YURIDIK FANLAR AXBOROTNOMASI

ВЕСТНИК ЮРИДИЧЕСКИХ НАУК

REVIEW OF LAW SCIENCES

huquqiy ilmiy-amaliy jurnal

правовой научно-практический журнал

legal scientific-practical journal

2021/3

MUNDARIJA

12.00.02 – KONSTITUTSIYAVIY HUQUQ. MA'MURIY HUQUQ. MOLIYA VA BOJXONA HUQUQI

12.00.03 – FUQAROLIK HUQUQI. TADBIRKORLIK HUQUQI. OILA HUQUQI. XALQARO XUSUSIY HUQUQ

12.00.08 – JINOYAT HUQUQI. HUQUQBUZARLIKLARNING OLDINI OLISH. KRIMINOLOGIYA. JINOYAT-IJROIYA HUQUQI

12.00.09 – JINOYAT PROTSESSI. KRIMINALISTIKA. TEZKOR-QIDIRUV HUQUQ VA SUD EKSPERTIZASI

12.00.10 – XALQARO HUQUQ

12.00.11 – PARLAMENT HUQUQI

13.00.02 – TA'LIM VA TARBIYA NAZARIYASI VA METODIKASI (SOHALAR BO'YICHA)

UDC: 343.9
ORCID: 0000-0003-0480-317X

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКИХ ДАННЫХ В ПЕРИОД ДИДЖИТАЛИЗАЦИИ ОБЩЕСТВА

Югай Людмила Юрьевна,
доктор философии (PhD) по юридическим наукам,
докторант факультета послевузовского образования
Академии МВД Республики Узбекистан,
e-mail: yugai.lyudmila@mail.ru

Аннотация. *В условиях цифровизации общества в процесс идентификации и верификации личности широко внедряются инновационные технологии, базирующиеся на биометрических данных, что делает тему исследования актуальной. Кроме того, криминалистические биометрические базы данных решают важные задачи по идентификации личности неопознанных трупов, лиц, совершивших преступление, лиц, находящихся в розыске. Обозначена необходимость повышения уровня обеспечения защиты биометрических персональных данных в связи с участившимися случаями их утери или краж по всему миру. Цель работы – исследовать значение и классификацию биометрических данных, осветить нормативно-правовые акты, регламентирующие отношения в сфере оборота биометрической информации, риски и угрозы безопасности биометрических данных. В ходе исследования использовались методы системно-структурного, сравнительно-правового и статистического анализа, формально-логические, общенаучные и частнонаучные методы научного познания. В результате проведенной работы на основе обзора различных подходов отечественных и зарубежных ученых и практиков рассмотрены вопросы использования биометрической информации в различных сферах социальной жизни, а также технические, организационные и правовые аспекты обеспечения безопасности биометрических данных. Результаты исследования можно использовать в деятельности, связанной с оборотом биометрической информации, в судебно-экспертной практике, на занятиях в образовательных учреждениях и курсах повышения квалификации судебных экспертов. Даны предложения и рекомендации по совершенствованию уровня обеспечения безопасности биометрических баз данных, интеграции различных видов биометрических модальностей, систематическому тестированию биометрических систем в целях защиты от внешних противоправных воздействий.*

Ключевые слова: *биометрические технологии; персональные данные; информационная безопасность; биометрия; базы данных.*

ЖАМИЯТНИ РАҚАМЛАШТИРИШ ЖАРАЁНИДА БИОМЕТРИК МАЪЛУМОТЛАРНИНГ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ МАСАЛАСИ

Югай Людмила Юрьевна,
юридик фанлар бўйича фалсафа доктори (PhD),
Ўзбекистон Республикаси ИИВ Академиясининг
Олий таълимдан кейинги таълим факультети докторанти

Аннотация. *Тадқиқот мавзуси жамиятни рақамлаштириш шароитида шахсни идентификация ва верификация қилиш жараёнига биометрик маълумотларга асосланган инновацион тех-*

нологияларнинг жорий этилаётгани сабабли долзарб саналади. Бундан ташқари, маълумотларнинг криминалистик биометрик базалари шахси аниқланмаган жасадлар, жиноят содир этган шахслар, қидирувда бўлган шахсларни аниқлаш бўйича муҳим вазифаларни ҳам ҳал этади. Бутун дунёда шахсга доир биометрик маълумотларнинг йўқолиши ва ўғирланиши ҳолатларининг кўпайиши сабабли уларнинг ҳимоясини таъминлаш даражасини ошириш зарурлиги белгиланди. Тадқиқотнинг мақсади – биометрик маълумотларнинг аҳамияти ва таснифини ўрганиш, биометрик маълумотлар айланмаси, биометрик маълумотлар хавфсизлигига оид хавфлар ва таҳдидлар соҳасидаги муносабатларни тартибга солувчи меъёрий-ҳуқуқий ҳужжатларни ёритишдан иборат. Тадқиқотда тизимли-таркибий, қиёсий-ҳуқуқий ва статистик таҳлил усуллари, илмий билимларнинг расмий-мантиқий, умумилмий ва аниқ илмий усулларидан фойдаланилди. Олиб борилган изланишлар натижасида мамлакатимиз ҳамда хорижлик олимлар ва амалиётчиларнинг турли ишларини кўздан кечириш асосида биометрик маълумотларни ижтимоий ҳаётимизнинг турли соҳаларида қўллаш, шунингдек, биометрик маълумотлар хавфсизлигини таъминлашнинг техник, ташкилий ва ҳуқуқий жиҳатлари каби масалалар кўриб чиқилди. Тадқиқот натижаларини биометрик маълумотлар айланмаси билан боғлиқ фаолиятда, суд-экспертиза амалиётида, таълим муассасалари ва суд экспертларининг малакасини ошириш курслари машғулотларида қўллаш мумкин. Биометрик маълумотлар базасининг хавфсизлигини таъминлаш даражасини такомиллаштириш, биометрик модалликнинг ҳар хил турларини интеграция қилиш, ташқи ноқонуний таъсирлардан ҳимоя қилиш мақсадида биометрик тизимларни изчил синовдан ўтказиш бўйича таклиф ва тавсиялар берилди.

Калит сўзлар: *биометрик технологиялар; шахсга доир маълумотлар; ахборот хавфсизлиги; биометрия; маълумотлар базаси.*

ON THE ISSUE OF ENSURING BIOMETRIC DATA SECURITY DURING THE PERIOD OF THE DIGITALIZATION OF SOCIETY

Yugai Lyudmila Yuriyevna,
Doctor of Philosophy (Ph.D.) in Juridical Science
Doctoral student at the Faculty of Postgraduate Education of the
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract*. The theme of the research is relevant since innovative technologies based on biometric data are widely introduced into the process of identification and verification of a person in the context of the digitalization of society. In addition, forensic biometric databases solve important tasks for personal identification of unidentified corpses, persons who have committed a crime, and persons on the wanted list. The need is noted for increasing the level of ensuring the protection of biometric personal data, in connection with the increasing cases of their loss or theft around the world. The research is aimed at investigating the meaning and classification of biometric data, highlighting the normative-legal acts regulating relations in the sphere of biometric information circulation, risks and threats to the security of biometric data. During the study, the methods of system-structural, comparative-legal and statistical analysis, formal-logical, general scientific and specific scientific methods of scientific knowledge were used. As a result of activities carried out based on a review of various approaches of domestic and foreign scientists and practitioners, the issues of using biometric information in various spheres of social life, as well as technical, organizational and legal aspects of ensuring the security of biometric data, are considered. The research results can be used in activities related to the circulation of biometric information, in forensic practice, during the classes in educational institutions and advanced training courses for forensic experts. Suggestions and recommendations are given for improving the level of ensuring the security of biometric databases, integrating various types of biometric modalities, systematic testing of biometric systems to protect against external unlawful influences.*

Keywords: *biometric technologies; personal data; information security; biometrics; databases.*

Введение

В период цифровой трансформации общества и внедрения инноваций вопросы защиты информации от несанкционированного доступа приобретают особую значимость. В Послании Олий Мажлису Президент Республики Узбекистан Шавкат Мирзиёев определил для нашего государства в качестве одной из приоритетных задач – освоение цифровых знаний и информационных технологий. В настоящее время в нашей стране мы наблюдаем увеличение объемов обмена большими данными, расширение сервиса электронных услуг, которые вносят существенный вклад в дальнейшее развитие современного общества.

Возникает своеобразный парадокс. С одной стороны, развитие информационных технологий и их широкое внедрение в жизнь общества способствуют открытости, транспарентности, противодействуют коррупционным составляющим, создают удобства для населения, ликвидируют бюрократические препоны для решения жизненных вопросов, снижают сроки получения тех или иных услуг, с другой же, создают своеобразные риски и угрозы для владельцев персональных данных в случае их утечки или кражи.

Отдельным видом персональных данных являются биометрические данные человека. Вопросам защиты биометрической информации и технологий посвятили свои научные работы Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin [1], M.S. Siddiqui [2], S. Phadke [3], С.Б. Баженов, Д.В. Попов, В.Е. Дивольд, А.А. Морозов, Д.М. Сафронов, А.В. Серов [4, с. 42-51], Е.В. Полуянова, С.Д. Ковалев [5, с. 45-51], В.Д. Тульских [6], А. Подрез [7, с. 61-66], А.В. Полещук [8, с. 44-47], М.С. Кривогин [9], М.С. Бекмурзин, В.П. Захаров, О.И. Зачек [10, с. 44-49] и многие другие ученые.

Данное научное направление интенсивно развивается и является объектом исследования технической, медицинской, биологической и юридической наук.

Целью исследования является раскрытие практики использования биометрических технологий в условиях современного информационного развития общества во всех направлениях деятельности государства, в том числе и в сфере раскрытия и расследования преступлений, анализ правовой базы и проблем обеспечения сохранности биометрических персональных данных за рубежом и в Республике Узбекистан, систематизация и выделение практически значимых рекомендаций для безопасности биометрических технологий.

Материалы и методы

Биометрия широко используется при аутентификации личности в мобильных телефонах, ноутбуках, компьютерах, проведении нотариальных сделок, прохождении вступительных экзаменов в высшие учебные заведения, подтверждении факта составления электронного протокола об административном правонарушении при нарушении правил дорожного движения, в банковской деятельности и т. д. Вышеуказанное создает огромные риски и угрозы при недостаточно ответственном отношении к сохранности персональных данных.

Биометрическая информация хранится в специализированных автоматизированных базах данных. Биометрические системы представляют собой технологии идентификации и верификации личности, базирующиеся на основе анатомических или биологических параметров человека. Данные системы имеют широкое распространение за счет удобства применения и оперативности проверки по базам.

Специалисты дифференцируют биометрические параметры на статические и динамические.

К статическим биометрическим параметрам относятся отпечатки пальцев рук, черты лица, особенности строения ДНК,

строение радужки и сетчатки глаза, термограмма лица, ладони и т. д.

К динамическим (поведенческим или физиологическим) биометрическим параметрам относятся походка человека, голос, почерк, особенности набора клавиш на клавиатуре, сердцебиение и т. д.

В большей степени имеют распространение биометрические базы данных, основанные на статических биометрических данных (папиллярных узорах пальцев рук, чертах лица и ДНК).

Вопросы внедрения биометрических технологий вызывают разделение взглядов и мнений ученых на два лагеря. Ряд специалистов подчеркивают возможность тотального контроля и злоупотребления биометрическими персональными данными в ущерб личным правам и свободам, неприкосновенностью частной жизни. Их противники аргументируют необходимость применения данных технологий обеспечением общественного порядка и безопасности, удобством идентификации и верификации.

Е.В. Киричек отмечает, что любое государство заинтересовано быть монополистом в информационном пространстве в целях осуществления полного (тотального) контроля за всеми сферами жизнедеятельности человека. В этом отношении защита интересов государства в современном мире выдвигается на первый план и, надо сказать, довольно успешно в отличие от интересов личности, ее личной свободы. В демократическом правовом государстве интересы личности приоритетны, они не должны пренебрегаться и попираться. И именно этот принцип является определяющим при создании механизма комплексной защиты персональных данных [11, с. 98-100].

Толчком развития биометрических технологий идентификации личности в мире стали террористические акты в США в 2001 г., это обусловило развитие законодательной, организационной и технической базы.

Возникает сложная правовая дилемма. На одной чаше весов находятся личные права и свободы граждан, а на другой чаше – безопасность общества и государства, общественный порядок и планомерное развитие всех общественных институтов. На наш взгляд, в условиях политической и социально-экономической нестабильности отдельных регионов, увеличения географии миграционных процессов, роста религиозного экстремизма, терроризма, торговли людьми, наркотическими средствами и оружием, расширения трансграничной преступности, региональных и военных конфликтов целесообразно, в первую очередь, принять меры по обеспечению устойчивого развития общества, мирной жизни и безопасности всех граждан с безусловным соблюдением всех личных прав и гарантий конфиденциальности биометрических данных.

Некоторые государства относят биометрическую информацию к чувствительным категориям персональных данных. К ним относятся: Австрия, Босния и Герцоговина, Италия, Македония, Румыния, Украина, Черногория, Чехия и Эстония. В Болгарии и Польше биометрические данные в качестве общей категории не упоминаются, однако их отдельные виды, например генетические, могут относиться к специальным категориям. Во Франции, Португалии, Люксембурге, Латвии, Словении, Грузии, Македонии и Черногории для осуществления оператором обработки биометрических данных необходимо получить предварительное согласие национального органа по защите персональных данных [9].

Закон, регулирующий защиту персональных данных, имеется в большинстве стран – в России, Украине, Казахстане, Азербайджане, Китае, Сингапуре, Австралии, а также странах Латинской Америки, Европы и др. Данный закон у каждого государства может называться иначе чем у

другого, в некоторых государствах принят отдельный закон о персональных данных, а в других случаях отношения по сбору, обороту, хранению персональных данных регламентируются другими законодательными актами, затрагивающими их. В данных законах урегулирован механизм сбора, оборота, хранения персональных данных между субъектом персональных данных, собственником базы персональных данных и другими лицами. Эти и другие понятия почти во всех странах одинаковы и базируются на правах граждан этих стран на неприкосновенность частной жизни. Базовым международным документом, регламентирующим отношения в сфере оборота персональной информации, является Конвенция о защите физических лиц при автоматизированной обработке персональных данных, принятая в Страсбурге в 1981 г.

В США защита персональных данных на федеральном уровне регулируется отдельными отраслями права. К примеру, Закон о торговле финансовыми инструментами запрещает публиковать данные, связанные с покупкой акций, Закон о страховых агентах запрещает обнародовать информацию о застрахованных людях. Отдельного федерального закона о персональных данных, который бы регулировал их защиту, в США нет, он есть только в ряде штатов, например, в Калифорнии, Массачусетсе или округе Колумбия. Там же, в Кремниевой Долине, Гарварде и Массачусетском техническом университете (MIT), сконцентрировано большинство IT-компаний, которые и попадают под действие этого закона [12]. При том, что в данных странах вышеуказанный закон принят уже относительно давно, со временем всплывают коллизии, связанные с оборотом персональных данных в современных условиях.

Большинство стран Совета Европы уже ратифицировало Конвенцию № 108 «О защите физических лиц при автоматизированной обработке персональных данных» (1981), а страны, входящие в Европейский союз, – Директиву 95/46/ЕС от 24 октября 1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». Их принятие было направлено на защиту прав граждан при обработке персональных данных, которые в зависимости от степени чувствительности подразделяются на две категории – обычные и специальные. Такое разделение в дальнейшем было воспринято многими странами мира и стало использоваться в национальных нормативно-правовых актах как образец надлежащего учета интересов субъектов персональных данных [13, с. 80-89].

Кроме того, с мая 2018 г. в Европе данная сфера отношений регулируется Общим регламентом о защите персональных данных (General Data Protection Regulation – GDPR). GDPR ЕС устанавливает требования на территории Европейского союза – право на забвение, недвусмысленное и положительное согласие, а также среди прочего суровое наказание за несоблюдение этих правил.

Право на забвение означает, что субъект данных имеет право отозвать свое согласие в любое время, также известное как «право быть забытым».

Об утечке персональных данных организация, осуществляющая оборот биометрических данных, должна сообщить властям в течение 72 часов. В случае несоответствующего обеспечения безопасности персональных данных компания должна заплатить штраф около 20 млн евро.

Организации, не зарегистрированные в ЕС, подпадают под действие GDPR, если они обрабатывают персональные данные о субъектах данных из ЕС. Вышеуказанное распространяет действие GDPR за пределы ЕС.

В Китае сохранность биометрических данных обеспечивается Законом о

кибербезопасности (Cybersecurity Law – CSL), вступившим в силу 1 июня 2017 г., и Спецификацией безопасности личной информации (Personal Information Security Specification), принятой в мае 2018 г. Данная Спецификация является руководством по сбору, хранению и обработке данных.

Закон о защите личной информации (The personal information protection law – PIPL) был разработан в 2020 г. и находится на пересмотре. 10 июня 2021 г. в Китае был принят новый Закон о безопасности данных (Data Security Law – DSL), который вступит в силу 1 сентября 2021 г.

В Китае на сегодняшний день реализуется широкий государственный надзор, связанный с практически повсеместным сбором биометрических данных. Однако при этом параллельно повышается конфиденциальность субъектов биометрических данных в условиях киберсуверенитета.

В Индии биографические и биометрические данные всех жителей в возрасте старше 18 лет интегрируются в национальную биометрическую систему Aadhaar. В системе хранятся данные об имени, дате рождения, поле, адресе, отпечатках пальцев и радужной оболочке глаз. После чего каждому жителю присваивается 12-значный идентификационный номер, который может использовать любое зарегистрированное лицо для идентификации резидента Индии.

28 февраля 2019 г. в Индии был одобрен закон, регулирующий программу биометрической идентификации в стране [14].

В соответствии со ст. 13 Закона Республики Узбекистан «О принципах и гарантиях свободы информации» от 12 декабря 2002 г. № 439-II, информация о персональных данных физических лиц относится к категории конфиденциальной информации. Исходя из положений ст. 11 Закона Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II, конфиденциальную информацию содержат информационные ресурсы ограниченного доступа. Информационная безопасность личности обеспечивается путем защиты тайны частной жизни. Не допускается сбор, хранение, обработка, распространение и использование информации о частной жизни, а равно информации, нарушающей тайну частной жизни без согласия лица, кроме случаев, предусмотренных законом. Оборот данного рода информации регламентируется Законом Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547. Данный закон определяет порядок обработки и защиту персональных данных, права и обязанности участников обработки персональных данных, а также их ответственность.

В соответствии со ст. 27^1 данного закона, базы данных, на которых собираются, систематизируются и хранятся персональные данные граждан Республики Узбекистан при использовании информационных технологий, в том числе во всемирной информационной сети Интернет, должны быть физически размещены на территории Республики Узбекистан и зарегистрированы в установленном порядке в Государственном реестре баз персональных данных.

Необходимо отметить, что в эпоху диджитализации особое значение приобретают создание национальных и международных биометрических баз данных лиц, находящихся в розыске, особо опасных рецидивистов, террористов и экстремистов, использование и обмен биометрической информацией в рамках борьбы с терроризмом, экстремизмом, торговлей людьми, торговлей оружием, незаконным оборотом наркотических средств и другими видами транснациональных преступлений.

Вышеуказанное обуславливает необходимость скоординированных действий между государствами в контексте обеспечения информационной безопасности. В первую очередь, необходимо урегули-

ровать вопросы, связанные с защитой биометрических данных лиц, направить усилия на то, чтобы сбор, хранение и использование данных сведений велись в соответствии с имеющимися международными стандартами в области прав человека и международными законами о неприкосновенности частной жизни, в том числе Международным пактом о гражданских и политических правах, принятым резолюцией 2200 А (XXI) Генеральной Ассамблеи Организации Объединенных Наций от 16 декабря 1966 г., а также Всеобщей декларацией прав человека ООН, принятой на третьей сессии Генеральной Ассамблеи резолюцией 217 А (III) от 10 декабря 1948 г.

С учетом возрастания роли личных прав и свобод граждан важным вопросом является обеспечение сохранности биометрических баз данных, а также защита лиц, у которых были похищены их биометрические данные или которые просто стали жертвой ошибки в системе.

В последнее время по всему миру участились случаи кражи персональных данных с целью мошенничества, снятия денежных средств с банковских счетов и т. д. Так, в 2016 г. в Гане были похищены биометрические данные избирателей; в 2017 г. были украдены биометрические данные (отпечатки пальцев) филиппинских избирателей; были украдены отпечатки пальцев покупателей американской компании Avanti Markets; кроме того, в Индии была зарегистрирована утечка из всеобщей биометрической системы Aadhaar, которая используется для аутентификации в банках и при получении государственных услуг. В 2018 г. в Зимбабве похитили отпечатки пальцев и фотографии избирателей. В 2019 г. в открытый доступ попала многомиллионная дактилоскопическая база южнокорейской компании Suprema. В России похищены записи голоса клиентов Сбербанка [15].

В марте 2020 г. была выявлена утечка персональных данных более 267 млн пользователей Facebook. В августе 2020 г. эксперты из компании DarkNet Data Leakage & Breach Intelligence (DLBI) обнаружили в Сети персональные данные 150 млн пользователей Facebook, Instagram и LinkedIn. Персональные данные были похищены с сервера в США [16].

При этом хакеры атакуют информационные базы правоохранительных органов. К примеру, в 2011 г. были взломаны сайты нескольких полицейских участков в США. В феврале 2012 г. был заблокирован сайт МВД Украины. В апреле 2012 г. вышел из строя сайт МВД Великобритании. В марте 2013 г. взломан сайт суда Южного Урала в Челябинской области Российской Федерации [10, с. 44-49].

В результате хакерской атаки 20 ноября 2017 г. были недоступны сайты Министерства юстиции Республики Узбекистан, хокимията Ташкента, Государственного центра тестирования и другие сайты государственных учреждений и организаций. 24 июля 2020 г. хакеры атаковали сайт Агентства по противодействию коррупции, оставив при этом сообщение о завладении соответствующими данными [17].

Биометрические идентификаторы (черты лица, голос, особенности папиллярного узора и т. д.) используются как средство подтверждения личности в банковской, нотариальной, избирательной сферах, системах контроля управления доступом и др. Биометрический учет является важным сегментом криминалистической регистрации. Биометрические характеристики являются относительно устойчивыми и неизменными. Их сложно поменять или подобрать как пароль. Это является одновременно их достоинством и недостатком. Последствия от открытого доступа, модификации, кражи или утери биометрических данных из централизованных хранилищ влечет еще более тяжкие последствия, чем

утечка традиционных данных или хищение каких-либо материальных ресурсов.

В связи с тем, что в последнее время во многих странах при осуществлении голосования в целях подтверждения личности избирателя используются биометрические параметры, при необходимости, используя украденные биометрические данные, косвенно можно воздействовать на ход и результаты избирательных процессов.

Кроме того, в ходе проведенных исследований А. Подрезом было установлено, что около 26 % всех наиболее распространенных биометрических проектов в мире встречаются в банковской сфере, причем их география очень обширна – Канада, США, Мексика, Коста-Рика, Гватемала, Нидерланды, Великобритания, Франция, Китай, Индия, Япония, Южная Корея, Сингапур, Катар, Пакистан, Кувейт, ЮАР и другие страны [7, с. 61-66].

Проект внедрения биометрических систем идентификации личности в банковской деятельности на сегодняшний день реализуется в Республике Узбекистан. Создается единая биометрическая система, которая позволит финансовым организациям и ритейлу проводить удаленную идентификацию, а также оказывать электронные услуги в дистанционном режиме [18].

Исходя из этого, можно сделать вывод, что сбой биометрической банковской системы или кража биометрических данных может повлечь за собой экономический ущерб не только для отдельного лица или государства, но может приобрести также и межгосударственный характер.

Результаты исследования

В законодательстве Республике Узбекистан отводится особое внимание защите биометрических данных. В статье 27 Основного закона Республики Узбекистан каждому лицу гарантируется право на защиту частной жизни от вмешательства. Право на неприкосновенность частной жизни включает также и защиту персональных данных, в том числе биометрических данных.

Кроме того, статья 27 Закона Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547 определяет, что государство гарантирует защиту персональных данных.

В соответствии со статьей 8 Закона Республики Узбекистан «О государственной геномной регистрации» от 24 ноября 2020 г. № ЗРУ-649, геномная информация, а также сведения о личности человека, проходящего государственную геномную регистрацию, являются конфиденциальными.

Категорически запрещается распространение информации без согласия лица или его законного представителя, кроме как в интересах правосудия на основании запросов компетентных органов.

В сфере информационной безопасности, в том числе и контексте безопасности биометрических персональных данных, профессор А.К. Расулев выделяет правовые, социальные и организационно-технические меры [19, с. 340-341]. Р.К. Кабулов и Э.С. Абдурахманов считают, что данная проблема комплексная и состоит в основном из технических и организационных аспектов [20, с. 55].

На наш взгляд, защита персональных биометрических данных осуществляется путем реализации правовых, организационных и технических мер.

Технические аспекты включают в себя весь необходимый комплекс программно-технического обеспечения биометрической системы. К данным мерам относятся использование электронных, электронно-механических, механических устройств и конструкций для создания препятствий на возможных путях проникновения и получения доступа нарушителями к элементам системы и биометрическим дан-

ным. К ним относятся также средства визуального наблюдения, связи, охранной сигнализации, обнаружения и тушения пожара, оборудование обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установка резервных систем электропитания, оснащение помещений замками, установка сигнализации, разное электронное оборудование и специализированное программное обеспечение, предназначенное для организации вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое.

Организационные аспекты обеспечивают защиту систем от несанкционированного доступа к биометрическим базам данных, что может повлечь кражу, изменение, умышленное или случайное уничтожение. К данным аспектам относятся специально разработанные административно-процедурные меры, предусматривающие строгий регламент, с помощью которого определен процесс работы системы получения и обработки биометрических данных, эксплуатации ресурсов системы, отбора и деятельности персонала, порядка взаимодействия пользователей и работников организации с информационными системами, так, чтобы затруднить или исключить возможность угрозы безопасности либо снизить их риски.

Главную роль при обеспечении информационной безопасности играет государство, которое в соответствии с действующим законодательством должно обеспечивать безопасность каждого гражданина. Именно государство несет большие потери от нарушения системы защищенности объектов в информационной среде [19, с. 230].

К правовым мерам относятся законодательные акты, приказы и другие нормативные документы, с помощью которых осуществляется регламентация правил обращения с защищаемыми биометрическими данными. Данный комплекс нормативно-правовых актов определяет ответственность за нарушение требований по защите персональных данных, обеспечивающих реализацию права на защиту от вмешательства в частную жизнь; права и обязанности субъектов информационных отношений при получении, обработке, эксплуатации данных; целостность и сохранность персональных данных; соблюдение конфиденциальности персональных данных; предотвращение незаконной обработки персональных данных.

Статья 46^2 Кодекса об административной ответственности Республики Узбекистан предусматривает ответственность за незаконный сбор, систематизацию, хранение, изменение, дополнение, использование, предоставление, распространение, передачу, обезличивание и уничтожение персональных данных, в том числе и биометрических. После повторного совершения данного деяния предусмотрена уже уголовная ответственность по статье 141^2 Уголовного кодекса Республики Узбекистан.

Е.Г. Барковская для обеспечения безопасности биометрических данных лиц предлагает объединить все учеты, хранящие биометрические данные человека, в единую систему и соединить их информационными связями. Единым объединяющим «идентификатором» должен выступать индивидуальный номер или код [21, с. 5-8].

По мнению С.С. Самищенко, в целях обеспечения конфиденциальности биометрических данных необходимо раздельное хранение биометрической и личностной информации граждан [22, с. 264-265]. Биометрические данные, хранящиеся в базе, будут иметь «безымянный» материал, имеющий только регистрационный номер.

С.Ю. Чимаров отмечает, что констатация возникновения инновационной пара-

дигмы учета биометрических показателей человека цифровой эпохи свидетельствует о необходимости учреждения новых юридических конструкций защиты прав человека, с учетом вызовов формирующегося цифрового общества, обусловленных появлением оригинальных цифровых решений Шестого технологического уклада развития общества [23, с. 169-171].

Анализ результатов исследования

Особую важность в обеспечении безопасности биометрических данных имеют:

выявление уязвимых мест биометрических систем и их систематическое тестирование;

обезличивание биометрических данных;

проведение исследований по разработке дополнительных систем защиты биометрических данных;

своевременное выявление кибератак и разработка систем уровней защиты от них;

обеспечение защиты от утечек информации;

ведение соответствующих протоколов и аудита;

безопасная передача биометрических данных и т. д.

Выводы

Необходимо отметить, что на данный момент ни одна биометрическая система не может стопроцентно отвечать требованиям информационной безопасности. Тщательная проработка правовых, организационных, технических аспектов безопасности биометрических данных является условием, определяющим успешность и безопасность применения этой технологии. Тенденции развития современных цифровых технологий обуславливают необходимость постоянного совершенствования информационной защиты биометрических персональных данных.

REFERENCES

1. Huszti-Orbán K., Ní Aoláin F. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? Minnesota, Human rights center, the University of Minnesota, 2020, 45 p.

2. Siddiqui M.S. Safety of biometric data with mobile phone operators. Available at: https://www.researchgate.net/publication/305638674_Safety_of_ biometric_data_with_mobile_phone_operators/ (accessed 23.06.2013).

3. Phadke S. The Importance of a Biometric Authentication System. The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), September-October 2013, vol. 1, no. 4, pp. 128-132.

4. Bazhenov S.V., Divol'd V.E., Morozov A.A., Popov D.V., Safronov D.M., Serov A.V. Sozdanie Koncepcii nacional'noj sistemy identifikacii lichnosti [Creation of the Concept of the National Personal Identification System]. Trudy Akademii upravlenija MVD Rossii – Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia, 2020, no. 2, pp. 42-51.

5. Polujanova E.V., Kovaljov S.D. Normativnoe regulirovanie ispol'zovanija biometricheskih personal'nyh dannyh v Rossijskoj Federacii. [Normative regulation of the use of biometric personal data in the Russian Federation]. Vestnik Tomskogo instituta povyshenija kvalifikacii rabotnikov FSIN Rossii – Bulletin of Tomsk Institute for Advanced Studies of the Federal Penitentiary Service of Russia, 2020, no. 3, pp. 45-51.

6. Tul'skih V.D. Ispol'zovanie biometricheskih tehnologij v jekspertno-kriminalisticheskoj dejatel'nosti [The use of biometric technologies in forensic activities]. Armija i obshhestvo – Army and Society, 2013, no. 1. Available at: https://cyberleninka.ru/article/n/ispolzovanie-biometricheskih-tehnologiy-v-ekspertno-kriminalisticheskoy-deyatelnosti/ (accessed 20.07.2021).

7. Podrez A. Biometricheskie tehnologii i perspektivy ih ispol'zovanija v finansovoj sfere [Biometric technologies and the prospects for their use in the financial sphere]. Bankaŭski vesnik – Bankauski Vesnik, 2018, no. 11, pp. 61-66.

8. Poleshhuk A.V. Osnovy zashhity personal'nyh dannyh [Fundamentals of Personal Data Protection]. T-Comm – Telekommunikacii i Transport. – T-Comm – Telecommunications and Transport, 2009, no. 5, pp. 44-47.

9. Krivogin M.S. Predposylki formirovanija special'noj pravovoj zashhity biometricheskih personal'nyh dannyh [Prerequisites for the formation of special legal protection of biometric personal data]. Obshhestvo: politika, jekonomika, pravo – Society: politics, economics, law, 2016, no. 8. (In Russ.) Available at: https://cyberleninka.ru/article/n/predposylki-formirovaniya-spetsialnoy-pravovoy-zaschity-biometricheskih-personalnyh-dannyh/ (accessed 20.07.2021).

10. Bekmurzin M.S., Zaharov V.P., Zachek O.I. Biometricheskie tehnologii v antiterroristicheskoj dejatel'nosti pravoohranitel'nyh organov: perspektivy i problemy ispol'zovanija [Biometric technologies in the anti-terrorist activities of law enforcement agencies: prospects and problems of use]. Vestnik Moskovskogo universiteta MVD Rossii – Bulletin of Moscow University of the Ministry of Internal Affairs of Russia, 2014, no.10, pp. 44-49.

11. Kirichek E.V. Nekotorye aspekty zashhity personal'nyh dannyh i realizacii «prava na zabvenie» v uslovijah cifrovizacii. Sibirskij juridicheskij forum: problemy obespechenija prav cheloveka: materialy Vserossijskoj nauchno-prakticheskoj konferencii [Some aspects of personal data protection and implementation of the "right to be forgotten" in the context of digitalization. Siberian Legal Forum: Problems of Ensuring Human Rights: Materials of the All-Russian Scientific and Practical Conference]. Barnaul, 2020, pp. 98-100 (In Russ.).

12. Filippenko Ja. Grazhdanin, projdemte. Kak rabotajut zakony o personal'nyh dannyh v Rossii i mire [Citizen, come along. How the laws on personal data work in Russia and the world]. Available at: http://www.forbes.ru/tehnologii/354899-grazhdanin-proydemte-kak-rabotayut-zakony-o-personalnyh-dannyh-v-rossii-i-mire/ (accessed 20.07.2021).

13. Krivonogin M.S. Osobennosti pravovogo regulirovanija biometricheskih personal'nyh dannyh [Features of legal regulation of biometric personal data]. Pravo. Zhurnal Vysshej shkoly jekonomiki – Law. Journal of the Higher School of Economics, 2017, no. 2, pp.80-89.

14. Biometric data and privacy laws (GDPR, CCPA/CPRA) [Biometric data and privacy laws (GDPR, CCPA/CPRA)]. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data/ (accessed 20.07.2021).

15. Kak zashhitit' biometricheskie dannye pol'zovatelej ot kriminal'nogo ispol'zovanija [How to protect users' biometric data from criminal use]. Available at: https://sk.ru/news/kak-zaschitit-biometricheskie-dannye-polzovateley-ot-kriminalnogo-ispolzovaniya/ (accessed 20.07.2021).

16. Desjat' samyh gromkih kiberatak XXI veka [The ten most high-profile cyberattacks of the 21st century]. Available at: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e/ (accessed 20.06.2021).

17. Hakery atakovali sajt Agentstva po protivodejstviju korrupcii [Hackers attacked the website of the Anti-Corruption Agency]. Available at: https://kun.uz/ru/news/2020/07/24/xakera-atakovali-sayt-agenstva-po-protivodeystviyu-korrupsii/ (accessed 20.07.2021).

18. Pred'javite lico: kak v Uzbekistane rabotaet biometrija [Show your face: how biometrics works in Uzbekistan]. Available at: https://uz.sputniknews.ru/20210602/predyavite-litso-kak-v-uzbekistane-rabotaet-biometriya-19042001.html/ (accessed 20.07.2021).

19. Rasulev A.A. Sovershenstvovanie ugolovno-pravovyh i kriminologicheskih mer bor'by v sfere informacionnyh tehnologij i bezopasnosti. Dis. dokt. jurid. nauk [Improvement of criminal law and criminological measures of struggle in the sphere of information technology and security. Dissertation of Doctor of Laws]. Tashkent, 2018, 341 p.

20. Kabulov R.K., Abdurahmanov Je.S. Prestuplenija v sfere informacionnyh tehnologij [Information Technology Crimes: A Study Guide]. Tashkent, 2009, 109 p.

21. Barkovskaja E.G. Sovershenstvovanie sistemy kriminalisticheskih uchetov v kontekste novyh biometricheskih tehnologij [Improving the system of forensic accounting in the context of new biometric technologies]. Jurist-Pravoved – Lawyer – Jurist, 2011, no. 1, pp. 5-8.

22. Samishhenko S.S. Sovremennaja daktiloskopija: teorija, praktika i tendencii razvitija. Dis. dokt. jurid. nauk [Modern fingerprinting: theory, practice and development trends. Dissertation of Doctor of Laws]. Moscow, 2003, 369 p.

23. Chimarov S.Ju. K voprosu o pravah cheloveka cifrovoj jepohi pri identifikacii ego biometricheskih pokazatelej. Sovremennaja jurisprudencija: aktual'nye voprosy, dostizhenija i innovacii. Materialy VII Mezhdunarodnoj nauchno-prakticheskoj konferencii [On the issue of the human rights of the digital era in the identification of his biometric indicators. Modern jurisprudence: current issues, achievements and innovations: Materials of the Seventh International Scientific and Practical Conference]. Penza, 2018, pp. 169-171 (In Russ.).