Материалы Всероссийской научно-практической конференции с международным участием «Современные проблемы антикриминальной деятельности российского государства»

Proceedings of the All-Russian Scientific-Practical Conference with international participation «Modern Problems of Anti-Criminal Activities of the Russian State»

УДК 336.6
DOI 10.33184/pravgos-2020.4.36

ЕДИНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА И ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КАК ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКОВСКИХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ: ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ

КУЗБАГАРОВ Муслим Назаргалиевич
кандидат юридических наук, доцент, доцент кафедры правоведения Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте РФ, доцент кафедры гражданско-правовых дисциплин Государственного института финансов, экономики, права и технологий, г. Санкт-Петербург, Россия.
E-mail: muslim_72@mail.ru

КУЗБАГАРОВА Елена Викторовна
кандидат юридических наук, доцент, доцент кафедры судебных экспертиз Санкт-Петербургского государственного архитектурно-строительного университета, г. Санкт-Петербург, Россия.
E-mail: elenakuzbagarova@mail.ru

Статья посвящена организационным и правовым вопросам использования единых систем идентификации в различных отраслях экономики, в частности в банковской сфере. Использование в Российской Федерации с

2011 г. Единой системы идентификации и аутентификации (ЕСИА) и с 2018 г. – Единой биометрической системы (ЕБС) стало одним из перспективных направлений в деятельности коммерческих банков и других субъектов финансовой системы. Активное внедрение ЕБС и ЕСИА в банковскую сферу целесообразно рассматривать как инструмент обеспечения безопасности банковских операций с использованием сети Интернет, созданный на основе современных инженерно-технических и программных разработок. **Цель:** анализ основных направлений использования ЕСИА и ЕБС в банковской сфере, выявление существующих организационных и правовых проблем, возникающих в деятельности банков при осуществлении операций. **Методы:** анализа и синтеза, обобщения, сравнения и системного подхода. **Результаты:** авторами обозначены организационные и правовые проблемы, возникающие в деятельности банков при осуществлении операций с использованием сети Интернет, предложены пути их решения.

Ключевые слова: единая система идентификации и аутентификации; единая биометрическая система; персональные данные; банковские операции; банковская система интернет-банкинга; правовое регулирование.

В соответствии с распоряжением Правительства РФ от 22 февраля 2018 г. № 293-р «О возложении на публичное акционерное общество междугородной и международной электрической связи "Ростелеком" функций оператора единой информационной системы персональных данных» с 1 июля 2018 г. в России введена ЕБС, которая является составной частью ЕСИА. ЕСИА и ЕБС позволяют производить удаленную идентификацию физических лиц: ЕБС – по степени схожести биометрического образца, ЕСИА – по логину/паролю.

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определено, что государственные органы, банки и иные организации в случаях, предусмотренных федеральными законами, после проведения идентификации при личном присутствии гражданина с его согласия на безвозмездной основе размещают в электронной форме:

1) сведения, необходимые для регистрации гражданина и юридического лица в ЕСИА, и иные сведения, если они предусмотрены федеральными законами, – в ЕСИА;

2) биометрические персональные данные гражданина, то есть данные изображения лица человека, полученные с помощью фото-, видеоус-

тройств; данные голоса человека, полученные с помощью звукозаписывающих устройств, – в ЕБС.

При необходимости использования ЕБС и ЕСИА в какой-либо сфере деятельности целесообразно определить, что здесь необходимо: идентификация, аутентификация или верификация. Идентификация направлена на использование персональных данных для установления личности человека. Цель верификации и аутентификации – установление действительности субъекта, но без установления его личности, то есть проверка истинности данных субъекта [1, с. 37].

Внедрение ЕБС и ЕСИА в России в настоящее время осуществляется в различных направлениях, исключением не стала и банковская сфера. В банковской сфере внедрена биометрическая идентификация – технология распознавания клиентов по биометрическим данным (изображению лица, отпечаткам пальцев, снимку радужной оболочки, записи голоса).

При осуществлении расчетных и кредитных обязательств население России и большинства стран мира активно использует банковскую систему дистанционного обслуживания интернет-банкинг, и процент вовлечения населения в данную сферу банковских услуг растет с каждым годом. Интернет-банкинг как конкурентно значимое средство имеет ряд преимуществ как для банковской сферы (сокращение расходов на функционирование офисов), так и для клиентов (отсутствие необходимости физического посещения банка и, как следствие, экономия времени и повышение активности использования электронных ресурсов). По числу безналичных платежей с использованием смартфонов (Apple Pay, Samsung Pay, Android Pay) Российская Федерация находится на первых местах в мире. Как видно, осуществление банковских операций все чаще происходит с использованием сети Интернет, электронных каналов связи.

Электронные расчеты в соответствии с Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»[1] являются разновидностью безналичных расчетов. Кроме того, данным законом определены некоторые особенности перевода денежных средств при проведении конкретных видов безналичных расчетов с учетом положений, определенных в иных нормативных актах, в частности с учетом Положения Банка России от 6 июля 2017 г. № 595-П «О платежной системе

[1] О национальной платежной системе : федер. закон от 27.06.2011 № 161-ФЗ (с изм. и доп., вступ. в силу с 03.08.2020) [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 12.11.2018).

Банка России»[1], Положения Банка России от 19 июня 2012 г. № 383-П «О правилах осуществления перевода денежных средств»[2]. В целях создания безопасной платформы функционирования интернет-банкинга на вооружение приняты ЕСИА и ЕБС как конкурентоспособные инструменты обеспечения безопасности банковских операций с использованием сети Интернет.

ЕБС значительно облегчает работу банков и весь процесс оформления банковских продуктов для клиента, так как для определения личности достаточно сопоставить голос и лицо клиента с данными в ЕБС. Клиенты банка, в свою очередь, могут оформить любой банковский продукт в любое время и в любом месте по телефону или в интернет-банке. Они могут осуществлять не только банковские операции и перевод денежных средств, но и кредитные обязательства.

Среди финтех-продуктов в России наибольшей популярностью пользуется онлайн-кредитование. По данным консалтинговой компании Deloitte, оно занимает 90 % от всей финтех-отрасли страны. Объем отрасли, по данным финтех-группы TWINO, в 2018 г. составил 80 млрд руб., что на 77 % больше, чем годом ранее. В 2017 г. российские онлайн-компании выдали на 67 % займов больше, чем в 2016-м. Однако в 2020 г. на фоне пандемии COVID-19 число полученных физическими и юридическими лицами кредитов снизилось на 3–8 % [2].

На Западе наиболее активно развивается онлайн-кредитование с использованием площадок P2P и P2B-кредитование. В России P2P-площадки также используются, но отсутствует правовая регламентация данного процесса, что, с одной стороны, создает ряд возможностей для их создателей, а с другой – увеличивает риски для займодателей на фоне сниженного уровня безопасности и роста числа фактов мошенничества в данной сфере. Ретейл в рамках создания безопасной платформы финансового существования вынуждает компании углубляться в сторону дополнительных сервисов и услуг, в том числе с использованием проверки клиентов по системам ЕБС и ЕСИА. Данные факты можно считать факторами для развития онлайн-кредитования в стране с учетом необходимости создания безопасной правовой и финансовой платформы данного вида деятельности в банковской сфере с учетом Указаний Банка России и ПАО «Ростелеком» № 4859-У/01/01/782-18 «О перечне угроз безопасности, ак-

[1] О платежной системе Банка России : положение Банка России от 06.07.2017 № 595-П // Вестник Банка России. 2017. № 90–91.

[2] О правилах осуществления перевода денежных средств : положение Банка России от 19.06.2012 № 383-П // Вестник Банка России. 2012. № 34.

туальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе»[1].

Для создания безопасной финансовой платформы компаниями активно используются перспективные инновационные технологии – искусственный интеллект, машинное обучение, предикативная аналитика и Big Data. В частности, в рамках скоринга при помощи искусственного интеллекта анализируют огромные объемы информации о потенциальном заемщике из самых разных источников, начиная от социальных сетей и заканчивая поведением человека при совершении покупок в интернет-магазинах и оплате мобильной связи. Современные системы позволяют обнаружить неочевидные тревожные сигналы и, наоборот, одобрить кредит тем заемщикам, которых «не пропустили» банковские системы аналитики [3]. С правовой точки зрения такой безопасной платформы в настоящее время в России нет.

Вместе с тем необходимо обратиться к нормам гражданского законодательства, регулирующим осуществление кредитных обязательств. К сожалению, для введенной Федеральным законом от 26 июля 2017 г. № 212-ФЗ «О внесении изменений в части первую и вторую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации»[2] конструкции консенсуального займа не было предложено аналогичное решение – требование об обязательном соблюдении письменной формы договора, которое выступало бы в качестве меры пра-

[1] О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе : указание Банка России и ПАО «Ростелеком» № 4859-У/01/01/782-18 [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 09.11.2020).

[2] О внесении изменений в части первую и вторую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 26.07.2017 № 212-ФЗ // Российская газета. 2017. № 167.

вового обеспечения безопасности совершения сделки, позволяющей впоследствии признать форму заключенной сделки соблюденной. Таким образом, в настоящее время в гражданском законодательстве России содержатся некоторые нормы, регулирующие банковскую деятельность по осуществлению расчетных и кредитных обязательств в системе интернет-банкинга, но они не направлены на регулирование банковской деятельности с использованием сети Интернет в целом.

В этой связи актуальной становится проблема правового обеспечения безопасности осуществления банковских операций в сети Интернет. Банки осуществляют внутренний контроль, в частности управляют информационными потоками (получение и передача информации) и обеспечивают информационную безопасность, в том числе при активном использовании ЕБС и ЕСИА, однако очевидным является тот факт, что в сфере интернет-банкинга безопасность обеспечивается недостаточно. Возникает обоснованная необходимость ввода и развития так называемых новых мер превентивного характера, которые должны быть закреплены на законодательном уровне. Все указанные мероприятия должны осуществляться в рамках государственного контроля банковской сферы.

Безусловно, банки сами стремятся к обеспечению дополнительной информационной безопасности и поэтому на данный момент времени практически любая транзакция должна быть подтверждена теми или иными действиями, то есть инициации транзакции на сайте кредитной организации или в приложении на смартфоне будет недостаточно. В нашей стране в качестве дополнительного подтверждения транзакции преимущественно используется введение кода, присланного в SMS-сообщении, но существуют и иные варианты подтверждения. Например, в некоторых скандинавских банках при оплате товара, купленного в Интернете, необходимо подтвердить транзакцию через банковское приложение (запрос появляется на экране смартфона, в котором установлено данное приложение).

В современном мире информационных технологий на данный момент эти меры уже в неполной мере обеспечивают безопасность, и главной проблемой реализации банковской деятельности по осуществлению расчетных и кредитных обязательств в системе Интернет является обеспечение сохранности средств как клиентов, так и банка. По мнению авторов, в настоящее время назрела необходимость не просто внесения изменений в действующее гражданское законодательство, а принятия новых нормативно-правовых актов, направленных на регулирование дистанционного банковского обслуживания, в том числе с использованием интернет-банкинга, и они должны быть основаны на положениях указа Прези-

дента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[1].

Письмо Банка России от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании»[2] предписывает банкам доводить информацию, в содержании которой описываются незаконные способы получения пароля или кода. Таким образом, возникает возможность доступа к данным, содержащимся в ЕСИА. Так, многие крупные российские банки разработали памятки безопасности для своих клиентов[3] и рекомендуют использовать не только ЕСИА, но и данные, содержащиеся в ЕБС.

Биометрическая система основывается на технологии записи образца индивидуальной биометрической черты пользователя, ее последующей обработки и сохранения. Биометрическая система в процессе обработки загруженной индивидуальной биометрической черты выделяет в ней идентификационные признаки и с помощью математической обработки переводит ее в математический код, который отправляется на хранение на сервер программы, присваивая ему идентификационный номер или иные информационные данные, например имя человека. В процессе использования системы будет осуществляться запрос на аутентификацию, то есть предоставляемые биометрические данные должны быть сравнены с теми, которые находятся в информационном банке. Успешная аутентификация позволяет человеку получить доступ к программе. Таким образом, основной задачей функционирования биометрической системы, в том числе и в банковской сфере, является аутентификация клиента.

Преимущества внедрения биометрических технологий в банковскую сферу достаточно подробно описаны в ряде научных статей [4; 5; 6]. Обобщенно можно сказать, что данные, хранящиеся в ЕБС, невозможно похитить, потерять или забыть, как следствие, это можно рассматривать как один из инструментов обеспечения безопасности совершения банковских операций с минимальной вероятностью ошибочной аутентификации. Российские банки стали широко использовать технологии распознавания голоса, приме-

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 [Электронный ресурс] // Доступ из справ.-правовой системы «Гарант» (дата обращения: 30.09.2020).

[2] О рисках при дистанционном банковском обслуживании : письмо Банка России от 07.12.2007 № 197-Т // Вестник Банка России. 2007. № 68.

[3] Памятка по безопасности при использовании удаленных каналов обслуживания ПАО Сбербанк [Электронный ресурс]. URL: https://docviewer.yandex.ru/view/524327421 (дата обращения: 10.11.2020).

няемые в call-центрах, сканирование отпечатков пальцев при входе в мобильное приложение банка и технологии распознавания лица.

Введение биометрических паспортов, содержащих биометрические данные клиента на встроенном чипе, станут основным источником качественного, защищенного и ускоренного обслуживания клиентов. Биометрический паспорт гражданина необходимо рассматривать как документ, удостоверяющий биометрические данные клиента банка [7, с. 126].

Банк России в рамках своих полномочий подготовил комплекс мер по повышению темпов развития ЕБС, который включает определенные регуляторные послабления (снижение размера требований по формированию резерва на возможные потери по ссудам), а также дополнительные требования, обязывающие коммерческие банки предоставлять установленный регулятором минимальный набор услуг (открытие вкладов, осуществление денежных переводов, предоставление потребительских кредитов и т. д.). Данные меры, по мнению экспертов и участников финансового рынка, способны интенсифицировать темпы развития программы использования биометрии, но в целом, вероятно, общую ситуацию существенно не изменят [5, с. 145].

ЕБС реализует возможность выявления именно живого человека по загруженным в базу биометрическим характеристикам. Используемые ПАО «Ростелеком» технологии являются лучшими разработками в данной области, ибо разработчики системы исходили из необходимости обеспечения безопасности и сохранности биометрических данных граждан и выявления мошеннических действий в банковской сфере. Здесь стоит обозначить существенный момент, который заключается в потенциальной угрозе совершения мошеннических действий в отношении других организаций, в нашем случае – банков, имеющих доступ к базам данных, через электронные каналы которых доступно проникновение в ЕСИА и ЕБС. В этой связи необходимо, чтобы банковские информационные технологии отвечали следующим характеристикам: 1) информация, хранящаяся на сервере, должна находиться в виртуальном поле доступа и администрироваться при помощи специализированного программного обеспечения; 2) система, используемая банками, должна регулярно проходить аттестацию Центрального Банка по удовлетворению требованиям и условиям безопасности; 3) трафик между системами должен шифроваться, то есть необходимо использовать SSL; 4) обязательно разграничение прав и доступов, то есть не со всех IP-адресов можно сделать запрос в базы ЕСИА и ЕБС, и только определенному кругу лиц [4, с. 334].

В отличие от банковского хранения информации, на сегодняшний день, к сожалению, невозможно обеспечить надежную защиту смартфонов, компьютеров, ноутбуков, которые используются пользователями для личных целей, от различных атак и вирусных программ. Несмотря на то что на устройствах могут устанавливаться антивирусные программы, остается риск угрозы взлома и получения необходимой информации третьим лицом. В связи с этим банки должны надлежащим образом информировать своих клиентов о том, что система интернет-банкинга, несмотря на ее совершенствование, не может гарантировать полную безопасность, остается риск угрозы ее взлома вирусной программой, и тогда банк не отвечает за такой случай. В отдельных случаях для проведения банковских операций через интернет-банкинг было бы целесообразно использовать какое-то отдельное устройство.

Необходимо отметить, что в определенных случаях виной завладения денежными средствами являются необдуманные действия самого клиента или слабая организация безопасности банком или кредитным учреждением. Во всех случаях несанкционированного списания денежных средств со счета клиента и решения вопроса ответственности банка или кредитной организации службе безопасности необходимо проанализировать ситуацию с несанкционированным списанием денежных средств и установить обстоятельства совершения данных действий с целью недопущения в будущем таких фактов, учета их при выработке методов защиты.

На данный факт указывает и судебная практика, в частности Верховным судом Республики Карелия было обосновано следующее: «Клиент должен получить гарантию от банка при получении банковской услуги, что его средства будут надежно защищены посредством дистанционного банковского обслуживания»[1]. Данное положение подразумевает, что банки несут полную ответственность за создание банковского продукта, который должен быть безопасным и исключать возможность несанкционированного доступа к клиентскому счету.

При установлении фактов недоработки со стороны банка всех необходимых условий создания безопасного использования услуг дистанционного банковского обслуживания обязанность по устранению данных фактов и компенсации материального ущерба возлагается на банк или иную коммерческую организацию, однако банк не отвечает за неосторожные действия клиента и не может такое гарантировать. Конечно, банковская

[1] Апелляционное определение Верховного суда Республики Карелия от 14.01.2014 по делу № 33-130/2014 [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 12.11.2020).

услуга может быть безопасной и должна быть таковой, но доступ к счету может быть и следствием неосторожных действий самого клиента. Совершение мошеннических действий со стороны третьих лиц только растет в это области. Сегодня это могут быть сайты-«двойники», на которых клиент по ошибке ввел свои данные, SMS-уведомления, прямые звонки с номеров, принадлежащих банкам (например, с номера 900), и т. п. Также часты случаи, когда клиент «привязывает» номер мобильного телефона к системе интернет-банкинга, а затем передает его другому лицу. В таких случаях банк не несет ответственность за причиненный ущерб, если он своевременно поставил клиента в известность о недопустимости таких действий с его стороны. Освобождение от гражданско-правовой ответственности для такого случая предусмотрено ст. 1098 ГК РФ.

Согласно данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) ЦБ РФ процент операций, совершенных без согласия клиентов с помощью методов социальной инженерии в результате побуждения клиента провести транзакцию или из-за злоупотребления доверием, в 2019 г. снизился до 69 % (в 2018 г. он составлял 97 %). В результате таких банковских операций с карт россиян было похищено почти 6,5 млрд руб. при «среднем чеке» 10 тыс. руб. [8]. Снижение числа несанкционированных списаний денежных средств со счетов клиентов банков в том числе обусловлено и предоставлением физическими лицами своих биометрических данных в ЕБС и дальнейшим активным использованием данной системы при проведении банковских операций.

В то же время необходимо отметить, что банк, кредитное учреждение будут нести ответственность в случае оказания услуг ненадлежащего качества, если они не соответствуют должному уровню безопасности, регламентированному и закрепленному в Стандарте Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»[1]. К мерам защиты на основании указанного документа относятся: защита платежной информации от искажения, возможность блокировать прием к исполнению распоряжений со стороны клиентов, доставка электронных «платежек» участникам обмена.

Оказание услуги интернет-банкинга в техническом плане является довольно специфическим, так как существуют определенные риски для

[1] Об утверждении Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения : распоряжение Банка России от 17.05.2014 № Р-399 СТО БР ИББС-1.0-2014 [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 03.10.2020).

пользователей такой услуги. В связи с этим возникает необходимость в специальном нормативном регулировании указанных правоотношений на законодательном уровне. Несмотря на то что Банком России даны определенные рекомендации в сфере информационной безопасности, их правоприменение на современном этапе затруднено. Банковские услуги, которыми можно пользоваться посредством интернет-банкинга, довольно разнообразны. Пользователь интернет-банкинга имеет возможность получения полного комплекса банковских услуг, которые предоставляются клиентам, приходящим в само банковское учреждение. При помощи услуг интернет-банкинга у пользователей есть возможность перевода средств со счета на счет, осуществления банковских платежей, оплаты коммунальных услуг. Клиенту интернет-банкинга не обязательно посещать офис – все операции он может осуществлять не выходя из дома, но существует и определенное исключение, то есть банковские услуги, предусматривающие расчетные операции, связанные с наличными средствами. Интернет-банкинг имеет массу важных для клиентов преимуществ: экономия времени (не нужно посещать банк лично), возможность управления собственными средствами в любое время суток.

При наличии перечисленных положительных моментов, связанных с использованием интернет-банкинга, не стоит отрицать и тот факт, что любая система может дать сбой. Однако система интернет-банкинга оснащена мощной защитой, а функциональность расчетных операций является практически идеальной, то есть риск возникновения сбоев и ошибок минимизирован, но все же присутствует. Важным элементом безопасности при пользовании услугами интернет-банкинга выступает подтверждение финансовых операций посредством разового пароля. Для того чтобы существенно уменьшить потенциальные риски банков в рассматриваемой сфере, стоит объединить подходы и требования регуляторов к обеспечению необходимого уровня безопасности систем интернет-банкинга.

На основании изложенного авторы предлагают в качестве основного направления формирования современного правового регулирования банковской деятельности по осуществлению банковских операций с использованием интернет-банкинга разработать и принять единый Закон «О дистанционном банковском обслуживании». В данном нормативно-правовом акте необходимо систематизировать все вопросы, касающиеся регулирования всех направлений дистанционного банковского обслуживания, в том числе и сети Интернет, и осуществления банковских операций с использованием интернет-банкинга.

Библиографический список

1. Брызгин А.А., Минбалеев А.В. Правовой режим биометрических персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 35–42.

2. Банк России дал прогноз по динамике кредитования в 2020 году. URL: https://www.banki.ru/news/lenta/?id=10923917.

3. Тулешов А. Онлайн-кредитование: основные тренды в России и в мире. URL: https://tuleshov.com/onlajn-kreditovanie-osnovnye-trendy-v-rossii-i-v-mire.

4. Шакер И.Е. Использование биометрической аутентификации и перспективы ее применения в банковской системе России // Экономика и управление. 2016. № 5. С. 83–89.

5. Берлин С.И.., Батори Г.А., Копылова Д.В. Биометрия в банковской сфере. Исследования вопроса безопасности хранения биометрических данных // Вестник Академии знаний. 2019. № 32 (3). С. 330–336.

6. Протасов П.А. Биометрия в банковской системе РФ // Вестник Томск. гос. ун-та. Сер.: Экономика. 2020. № 49. С. 141–148.

7. Мазуркевич Н.В., Петрович М.Ю. Биометрические технологии – инновационный механизм защиты от мошенничества в банковской сфере // Банковская система: устойчивость и перспективы развития : сб. науч. ст. Десятой междунар. науч.-практ. конф. по вопросам банковской экономики, Пинск, 25 окт. 2019 г. / редкол.: К.К. Шебеко [и др.] ; Мин-во образования Респ. Беларусь. Пинск : ПолесГУ, 2019. С. 124–128.

8. В ЦБ назвали сумму украденных средств с банковских карт россиян в 2019 году. URL: https://iz.ru/977900/2020-02-19/v-tcb-nazvali-summu-ukradennykh-sredstv-s-bankovskikh-kart-rossiian-v-2019-godu.

Дата поступления: 20.11.2020

THE UNIFIED BIOMETRIC SYSTEM AND UNIFIED SYSTEM OF IDENTIFICATION AND AUTHENTICATION AS TOOLS TO ENSURE THE SECURITY OF BANKING OPERATIONS USING THE INTERNET: LEGAL AND ORGANIZATIONAL ISSUES

KUZBAGAROV Muslim Nazargalievich
Candidate of Sciences (Law), Associate Professor, Assistant Professor of the Department of Law, North-Western Institute of Management of the Russian Presidential Academy of National Economy and Public Administration, Assistant Professor of the Department of Civil Law Disciplines, State Institute of Finance, Economics, Law and Technology, Saint-Petersburg, Russia.
E-mail: muslim_72@mail.ru

KUZBAGAROVA Elena Viktorovna
Candidate of Sciences (Law), Associate Professor, Assistant Professor of the Department of Forensic Expertise, St. Petersburg State University of Architecture and Civil Engineering, Saint-Petersburg, Russia.
E-mail: elenakuzbagarova@mail.ru

The paper is devoted to the organizational and legal issues of using the unified identification systems in various sectors of the economy, in particular in the banking sector. In the Russian Federation since 2011 the use of the unified identification and authentication system (ESIA) and since 2018 the use of the unified biometric system (EBS) has become one of the most promising areas in the activities of commercial banks and other subjects of the financial system. It is advisable to consider the active introduction of the EBS and ESIA into the banking sector as a tool for ensuring the security of banking transactions using the Internet, developed on the basis of modern engineering, technical and software developments. **Purpose:** to analyze the main directions of the use of the ESIA and EBS in the banking sector, to determine the existing organizational and legal issues arising in the practical activities of banks when implementing banking operations. **Methods:** the research is carried out on the basis of the methods of analysis and synthesis, generalization, comparison and a systematic approach. **Results:** based on the results of the study, the authors identify the existing organizational and legal issues arising in the practical activities of banks when carrying out banking operations using the Internet, and suggest ways to solve them.

Keywords: unified identification and authentication system; unified biometric system; personal data; banking operations; banking system of the Internet banking, legal regulation.

References

1. Bryzgin A.A., Minbaleev A.V. Legal regime of biometric personal data. *Vestnik UrFO. Bezopasnost' v informacionnoj sfere = Bulletin of the Ural Federal District. Information security*, 2012, no. 2 (4), pp. 35–42. (In Russian).

2. *Bank Rossii dal prognoz po dinamike kreditovaniya v 2020 godu* [The Bank of Russia gave a forecast for the dynamics of lending in 2020]. Available at: https://www.banki.ru/news/lenta/?id=10923917. (In Russian).

3. Tuleshov A. *Onlajn-kreditovanie: osnovnye trendy v Rossii i v mire* [Online lending: main trends in Russia and in the world]. Available at: https://tuleshov.com/onlajn-kreditovanie-osnovnye-trendy-v-rossii-i-v-mire. (In Russian).

4. SHaker I.E. The use of biometric authentication and the prospects for its application in the banking system of Russia. *Ekonomika i upravlenie = Economics and Management*, 2016, no. 5, pp. 83–89. (In Russian).

5. Berlin S.I.., Batori G.A., Kopylova D.V. Biometrics in banking. Research on the security of biometric data storage. *Vestnik Akademii znanij = Bulletin of the Academy of Knowledge*, 2019, no. 32 (3), pp. 330–336. (In Russian).

6. Protasov P.A. Biometrics in the banking system of the Russian Federation. *Vestnik Tomskogo gosudarstvennogo universiteta. Seriya: Ekonomika = Bulletin of the Tomsk State University. Series: Economics*, 2020, no. 49, pp. 141–148. (In Russian).

7. Mazurkevich N.V., Petrovich M.YU. Biometric technologies – an innovative anti-fraud mechanism in the banking sector. In SHebeko K.K. (ed.). *Bankovskaya sistema: ustojchivost' i perspektivy razvitiya* [Banking system: sustainability and development prospects]. Pinsk, PolesGU Publ., 2019, pp. 124–128. (In Russian).

8. *V CB nazvali summu ukradennyh sredstv s bankovskih kart rossiyan v 2019 godu* [The Central Bank named the amount of funds stolen from bank cards of Russians in 2019]. Available at: https://iz.ru/977900/2020-02-19/v-tcb-nazvali-summu-ukradennykh-sredstv-s-bankovskikh-kart-rossiian-v-2019-godu. (In Russian).

Received: 20.11.2020