа зарубежного опыта выявляются следующие случаи использования изображения физического лица без его согласия:

– изображение человека относится к его публичной деятельности либо официальной должности;

– предоставление изображения человека по запросу правоохранительных органов;

– фиксация изображения человека в общественных местах.

Помимо указанных случаев использования изображения человека без его согласия, выявляется ограничительный принцип: использование изображения не должно унижать честь, достоинство и деловую репутацию человека, нарушать его половую неприкосновенность, противоречить моральным устоям [22].

Таким образом, необходимо разграничивать интересы государства в рамках обеспечения общественной безопасности и интересы личности в рамках защиты неприкосновенности частной жизни.

Считаем, что на сегодняшний день существуют предпосылки для дальнейшего развития законодательства в сфере защиты персональных данных в части видеонаблюдения и выделения отдельного подвида биометрических персональных данных – визуальных персональных данных. Граждане должны иметь право на контроль за своими визуальными персональными данными.

Заключение. В настоящее время применение систем видеонаблюдения является неотъемлемым признаком развитых стран, движущихся по пути построения «умных» городов. В эпоху развития искусственного интеллекта возможности данных систем не ограничиваются просто съемкой или обезличенным видеонаблюдением, а предоставляют возможности распознавания и полной идентификации человека. В связи с тем, что процесс информатизации привел к созданию многочисленных баз данных, включая автоматизированные информационные системы персональных данных (АС «Паспорт», ГИС «Регистр населения» и др.), интеграция этих систем с системами видеонаблюдения является вопросом времени. Впоследствии полная идентификация человека станет возможной в автоматическом режиме.

Следует отметить положительный аспект применения систем интеллектуального видеонаблюдения: сократилось количество противоправных действий, повысилась раскрываемость преступлений, появилась возможность предотвращения крупных аварий и т. д. С другой стороны, вопросы неприкосновенности частной жизни и обеспечения информационной безопасности личности выходят на первый план. Потому необходимо на правовом уровне обеспечивать баланс интересов государства и личности. Со стороны использования систем видеонаблюдения государством, в том числе РСМОБ, следует обеспечивать защиту на техническом, организационном (строгая регламентация доступа, ответственность лиц, имеющих доступ к системам, и др.) и правовом (с точки зрения защиты права на неприкосновенность частной жизни) уровнях.

В связи с тем, что видеокамеры широко применяются частными лицами (видеорегистраторы, съемки блогеров, самовольно установленные камеры видеонаблюдения и др.), угроза для человека в части сохранения приватности возрастает. С учетом имеющихся технических возможностей и с использованием общедоступных персональных данных, распространенных самим человеком (социальные сети и др.), идентификация человека также возможна.

Полагаем своевременным дальнейшее совершенствование законодательства в сфере

защиты персональных данных путем выделения отдельного подвида – визуальных персональных данных – и разработки правового регулирования в данной сфере. В том числе: рассмотрение случаев, когда можно применять собранную с помощью использования систем видеонаблюдения биометрическую информацию (например, в расследовании преступлений и т. п.); кто (круг лиц) и каким образом может использовать данную информацию; каким образом граждане могут оспаривать и исключать информацию о себе из таких баз.

Список литературы

1. Шрейнер, И. Ю. Внедрение системы «умный город» для повышения безопасности городской среды / И. Ю. Шрейнер, И. С. Пашкова // Безопасность городской среды: мат-лы IV Междунар. науч.-практ. конф., Омск, 16-18 ноября 2016 г. - Омск: Омский гос. техн. ун-т, 2017. - С. 314-316.
2. Абламейко, М. С. Использование систем искусственного интеллекта при обеспечении общественной безопасности в «умном городе»: юридические аспекты / М. С. Абламейко, Н. В. Шакель, Р. П. Богуш // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. - 2021. - № 5. - С. 84-92.
3. Веренчиков, И. Р. Особенности криминалистического распознания лиц: проблемы и перспективы. Право в современном белорусском обществе: сб. научн. тр. / И. Р. Веренчиков, А. Е. Середа // Нац. центр законодательства и правовых исследований Респ. Беларусь; редкол.: Н. А. Карпович (гл. ред) [и др.]. - Минск: Колорград, 2022. - Вып. 17. - С. 733-741.
4. Как работает распознание лиц и каким образом можно обойти данную систему для правонарушителей [Электронный ресурс]. - Режим доступа: https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7. - Дата доступа: 07.02.2022.
5. «Улыбнитесь»: в каких городах мира больше всего камер видеонаблюдения [Электронный ресурс]. - Режим доступа: https://devby.io/news/ulybnites-v-kakih-gorodah-mira-bolshe-vsego-kamer-videonabludeniya. - Дата доступа: 07.02.2022.
6. Hatmaker, T. Bipartisan Bill Proposes Oversight for Commercial Facial Recognition [Electronic resource] / T. Hatmaker. - Mode of access: http://social.techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act. - Date of access: 07.02.2022.
7. О республиканской системе мониторинга общественной безопасности [Электронный ресурс]: Указ Президента Республики Беларусь, 25 мая 2017 г., № 187. - Режим доступа: https://www.etalonline.by/document/?regnum=p31700187. - Дата доступа: 07.02.2022.
8. Богуш, Р. П. Обнаружение объектов на изображениях с большим разрешением на основе их пирамидально-блочной обработки / Р. П. Богуш, И. Ю. Захарова, С. В. Абламейко // Информатика. - 2020. - № 2. - С. 109-117.
9. Ye, S. Person Tracking and Re-Identification in Video for Indoor Multi-Camera Surveillance Systems / S. Ye, R. Bohush, C. Chen, I. Zakharava, S. Ablameyko // Pattern Recognition and Image Analysis, 2020. - Vol. 30, № 4. - P. 827-837.
10. Hjelm, E. Face Detection: a Survey / E. Hjelm, Boon Kee Low // Computer Vision and Image Understanding. - 2001. - Vol. 83. - P. 236-274. - doi:10.1006/cviu.2001.0921.
11. Ma, M. H. Multi-View Face Detection and Landmark Localization Based on MTCNN, In Proc. of the Chinese Automation Congress / M. H. Ma, J. Wang. - Xi'an, 2018. - P. 4200-4205.
12. InsightFace Model Zoo [Electronic resource]. - Mode of access: https://github.com/deepinsight/insightface/wiki/Model-Zoo MTCNN. - Date of access: 12.02.2022.
13. MOTChallenge: The Multiple Object Tracking Benchmark [Electronic resource]. - Mode of access: https://motchallenge.net. - Date of access: 24.06.2022.
14. В Китае научились распознавать 95% лиц в масках [Электронный ресурс]. - Режим доступа: https://www.forbes.ru/newsroom/biznes/395425-v-kitae-nauchilis-raspoznavat-95-lic-v-maskah. - Дата доступа: 10.02.2022.
15. Климович, А. П. Влияние цифровых технологий на современное общество. Пример системы рейтинга социального кредита в Китае / А. П. Климович // Цифровая социология. - 2020. - Т. 3. - № 3. - С. 35-44.
16. О защите персональных данных [Электронный ресурс]: Закон Республики Беларусь, 7 мая 2021 г., № 99-З / Национальный центр правовой информации Республики Беларусь. - Минск, 2021. - Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1&p5=0. - Дата доступа: 10.01.2023.
17. Абламейко, М. С. Защита визуальных персональных данных: правовые аспекты / М. С. Абламейко // Веб-программирование и интернет-технологии WebConf2021: материалы 5-й Международной научно-практической конференции, Минск, 18-21 мая 2021 г. / БГУ, Механико-математический фак.; редкол.: И. М. Галкин (отв. ред.) [и др.]. - Минск: БГУ, 2021. - 400 с. - Деп. в БГУ 07.05.2021, № 005207052021.
18. Вильтовский, Д. Персональные данные усложнят жизнь работодателям [Электронный ресурс] / Д. Вильтовский // Режим доступа: https://neg.by/novosti/otkrytj/personalnye-dannye-uslozhnyat-zhizn-rabotodatelyam. - Дата доступа: 10.11.2021.
19. Li, W. Deep Filter Pairing Neural Network for Person Re-identification [Электронный ресурс]. / W. Li, R. Zhao, T. Xiao., X. Wang // DeepReID: IEEE Conference on Computer Vision and Pattern Recognition. - 2014. - P. 152-159. - Режим доступа: https://doi.org/10.1109/CVPR.2014.27. - Дата доступа: 10.02.2022.
20. Exposing.ai. Duke MTMC. [Electronic resource]. - Mode of access: https://exposing.ai/duke_mtmc. - Date of access: 04.06.2022.
21. Dataset and Code [Electronic resource]. - Mode of access: https://www.pkuvmc.com/dataset.html. - Date of access: 04.06.2022.
22. Сухопаров, В. П. Охрана изображения человека в контексте уточнения правового статуса блогера в законодательстве Республики Беларусь / В. П. Сухопаров // Конституционное и муниципальное право. - 2021. - № 5. - С. 30-34.

References

1. Shrejner I. Ju., Pashkova I. S. Vnedrenie sistemy «umnyj gorod» dlja povyshenija bezopasnosti gorodskoj sredy [Implementation of the «smart city» system to improve the safety of the urban environment]. Omsk: Omskij gosudarstvennij tehnicheskij universitet, 2017. P. 314-316. (Russian).
2. Ablameyko M. S., Shakel' N. V., Bogush R. P. Ispol'zovanie sistem iskusstvennogo intellekta pri obespechenii obshhestvennoj bezopasnosti v «umnom gorode» [The use of artificial intelligence systems in ensuring public safety in a «smart city»]. *Vestnik Polockogo gosudarstvennogo universiteta*, 2021. № 5. P. 84-92. (Russian).
3. Verenchikov I. R., Sereda A. E. Osobennosti kriminalisticheskogo raspoznanija lic. Pravo v sovremennom belorusskom obshhestve [Features of forensic face recognition. Law in modern Belarusian society]. / Nacionalnij centr zakonodatel'stva i pravovyh issledovanij Respubliki Belarus'. Minsk: Kolorgrad, 2022. Vol. 17. P. 733-741. (Russian).
4. Kak rabotaet raspoznanie lic i kakim obrazom mozhno obojti dannuju sistemu dlja pravonarushitelej [How facial recognition works and how it can be bypassed for offenders]. Available from: https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7. (accessed: 07.02.2022). (Russian).
5. «Ulybnites'»: v kakih gorodah mira bol'she vsego kamer videonabljudenija [«Smile»: which cities in the world have the most CCTV cameras]. Available from: https://devby.io/news/ulybnites-v-kakih-gorodah-mira-bolshe-vsego-kamer-videonabludeniya. (accessed: 07.02.2022). (Russian).
6. Hatmaker T. Bipartisan Bill Proposes Oversight for Commercial Facial Recognition. Available from: http://social.techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act. (accessed: 07.02.2022).
7. O respublikanskoj sisteme monitoringa obshhestvennoj bezopasnosti [On the republican system of monitoring public safety]. Available from: https://www.etalonline.by/document/?regnum=p31700187. - (accessed: 07.02.2022). (Russian).
8. Bogush R. P., Zaharova I. Ju. , Ablamejko S. V. Obnaruzhenie ob'ektov na izobrazhenijah s bol'shim razresheniem na osnove ih piramidal'no-blochnoj obrabotki [Object detection in high-resolution images based on their pyramid-block processing]. *Informatika*. 2020. № 2. P. 109-117. (Russian).
9. Ye S., Bohush R., Chen C., Zakharava I., Ablameyko S. Person Tracking and Re-Identification in Video for Indoor Multi-Camera Surveillance Systems. *Pattern Recognition and Image Analysis*, 2020. Vol. 30, № 4. P. 827-837.
10. Hjelm E. Boon Kee Low Face Detection: a Survey. *Computer Vision and Image Understanding*. 2001. Vol. 83. P. 236-274. - doi:10.1006/cviu.2001.0921.
11. Ma M. H., Wang J. Multi-View Face Detection and Landmark Localization Based on MTCNN, In Proc. of the Chinese Automation Congress. Xi'an, 2018. P. 4200-4205.
12. InsightFace Model Zoo. Available from: https://github.com/deepinsight/insightface/wiki/Model-Zoo MTCNN. (accessed: 12.02.2022).
13. MOTChallenge: The Multiple Object Tracking Benchmark. Available from: https://motchallenge.net. (accessed: 24.06.2022).
14. V Kitae nauchilis' raspoznavat' 95% lic v maskah [China has learned to recognize 95% of masked faces]. Available from: https://www.forbes.ru/newsroom/biznes/395425-v-kitae-nauchilis-raspoznavat-95-lic-v-maskah. (accessed: 10.02.2022). (Russian).
15. Klimovich A. P. Vlijanie cifrovyh tehnologij na sovremennoe obshhestvo [The impact of digital technologies on modern society]. *Cifrovaja sociologija*. 2020. Vol. 3. № 3. P. 35-44. (Russian).
16. O zashhite personal'nyh dannyh [On the protection of personal data]. Nacional'nyj centr pravovoj informacii Respubliki Belarus'. Available from: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1&p5=0. (accessed: 10.01.2023). (Russian).
17. Ablameyko M. S. Zashhita vizual'nyh personal'nyh dannyh [Protection of visual personal data]. Minsk: BGU, 2021. 400 p. (Russian).
18. Vil'tovskij D. Personal'nye dannye uslozhnjat zhizn' rabotodateljam [Personal data will make life difficult for employers]. Available from: https://neg.by/novosti/otkrytj/personalnye-dannye-uslozhnyat-zhizn-rabotodatelyam. (accessed: 10.11.2021). (Russian).
19. Li W., Zhao R., Xiao T., Wang X. Deep Filter Pairing Neural Network for Person Re-identification. DeepReID: IEEE Conference on Computer Vision and Pattern Recognition. 2014. P. 152-159. Available from: https://doi.org/10.1109/CVPR.2014.27. (accessed: 10.02.2022).
20. Exposing.ai. Duke MTMC. Available from: https://exposing.ai/duke_mtmc. (accessed: 04.06.2022).
21. Dataset and Code. Available from: https://www.pkuvmc.com/dataset.html. (accessed: 04.06.2022).
22. Suhoparov V. P. Ohrana izobrazhenija cheloveka v kontekste utochnenija pravovogo statusa blogera v zakonodatel'stve Respubliki Belarus' [Protection of the image of a person in the context of clarifying the legal status of a blogger in the legislation of the Republic of Belarus]. *Konstitucionnoe i municipal'noe pravo*. 2021. № 5. P. 30-34. (Russian).

Abstract. Keywords

The article describes the results of using video surveillance systems, discusses the signs by which a person is detected and recognized. The experience of a number of countries in implementing artificial intelligence systems to strengthen public safety in existing «smart cities» is analyzed. The introduction of the term «visual personal data» and the definition of measures for its application in the existing legal field for the protection of personal data both on the part of the operator of such systems and on the part of the citizen are proposed. Proposals for the development of the legal framework in the Republic of Belarus in order to protect the rights of citizens are outlined.

Keywords: smart city; intelligent video surveillance; biometric personal data; visual personal data; face recognition; human identification; information security

Received (дата поступления): 08.02.2023