

УДК 342.951

DOI: 10.26467/2079-0619-2018-21-4-39-47

СОВРЕМЕННАЯ КОНЦЕПЦИЯ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ АВИАПАССАЖИРОВ

Н.М. ТЮКАЛОВА¹, А.А. РАЗУВАКИН¹*¹Дальневосточный юридический институт МВД России, г. Хабаровск, Россия*

В статье представлены основные положения концепции цифровой идентификации пассажиров авиарейсов, основанной на использовании технологии blockchain (блокчейн). Резюмируется, что внедрение защищенной биометрической идентификации пассажиров в аэропорту снизит временные и финансовые затраты, связанные с досмотром и прохождением паспортного и таможенного контроля. Анализируются проблемные аспекты действующего законодательства РФ, регламентирующего применение указанной технологии. Рассматривается технология Smart Path, разработанная компанией SITA, суть которой заключается в использовании биометрических данных как единого идентификационного токена на каждом этапе путешествия. Исследуются возможности применения технологии блокчейн в основе идентификации пассажиров перед вылетом, при этом технология блокчейн устраняет необходимость в централизованной обработке и хранении персональных данных авиапассажира. Основанная на криптосистеме компьютерная наука о цепочке блоков обеспечивает конфиденциальность данных и отсутствие возможности утечки сведений или их нецелевого использования. Особо отмечается, что технология криптографической защиты биометрических данных авиапассажира станет препятствием для использования персональной информации в противоправных целях, а возможности технологии блокчейн позволят производить трансграничный обмен данными во время международных перелетов. Делается вывод, что с применением этой технологии исчезнет потребность в содержании штата работников, отвечающих за проверку документов и контроль за идентификацией пассажиров. Все эти функции заменит распределенная база данных, которую невозможно уничтожить или взломать. На основе проведенного исследования предлагается внести изменения в действующее законодательство, регламентирующее процедуру сбора и обработки персональных данных пассажиров авиарейсов.

Ключевые слова: блокчейн, цифровая идентификация, распределенный реестр, досмотр, паспортный контроль, таможенный контроль.

Цифровая революция, охватившая современное общество, породила множество уникальных технологий, прочно вошедших в нашу повседневную жизнь и изменивших ее кардинальным образом. Современный человек уже немислим без смартфона или устройства, его заменяющего, так как вся важная информация, включая информацию о номерах телефонов близких людей или родственников, банковских картах, данных паспорта, индивидуального номера налогоплательщика, водительского удостоверения, авиабилетов, показателей температуры в квартире, даже управление бортовым компьютером автомобиля – все это сосредоточено в одном устройстве.

Интернет-технологии (далее – ИТ) позволяют экономить время при покупке продуктов в магазине или, например, при заказе такси. Больше не нужно тратить время для того, чтобы записаться на прием к врачу, достаточно просто зайти на сайт или открыть приложение, найти нужного врача и кликнуть на кнопку «Записаться на прием». Сегодня это стало возможным.

Вместе с этим повсеместное развитие ИТ в некоторых сферах не привело к желаемому результату. Так, внедрение ИТ в обработку персональных данных пассажиров авиарейсов не исключило применение таких мер государственного принуждения, как паспортный и таможенный контроль, а также досмотр [1, с. 192]. Являясь мерами административного предупреждения, паспортный, таможенный контроль и досмотр предусматривают выполнение должностными лицами действий по предотвращению совершения противоправных деяний. Наша концепция предлагает альтернативный вариант реализации функций государства по предупреждению правонарушений посредством внедрения технологии цифровой идентификации пассажиров и развития автоматизированной системы самообслуживания.

Сейчас пассажирам приходится прибывать в аэропорт за два, а то и за три часа до вылета, испытывать дискомфорт, стоя в длинных очередях для регистрации на рейс, и т. д. Человеческий фактор оказывает решающее воздействие на длительность прохождения процедур в общей зоне аэропорта, что в эру цифровой эпохи является уже скорее анахронизмом. При этом вся авиационная индустрия вынуждена нести колоссальные расходы на содержание аппарата служб авиационной безопасности, что в конечном итоге включается в стоимость тарифа на авиаперевозку и вынуждает пассажиров расплачиваться за недостатки существующей системы контроля.

В сложившейся ситуации компании вынуждены вести борьбу за клиента, а победителем является тот, кто наиболее эффективно применил IT-технологии. В аэропортах происходит стремительная автоматизация основных производственных и бизнес-процессов, внедрение систем самообслуживания клиентов, развивается интернет-торговля и web-бронирование авиабилетов, электронная регистрация на рейс и т. д. Человек планомерно отстраняется от участия в процессах, в которых раньше он занимал главенствующее положение.

Однако в большинстве аэропортов существуют группы процессов, автоматизация в которых проходит медленными темпами либо вовсе не осуществляется. К таким процессам следует отнести процедуру паспортного, таможенного контроля, сдачу багажа, предполетный и послеполетный досмотры. Во-первых, это обусловлено специфичностью выполняемых действий в данных процессах, т. к. они связаны с обеспечением авиационной безопасности, а во-вторых, технологии самообслуживания весьма дорогостоящие и их внедрение может позволить себе далеко не каждое предприятие.

Вместе с тем уже сегодня во многих аэропортах происходит внедрение технологии самообслуживания и самоидентификации личности без контролеров, что позволяет значительно повысить производительность труда, сократить долю рабочих, занятых в различных сферах обслуживания, снизить производственные издержки и повысить скорость обслуживания.

Весьма значимым в решении этой проблемы может стать применение цифровой идентификации пассажира по биометрическим параметрам: лицевому изображению, голосу, отпечаткам пальцев – основанной на технологии «блокчейн». Это технология, способная радикально изменить наше представление о хранении информации, ее обработке, защите и возможности проверить правильность внесенных изменений.

Блокчейн (с английского *block chain* – цепочка блоков) – это название распределенной базы данных, которая и представляет собой построенную по определенным правилам последовательную цепочку блоков, которые содержат какую-либо информацию [2]. Каждый блок содержит метку времени и ссылку на предыдущий блок. Блоки увязаны между собой хронологически и криптографически.

Криптографическая увязка предполагает поддержку правил включения новых блоков в цепочку и отслеживание попыток изменения существующих блоков.

Также этот подход называют еще распределенным реестром, имея в виду тот факт, что не существует какого-либо централизованного органа (структуры, регулятора), который мог бы распоряжаться такой цепочкой блоков по собственному усмотрению. Соответственно, блокчейн как база данных не имеет централизованного контроля. Эта база данных открыта любому участнику сети и хранится на собственных компьютерах участников. Полная история изменений данных хранится в системе и защищается от изменений криптографическими механизмами. Возвращаясь к модели реестра, это можно представлять так, что подписанный электронной подписью реестр хранится в большом количестве копий в разных местах.

Естественно, что такая модель хранения порождает и свои проблемы, о которых часто предпочитают не упоминать. Во-первых, полное копирование всех данных, включая историю всех изменений, создает большие потребности в ресурсах памяти. Они необходимы для хранения всех этих копий на узлах, участвующих в обработке данных. Хранение истории изменений

приводит к тому, что потребности в ресурсах будут быстро возрастать по мере развития системы. Далее, распространение изменений по всем узлам существенно увеличивает как время транзакции, так и ее стоимость (в смысле вычислений). Естественно также, что могут быть виды деятельности, для которых открытое хранение информации в распределенной сети может оказаться неприемлемым (например, деятельность, связанная с коммерческой тайной или хранением персональной информации) [3, с. 131].

Принципы работы блокчейна впервые были описаны в 2008 году в работе «Биткойн: электронная денежная система одноранговой сети» человеком или группой исследователей под псевдонимом *Сатоши Накамото* [4, с. 2–3]. В этой работе блокчейн представлен как цепочка блоков транзакций криптографической платежной системы «Биткойн», где после совершения или оформления любой операции в цепочку добавляется новый блок.

Описанная модель называется *people to people* (или *peer-to-peer*) – таким образом, вам не нужны посредники для верификации личности или проведения транзакции. Этот процесс осуществляется с помощью массового сотрудничества и умного кода. Модель исключает вставку «фальшивого» блока или изъятия существующего – все сразу отображается в системе. Глобальная структура реагирует на любое движение. Технологически все происходит благодаря криптографическим алгоритмам (математическим операциям). Изначально указанная технология была применена как полностью реплицированная база данных в системе «Биткойн» – децентрализованной платежной системы, где все операции защищены криптографическим методом.

Сегодня технология блокчейн рассматривается как платформа для баз данных различных сфер деятельности. Швеция¹ и Объединенные Арабские Эмираты² планируют вести земельный реестр при помощи технологии блокчейн. В июне 2017 года компании Accenture и Microsoft представили систему цифровых удостоверений личности на блокчейне³.

В России границы применения технологии блокчейн имеют довольно широкий круг. Правовой основой применения технологии блокчейн является Федеральная целевая программа «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы», утвержденная Постановлением Правительства Российской Федерации № 426 от 21 мая 2013 года⁴. Задачей программы, в частности, является поддержка прикладных научных исследований и экспериментальных разработок, в том числе межотраслевого характера, направленных на создание продукции и технологий для модернизации отраслей экономики, выполняемых по приоритетам развития научно-технологической сферы с использованием результатов фундаментальных и поисковых исследований.

Во исполнение положения 4.9 программы «Развитие сервисов на основе информационных технологий в области медицины, здравоохранения, социального обеспечения, образования, науки и культуры», в органах государственной власти происходит активное экспериментальное внедрение технологии блокчейн. Так, в сентябре 2017 года Министерство здравоохранения

¹ Швеция тестирует технологию блокчейна для регистрации земли [Электронный ресурс] // Агентство новостей Reuters. Режим доступа: <https://www.reuters.com/article/us-sweden-blockchain/sweden-tests-blockchain-technology-for-land-registry-idUSKCN0Z22KV> (дата обращения: 01.02.2018).

² Теперь официально: земельный реестр Дубая начал «переезд» в блокчейн [Электронный ресурс]. Режим доступа: <https://coinmarket.news/2017/10/09/teper-ofitsialno-zemelnyj-reestr-dubaya-nachal-pereezd-v-blokchejn/> (дата обращения: 01.02.2018).

³ Правительство Бразилии тестирует блокчейн – систему удостоверения личности [Электронный ресурс]. Режим доступа: <https://coinmarket.news/2017/08/24/pravitelstvo-brazilii-testiruet-blokchejn-sistemu-udostoverenij-lichnosti/> (дата обращения: 01.02.2018).

⁴ О федеральной целевой программе «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы». Постановление Правительства РФ от 21 мая 2013 года № 426. Официальный портал правовой информации [Электронный ресурс]. Режим доступа: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102165433&rdk=&backlink=1> (дата обращения: 01.02.2018).

Российской Федерации заявило о запуске пилотного проекта по переводу электронных карт пациентов в российских медицинских учреждениях в систему на базе блокчейна⁵. Граждане смогут самостоятельно выбирать, с кем они поделятся личными сведениями.

В октябре 2017 года Министерством образования Российской Федерации был проведен конкурс по созданию и запуску цифровой платформы обмена знаниями и управления авторскими правами правообладателей. Исполнителем указанных работ, согласно конкурсной документации, является Сибирский федеральный университет. Срок исполнения контракта – сентябрь 2019 года⁶.

Совещательным органом, отвечающим за правовое, экспертное и информационно-консультативное обеспечение использования технологии блокчейн, является созданный при Комитете Госдумы Российской Федерации по вопросам развития цифровой экономики и внедрения блокчейн-технологий, промышленности, инновационному развитию и предпринимательству 28 сентября 2017 года Экспертный совет по цифровой экономике и блокчейн-технологиям⁷. В декабре Экспертный совет определил основные направления развития блокчейн технологий в России, в частности, было акцентировано внимание на проблеме законодательного регулирования вопроса оборота криптовалют, внедрения блокчейн-технологий в деятельность органов государственной власти⁸.

Распространение технологии блокчейн достигло апогея среди криптовалют. Сегодня криптовалюты привлекают к себе большое внимание, понятие Биткойн стало уже практически нарицательным. Вместе с тем необходимо отметить, что термин «валюта» (цифровая или нет) практически всегда будет естественным образом ассоциироваться с государственной регуляцией, совсем не ясно, сколько таких «валют» разрешит эмитировать государство и т. д. Иными словами, этот, несомненно, важный и интересный проект (криптовалюты) несколько затеняет иные возможности использования распределенного реестра, которые (что важно с практической точки зрения) совсем не требуют государственного регулирования. Однако как раз эти направления и должны быть основой для проектов с использованием баз данных.

В рамках проводимого исследования мы предлагаем применить технологию блокчейн для цифровой идентификации авиапассажира. Она будет включать в себя информацию о документе, удостоверяющем личность, перевозочных документах и биометрическую идентификацию. Совокупность указанных элементов образует «Единый токен пассажира». Токен (также аппаратный токен, USB-ключ, криптографический токен) – компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам.

Токен является основой цифровой биометрической идентификации пассажира. В теории представленная концепция выглядит следующим образом: пассажиры создают проверенный «токен» на своем мобильном телефоне, который содержит биометрические и другие персональные данные. В этом представлении будущих путешествий, независимо от того, где пассажир находится, он может просто сканировать свое лицо и сканировать свое устройство, чтобы убедиться, что он является авторизованным путешественником. Ввод биометрических данных

⁵ Технологию «блокчейн» применят для хранения электронных медкарт [Электронный ресурс]. Режим доступа: <https://vademec.ru/news/2017/09/06/elektronnye-meditsinskie-karty-rossiyan-budut-khranit-po-printsipu-blokcheyn/> (дата обращения: 01.02.2018).

⁶ Официальный сайт единой информационной системы в сфере закупок в информационно-телекоммуникационной сети Интернет [Электронный ресурс]. Режим доступа: <http://zakupki.gov.ru/epz/order/notice/ok44/view/common-info.html?regNumber=0173100003717000367> (дата обращения: 01.02.2018).

⁷ Официальный сайт Государственной думы Федерального Собрания Российской Федерации [Электронный ресурс]. Режим доступа: <http://www.duma.gov.ru/news/273/2092696/> (дата обращения: 01.02.2018).

⁸ На заседании Экспертного совета при Комитете Госдумы РФ обсудили ввоз майнеров и регулирование ICO [Электронный ресурс]. Режим доступа: <https://bits.media/news/na-zasedanii-ekspertnogo-soveta-pri-komitete-gosdumy-rf-obsudili-vvoz-maynerov-i-regulirovanie-ico/> (дата обращения: 01.02.2018).

пассажира происходит самостоятельно, путем сканирования лица и отпечатков пальцев (face & fingers ID). Эта технология была разработана в 2016 году шведской компанией SITA и получила название Smart Path («Умный путь»)⁹.

Суть технологии Smart Path заключается в использовании биометрических данных как единого идентификационного токена на каждом этапе путешествия. Токен легко интегрируется в существующую инфраструктуру аэропортов и системы авиакомпаний. Smart Path включает оборудование для самообслуживания, которое уже используется во всей отрасли, такое как киоски регистрации, блоки отсева пакетов, ворота для безопасного доступа на посадку и автоматическое пограничное управление, что делает развертывание этой технологии простым и экономичным.

Smart Path включает:

- киоски самообслуживания общего пользования (CUSS) с быстрыми надежными биометрическими возможностями регистрации;
- одинарные или двухстворчатые ворота для самостоятельной посадки, контроля доступа в стерильных зонах и зонах автоматизированного пограничного контроля;
- иную платформу, способную интегрировать подход к терминальному оборудованию общего пользования (CUTE), системам обработки пассажиров общего пользования (CUPPS) и киоскам самообслуживания общего пользования (CUSS);
- систему управления идентификационной информацией, которая фиксирует данные о пассажирских рейсах и связывает их с биометрическими параметрами.

Внедрение этой технологии можно сделать с минимальным участием работников аэропорта, так как биометрическую идентификацию пассажир проходит возле специально установленного для этих целей киоска при прибытии в аэропорт. Биометрические системы состоят из биометрического сканера (физического устройства, которое позволяет измерять ту или другую биометрическую характеристику) и алгоритма сравнения измеренной характеристики с предварительно зарегистрированной (биометрическим шаблоном). Например, пассажиры, прибывающие в международные аэропорты Австралии, имеют возможность самостоятельного прохождения паспортного контроля без участия сотрудников аэропорта с использованием автоматизированной системы SmartGate. Суть ее довольно проста: она использует данные биометрического паспорта и технологии распознавания лиц для выполнения таможенных и иммиграционных проверок, которые обычно проводятся офицерами пограничной службы¹⁰.

В момент считывания сканером биометрической информации программа синхронизируется с данными токена и подтверждает либо опровергает информацию о пассажире: его паспортные данные и данные перевозочных документов. После завершения процедуры синхронизации пассажиру выдаются бирки для багажа и открывается турникет для прохождения процедуры досмотра.

После прохождения досмотра пассажир сдает багаж, при этом специальное устройство считывает информацию с бирки багажа и пополняет в онлайн-режиме единый токен пассажира для последующей сверки во время путешествий, что облегчает процесс поиска багажа при трансфертных перелетах. Сюда входят системы поиска, распознавания и погрузки/разгрузки багажа, что ускоряет процесс его загрузки на борт самолета и выдачи в пункте назначения.

Например, в аэропорту Амстердама Схипхол хэндлинговые компании осуществляют физическую обработку багажа. Самой крупной из них является KLM – приблизительно 1100 сотрудников, тогда как количество сотрудников Amsterdam Airport Schiphol составляет 125 чел.,

⁹ Биометрия для повышения качества пассажирских перевозок. Революция в управлении идентификационной информацией [Электронный ресурс]. Режим доступа: <https://www.sita.aero/solutions-and-services/solutions/sita-smart-path> (дата обращения: 01.02.2018).

¹⁰ SmartGate – Frequently asked questions [Электронный ресурс] // Australian Customs and Border Protection Service. 2012. 28 MARCH. Режим доступа: <https://www.cbp.gov/travel/trusted-traveler-programs/global-entry/international-arrangements/australia/us-citizens> (дата обращения: 01.02.2018).

которые отвечают за развитие, управление и эксплуатацию всех багажных систем, включая компьютеры, программное обеспечение и управляющие системы. Эксплуатируемая ими система, состоящая из шести роботизированных погрузчиков багажа, разработанных Grenzebach, позволила увеличить пропускную способность аэропорта с 50 до 70 млн мест багажа (или на 40 %) ¹¹.

Технология Smart Path фиксирует биометрические данные пассажира с помощью лицевой проверки на входе в аэропорт. После проверки на проездные документы пассажира создается один безопасный токен. Затем на каждом шагу в пути – независимо от того, проходит ли пассажир сдачу багажа, пограничный контроль или посадку на борт – лицевое сканирование снимает необходимость отображения паспорта или посадочного талона.

Затем пассажир проходит в зал ожидания и ждет посадки на рейс. Вся процедура прохождения контроля занимает 15 минут.

Технология блокчейн устраняет необходимость в централизованной обработке и хранении персональных данных авиапассажиров. Основанная на криптосистеме компьютерная наука о цепочке блоков обеспечивает конфиденциальность данных и отсутствие возможности утечки сведений или их нецелевого использования. Также блокчейн обеспечивает:

- регистрацию событий, в том числе за предыдущий период, в целях оценки рисков (построение доверительных отношений);
- информирование о событиях в пределах аэропорта;
- повышение защищенности и достоверности данных пассажиров;
- отслеживание событий во время путешествия и управление данными о них.

В последующем, при прохождении процедур контроля в аэропорту страны прибытия, пассажиру будет нужно также пройти идентификацию, и система подтвердит предыдущую запись о его посадке в аэропорту страны убытия.

С применением этой технологии исчезнет потребность в содержании штата работников, отвечающих за проверку документов и контроль за идентификацией пассажиров. Все эти функции заменит распределенная база данных, которую невозможно уничтожить или взломать.

Примером попытки внедрения технологии Smart Path является аэропорт Дубай, в котором обработка багажа пассажиров происходит на основе технологии блокчейн. По мнению администрации аэропорта, использование указанной технологии позволит улучшить качество обслуживания и снизить время нахождения пассажира в зале выдачи багажа.

Основной проблемой, препятствующей распространению средств обмена информацией на основе технологии блокчейн в России, является полное отсутствие нормативно-правового регулирования. На сегодняшний день на сайте Минфина РФ опубликован законопроект «О цифровых финансовых активах», призванный регулировать отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязательств по смарт-контрактам ¹². В законе, в частности, предлагаются определения понятий «распределенный реестр цифровых транзакций», «токен», «криптовалюта». Главной особенностью законопроекта является его привязка к криптографическим платежным системам, что ограничивает рамки применения технологии блокчейн в иных, не связанных с валютой, сферах, например в сфере обеспечения авиационной безопасности.

¹¹ Amsterdam Airport Awards New Baggage Handling System Contract to Vanderlande Industries and IBM [Электронный ресурс] // Vanderlande Industries. 2009. 08 DEC. Режим доступа: <http://www.airport-technology.com/contractors/baggage/vanderlande/press12.html> (дата обращения: 01.02.2018).

¹² Проект федерального закона «О цифровых финансовых активах». Информация официального сайта Министерства финансов Российской Федерации [Электронный ресурс]. Режим доступа: https://www.minfin.ru/ru/document/?id_4=121810&order_4=P_DATE&dir_4=DESC&is_new_4=1&page_4=1&area_id=4&page_id=2104&popup=Y#ixzz56KfYgkM (дата обращения: 01.02.2018).

Вместе с этим уже сегодня технология Smart Path как система цифровой идентификации авиапассажиров может регулироваться нормами Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»¹³, Федерального закона от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»¹⁴ и Воздушного кодекса Российской Федерации¹⁵ (далее – ВК РФ), после внесения ряда соответствующих изменений.

В частности, следует внести изменения в ст. 85.1 ВК РФ, которая обязывает перевозчика обеспечивать передачу данных пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с законодательством Российской Федерации о транспортной безопасности и в области персональных данных, при международных перевозках также в уполномоченные органы иностранных государств в соответствии с международными договорами Российской Федерации или законодательством иностранных государств вылета, заменив термин «централизованные» на «децентрализованные». Это позволит распределить информацию о действиях пассажира в аэропорту на множество хранилищ, тем самым устранив необходимость в дополнительной передаче информации о пассажире в уполномоченные органы иностранных государств, т. к. получаемая информация будет общедоступной и обновляться на множестве устройств одновременно.

Федеральный закон «О персональных данных» (ч. 2, ст. 11) позволяет осуществлять обработку биометрических данных без согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности. К таким случаям Федеральный закон «О транспортной безопасности» относит в том числе досмотр, дополнительный досмотр и повторный досмотр в целях обеспечения транспортной безопасности (ст. 12.2).

Таким образом, применение указанной технологии в целях обеспечения транспортной безопасности является абсолютно законным.

В завершение следует отметить, что апробация представленной концепции в аэропортах Российской Федерации является весьма перспективным направлением. Это улучшит надзор за безопасностью в аэропорту, ускорит пассажирооборот и сократит ресурсы, необходимые для аэронавигации. Она будет способствовать развитию практики самообслуживания среди пассажиров, которые более склонны пользоваться предоставленными удобствами в аэропорту.

СПИСОК ЛИТЕРАТУРЫ

1. **Zheng Z. et al.** Blockchain Challenges and Opportunities: A Survey // Work Pap. 2016.
2. **Корнев А.П.** Административное право России: учебник. В 3-х ч. Ч. 1. М., 1996. 280 с.
3. **Намиот Д.Е.** Приложения блокчейн на транспорте / О.Н. Покусаев, В.П. Куприяновский, А.В. Акимов // International Journal of Open Information Technologies. 2017. № 12. С. 131.
4. **Satoshi N.** Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. С. 2–3.
5. **Маринцева К.В.** Классификация средств механизации и автоматизации процессов обслуживания авиапассажиров // Транспортные системы и технологии перевозок. 2012. № 3. С. 56–60.
6. **Зубков Б.В., Бочкарев А.Н.** Современные проблемы и риски в деятельности гражданской авиации, новые комплексные методы и средства обеспечения авиационной безопасности // Научный Вестник МГТУ ГА. 2007. № 122. С. 154–158.

¹³Собрание законодательства РФ. 2006. № 31. Ст. 3451. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

¹⁴Собрание законодательства РФ. 2007. № 7. Ст. 8374. Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности».

¹⁵Собрание законодательства РФ. 1997. № 12. Ст. 183. Воздушный кодекс РФ.

7. **Колпаков А.В.** Автоматическая система паспортного контроля на основе биометрических технологий / Н.Н. Чубуков, Т.В. Моисеева, С.А. Терехин, А.А. Мавзютов, Е.С. Столбецова, Д.Н. Копылов, И.Н. Спиридонов // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2011. № 5. С.64–68.

8. **Подложенов И.М.** Коммерческие банки: новые услуги и инновационные технологии коммуникации // Известия ПГУ им. В.Г. Белинского. 2011. № 24. С. 378–382.

9. **Корнилов В.Н.** Концепция безопасности аэропорта. Новые подходы // Транспорт Российской Федерации. Журнал о науке, практике, экономике. 2007. № 9(9). С. 45–49.

СВЕДЕНИЯ ОБ АВТОРАХ

Тюкалова Надежда Михайловна, кандидат юридических наук, доцент, профессор кафедры административного права и административно-служебной деятельности ОВД, n.tyikalova@mail.ru.

Разувакин Артем Андреевич, адъюнкт, Дальневосточный юридический институт МВД России, artrazuvakin@gmail.com.

MODERN CONCEPT OF DIGITAL IDENTIFICATION OF AIR PASSENGERS

Nadezhda M. Tyikalova¹, Artem A. Razavakin¹

¹*Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, Khabarovsk, Russia*

ABSTRACT

The article presents the main provisions of the digital passenger identification concept based on the use of blockchain technology. It is summarized that the introduction of secure biometric identification of passengers at the airport will reduce the time and financial costs associated with the inspection and going through the passport and customs control. The problematic aspects of the current legislation of the Russian Federation regulating the application of this technology are analyzed. The technology Smart Path, developed by SITA is considered. The essence of this technology is the use of biometric data as a single identification taken at each stage of the journey. The possibilities of using blockchain technology as the basis of passenger identification before the departure are analyzed, while the blockchain technology eliminates the need for centralized processing and storage of personal data of air passengers. A computer science dealing with the chain of blocks based on the cryptosystem ensures the confidentiality of data and the absence of the possibility of information leakage or misuse. It is specially noted that the technology of cryptographic protection of air passengers biometric data will become an obstacle to using personal information for illegal purposes, and the capabilities of blockchain technology will allow cross-border data exchange during international flights. It is concluded that with the use of this technology, there will be no need to maintain the staff of workers responsible for document verification and control over the identification of passengers. All these functions will be replaced by a distributed database, which cannot be destroyed or hacked. On the basis of the study, it is proposed to amend the current legislation regulating the procedure for collecting and processing the personal data of airline passengers.

Key words: blockchain, digital identification, distributed register, inspection, passport control, customs control.

REFERENCES

1. **Zheng, Z. et al.** (2016). *Blockchain Challenges and Opportunities: A Survey*. Work Pap.
2. **Korenev, A.P.** (1996). *Administrativnoe pravo Rossii*. Ucheb. V 3 ch. Ch. 1 [Administrative Law of Russia. Textbook in 3 parts]. Moscow, 280 p. (in Russian)
3. **Namiot, D.E., Pokusaev, O.N., Kupriyanovskij, V.P. and Akimov, A.V.** (2017). *Prilozheniya Blokchein na transporte* [Transport blockchain]. International Journal of Open Information Technologies, no. 12, p. 131. (in Russian)

4. **Satoshi, N.** (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*, pp. 2–3.
5. **Marinceva, K.V.** (2012). *Klassifikaciya sredstv mekhanizacii i avtomatizacii processov obsluzhivaniya aviapassazhirov* [Classification of means of mechanization and automation of air passengers service]. *Transportnye sistemy i tekhnologii perevozok*, no. 3, pp. 56–60. (in Russian)
6. **Zubkov, B.V. and Bochkarev, A.N.** (2007). *Sovremennye problemy i riski v deyatel'nosti grazhdanskoj aviacii, novye kompleksnye metody i sredstva obespecheniya aviacionnoj bezopasnosti* [Modern problems and risks in the activities of civil aviation, new integrated methods and means of aviation security]. *Scientific Bulletin of the Moscow State Technical University of Civil Aviation*, no. 122, pp. 154–158. (in Russian)
7. **Kolpakov, A.V., CHubukov, N.N., Moiseeva, T.V., Terekhin, S.A., Mavzyutov, A.A., Stolbecova, E.S., Kopylov, D.N., Spiridonov, I.N.** (2011). *Avtomaticheskaya sistema pasportnogo kontrolya na osnove biometricheskikh tekhnologij* [Automatic passport control system based on biometric technologies]. *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, no. 5, pp. 64–68. (in Russian)
8. **Podlozhenov, I.M.** (2011) *Kommercheskie banki: novye uslugi i innovacionnye tekhnologii kommunikacii* [Commercial banks: new services and innovative communication technologies]. *Izvestiya PGPU im. V.G. Belinskogo*, no. 24, pp. 378–382. (in Russian)
9. **Kornilov, V.N.** (2007). *Koncepciya bezopasnosti aehroporta. Novye podhody* [The concept of airport security. New approaches]. *Transport of the Russian Federation. A magazine of science, economy and practice*, no. 9(9), pp. 45–49. (in Russian)

INFORMATION ABOUT THE AUTHORS

Nadezhda M. Tyukalova, Candidate of Juridical Sciences, Associate Professor, Professor of Chair of Administrative Law and Administrative Official Activity of Internal Bodies, Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, n.tyukalova@mail.ru.

Artem A. Razuvakin, Postgraduate, Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, artrazuvakin@gmail.com.

Поступила в редакцию 28.03.2018
Принята в печать 17.07.2018

Received 28.03.2018
Accepted for publication 17.07.2018