Вестник Башкирского института социальных технологий). 2024. № 1(62). С. 11–16
Vestnik BIST (Bashkir Institute of Social Technologies). 2024;1(62):11–16

ЭКОНОМИКА И МЕНЕДЖМЕНТ ПРЕДПРИЯТИЙ

Научная статья
УДК 004.056.5
doi: 10.47598/2078-9025-2024-1-62-11-16

БЛОКЧЕЙН-ТЕХНОЛОГИЯ КАК СРЕДСТВО ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Дина Владимировна Клюкина[1], Федор Константинович Романов[2]✉
[1,2]Академия труда и социальных отношений, Москва, Россия
[1]falileeva142@mail.ru
[2]romanov.f.k.98@gmail.com✉

Аннотация. В современном мире каждый из нас неразделим с его персональными данным, которые по своей сути являются отражением человека в информационных процессах. Получение государственных, медицинских или банковских услуг, покупки через интернет и многое другое невозможно представить без использования персональных данных. Учитывая это, крайне остро встает вопрос о защите таких данных. Целью научной статьи является описание блокчейн-технологии и рассмотрение перспектив ее применения для защиты персональных данных. Особое внимание уделено последствиям от утечек или краж персональных данных. Кроме того, в статье описаны существующие наработки по практическому применению технологии блокчейн в сфере обеспечения защищенности персональных данных.
Ключевые слова: персональные данные, информационная безопасность, защита персональных данных, утечка персональных данных, кража персональных данных, блокчейн-технология, хранение информации, обработка информации
Для цитирования: Клюкина Д. В., Романов Ф. К. Блокчейн-технология как средство защиты персональных данных // Вестник БИСТ (Башкирского института социальных технологий). 2024. № 1 (62). С. 11–16. https://doi.org/10.47598/2078-9025-2024-1-62-11-16.

ECONOMY AND ENTERPRISE MANAGEMENT

Research article

BLOCKCHAIN TECHNOLOGY AS A MEANS OF PROTECTING PERSONAL DATA

Dina V. Klyukina[1], Fedor K. Romanov[2]✉
[1,2]Academy of Labor and Social Relations, Moscow, Russia
[1]falileeva142@mail.ru
[2]romanov.f.k.98@gmail.com✉

Abstract. In the modern world, each of us is inseparable from his personal data, which is essentially a reflection of a person in information processes. Obtaining government, medical or banking services, online shopping and much more is impossible to imagine without the use of personal data. Given this, the issue of protecting such data is extremely acute. The purpose of scientific article is to describe blockchain technology and consider the prospects of its application for the protection of personal data. Special attention is paid to the consequences of personal data breach. In addition, the article describes the existing developments on the practical application of blockchain technology in the personal data safeguard.
Keywords: personal data, information security, personal data protection, personal data leakage, personal data theft, blockchain technology, information storage, information processing

For citation: Klyukina D. V., Romanov F. K. Blockchain technology as a means of protecting personal data. *Vestnik BIST (Bashkirskogo instituta social`ny`x texnologij) = Vestnik BIST (Bashkir Institute of Social Technologies).* 2024;1(62):11–16. (In Russ.). https://doi.org/10.47598/2078-9025-2024-1-62-11-16.

Обеспечение информационной безопасности является одним из фундаментальных условий функционирования общества, особенно на современном этапе развития. Вовлечение человека в современные общественные и экономические процессы обеспечивается за счет персональных данных. Персональные данные, если опираться на законодательство Российской Федерации, представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу [1]. Очевидным является тот факт, что информационное общество является крайне уязвимым в силу наличия большого числа потенциальных и реализуемых угроз безопасности данных. Это же касается и персональных данных. Хищение и неправомерное использование таких данных влекут за собой крайне негативные последствия как для физических лиц, так и для организаций. Именно поэтому проблема защиты персональных данных на сегодняшний день является чрезвычайно актуальной, а разработке и внедрению все более эффективных средств защиты уделяется все больше внимания.

Ознакомившись с определением персональных данных, изложенном в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», можно сказать, что нормативно-правовая база Российской Федерации трактует данное понятие крайне широко [1]. Суды к персональным данным относят фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, информацию о количестве принадлежащих лицу акций и другую информацию. Однако стоит обратить внимание на то, что к персональным данным с точки зрения отечественного законодательства относится исключительно та информация, что в отдельности или в совокупности достоверно указывает на конкретное определяемое лицо [2].

Согласно аналитическому отчету компании «InfoWatch», занимающейся разработкой решений в сфере кибербезопасности, в 2022 году общее число утекших записей персональных данных и платежной информации в России составило 667,7 млн, что на 167,2% больше, чем в 2021 году [3, с. 6]. При этом в сравнении с 2018 годом, данный показатель вырос более чем в 23 раза.

Для большего понимания значимости деятельности по обеспечению безопасности персональных данных важно рассмотреть негативные последствия, возникающие вследствие реализации угроз.

В первую очередь, утечки или кражи персональных данных оказывают негативное воздействие на обычных граждан — субъектов персональных данных. При самом оптимистичном сценарии, вследствие неправомерного получения злоумышленниками личной информации человека, субъект персональных данных сталкивается с неприятными, но не приносящими экономический ущерб последствиями, к которыми чаще всего относятся недобросовестная реклама, транслируемая через личные звонки, в сообщениях, в различных мессенджерах и социальных сетях или через массовые рассылки с использованием электронной почты. Однако, к сожалению, использование злоумышленниками персональных данных может привести к более печальному исходу, способному сказаться на благополучии физического лица. Так мошенники, получив в свои недобросовестные руки личную информацию, могут использовать ее для взятия различных займов от лица субъекта персональных данных, учреждать так называемые организации «однодневки», используемые чаще всего для отмывания денежных средств, совершать незаконные сделки с недвижимостью, получать доступ к банковским приложениям, картам и счетам, открывать счета и электронные кошелки, которые в последующем могут быть задействованы в незаконной деятельности. Также злоумышленники могут совершать мошеннические действия от лица, чьи данные были похищены, применять персональные данные как средство шантажа или вымогательства. Все эти незаконные действия в конечном

итоге приводят к финансам потерям законопослушного человека.

Для дальнейшего освещения данной проблемы следует привести такое понятие, как оператор персональных данных. Согласно Федеральному закону «О персональных данных» оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными [1]. Данный Федеральный закон является основополагающим нормативно-правовым документом, регулирующим работу с персональными данными, обязанности операторов и, конечно же, определяет ответственность за нарушения. Исходя из этого, можно сделать вывод о том, что одним из основных последствий утечки персональных данных для операторов является необходимость отвечать перед законом. На сегодняшний день лица и организации, допустившие утечку персональных данных, несут административную ответственность согласно ч. 2 ст. 13.11 «Кодекса Российской Федерации об административных правонарушениях». В данном случае административный штраф на граждан составляет от 6 до 10 тыс. руб., на должностных лиц — от 20 до 40 тыс. руб., на юридических лиц — от 30 до 150 тыс. руб. [4]. Кроме необходимости уплаты относительно небольшого по своему размеру штрафа, компании, которые в большинстве своем представляют подавляющие число операторов персональных данных, в случае реализации угрозы персональным данным также несут прямые финансовые потери. Такие потери могут быть обусловлены выплатами компенсаций субъектам персональных данных, необходимостью затрат на расследование инцидента, связанного с утечкой данных, затратами на восстановление правомерного режима работы с персональными данными, вложениями в усовершенствование оборудования и программного обеспечения, невозможностью в полной мере выполнять свои обязательства перед контрагентами. Помимо прямых финансовых потерь организации, допустившие утечку персональных данных, могут потерять свою репутацию, что в свою очередь может привести к потере клиентов, партнеров, падению конкурентоспособности и зачастую снижению стоимости активов.

По данным исследования подразделения компании «IBM» «IBM Security» и исследовательского института «Ponemon» средний ущерб от утечек персональных данных в мире в 2020 году составил 4,35 млн долл. США [5, с. 5].

Способы хищения персональных данных могут быть крайне разнообразны, все зависит от конкретной организации, способов хранения и обработки информации и от средств обеспечения информационной безопасности. Однако существует два основных источника для получения незаконным путем персональных данных: кибератаки и действия инсайдеров. При этом, так называемые инсайдеры или сотрудники организаций, могут быть причиной утечки личной информации как вследствие непреднамеренных действий, так и умышленно. При этом, как отмечают эксперты, в государственном секторе работники являются основным каналом утечки данных [6].

Как уже отмечалось, проблема обеспечения защиты персональных данных является крайне актуальной. Способы неправомерного получения личной информации становятся все более изобретательными, вследствие чего перед организациями встает вопрос об усовершенствовании средств защиты. Не углубляясь в наиболее распространенные средства защиты персональных данных, стоит отметить, что для данной цели применяются организационные и технические меры по обеспечению безопасности персональных данных. Такие меры воздействует на два основных аспекта работы с персональными данными: обработку и хранение [7]. И само собой, для обеспечения безопасности личной информации используются различные технические средства.

Одной из наиболее перспективных и современных технологий, которая может быть использована для защиты персональных данных является блокчейн. Простыми словами, блокчейн (англ. *blockchain* — цепочка блоков) представляет собой технологию, которая позволяет

сохранять и передавать данные в виде последовательности связанных блоков [8]. Блок в свою очередь представляет собой единицу хранения информации, ячейку, в которой могут храниться в том числе и персональные данные. Вся информация в блоках зашифрована и представляет собой определенный набор символов, именуемый хэшем. Повторимся, структура блокчейна представляет собой последовательность или цепочку блоков, связанных между собой ссылкой, содержавшейся в каждом блоке и указывающей на предыдущий. Тем самым обеспечивается один из фундаментальных принципов функционирования блокчейн-технологии — принцип неизменяемости. Данный принцип состоит в невозможности изменить данные, так сказать, задним числом, поскольку это потребует изменения каждого блока в цепочке.

Помимо вышеуказанного распределенная или децентрализованная архитектура построения систем на основе блокчейн-технологии имеет принципиальную ценность в целях обеспечения защиты персональных данных. Благодаря такому принципу построения, хранение и обработка данных осуществляются не через один единый центр, а через распределенную сеть нескольких узлов системы, говоря простым языком, компьютеров. Таким образом обеспечивается целостность и устойчивость хранилища персональных данных от различных кибератак в силу того, что персональные данные хранятся на различных устройствах [9].

Такой вариант применения блокчейн-технологии в целях защиты персональных данных является самым очевидным и простым. Наибольший же интерес представляет разрабатываемая такими гигантами цифровой индустрии как «IBM» и «Microsoft» новая парадигма управления персональными данными, основанная на блокчейн-технологии.

Децентрализованная идентификация (англ. *Decentralized identity — DID*) — это совершенно новый подход к управлению и защите персональных данных. DID основывается на индивидуальном владении персональными данными. Это означает, что вся личная информация в цифровом виде хранится непосредственно на личных устройствах субъектов персональных данных [10]. Само собой, технологическим фундаментом такого подхода является блокчейн-технология.

Рассмотрим подробнее, как DID может быть реализована на практике. Как уже было сказано ранее, все персональные данные хранятся на личных устройствах их владельцев. При этом все устройства субъектов и операторов персональных данных обращены в децентрализованную сеть на основе блокчейна. Субъект самостоятельно инициирует передачу своей личной информации оператору персональных данных. Таким образом, у людей появляется возможность полностью контролировать передачу персональных данных кому-либо, благодаря чему пропадает необходимость доверять операторам в вопросе сохранности своих данных. При этом личная информация будет храниться под защитой, обеспеченной методами криптографического шифрования.

Говоря о DID, важно рассмотреть преимущества, которые она может дать. Для обычных людей возможность самостоятельно хранить и контролировать передачу своих данных избавляет от необходимости доверять операторам персональных данных в вопросе сохранности своей личной информации. Поскольку все персональные данные хранятся непосредственно у их владельцев, для организаций особую ценность представляет возможность сокращения затрат на создание, поддержание работоспособности и усовершенствование технических средств хранения, обработки и защиты информации. Кроме того, DID способна упростить для поставщиков товаров и услуг процедуру «знай своего клиента» (англ. *Know Your Customer — KYC*), тем самым сократить расходы на верификацию клиентов и партнеров. Государству в свою очередь децентрализованная идентификация вместе с развитием цифровых документов позволит создать эффективную и строго стандартизированную систему выдачи, обновления, изъятия и проверки различных удостоверяющих документов.

На сегодняшний день государственные институты и бизнес занимаются разработкой и внедрением локальных решений по защите персональных данных. Развитие децентрализованной идентификации хотя бы на национальном уровне потребует кооперации

различных участников и активного вовлечения в данный процесс государства.

Помимо вышесказанного, по мнению авторов, самым же существенным препятствием для внедрения блокчейн-технологии с целью защиты персональных данных, говоря о Российский Федерации, является необходимость переработки нормативно-правовой базы. Основная проблема в данном контексте заключается в строго регламентированных принципах обработки персональных данных. Поскольку блокчейн-технология является инновационной, не всегда имеется возможность адаптировать принципы ее работы к принципам, изложенным в Федеральном законе «О персональных данных».

Подводя итоги, отметим, что блокчейн-технология является крайне перспективной с точки зрения ее приспособления для обеспечения защиты персональных данных. Безопасность персональных данных представляет собой одну из наиболее значимых проблем современного информационного общества, и работа по созданию более эффективных средств и методов защиты персональных данных ведется непрерывно, представляя миру новые решения, в том числе основанные и на блокчейне.

Список источников

1. «О персональных данных» : Федеральный закон от 27.07.2006 N 152-ФЗ : последняя редакция // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=lovhelga6k558595471

2. Что относится к персональным данным? Являются ли государственный регистрационный знак и адрес владельца персональными данными? // ГАРАНТ.РУ : Информационно-правовой портал. URL: https://www.garant.ru/consult/civil_law/1622422/?ysclid=lopr0bfrlk381642666. Дата публикации: 03.05.2023.

3. Россия: утечки информации ограниченного доступа в 2022 г. // InfoWatch : сайт. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf?ysclid=lops6ucl7y397651242. Дата публикации: 17.04.2023.

4. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=lopticwtlf747464538

5. Fight back against data breaches // IBM : сайт. URL: https://www.ibm.com/reports/data-breach

6. Утечка информации в государственных учреждениях // Блог «Solar Dozor». URL: https://rt-solar.ru/products/solar_dozor/blog/3022/?ysclid=lolhkxefw5932739048. Дата публикации: 22.09.2022.

7. Трубачева С. И. Основные аспекты защиты персональных данных на предприятии // Вестник Волжского университета им. В. Н. Татищева. 2010 г. URL: https://cyberleninka.ru/article/n/osnovnye-aspekty-zaschity-personalnyh-dannyh-na-predpriyatii

8. Связанные одной цепью: как блокчейн защищает данные // Блог «Яндекс Практикум». URL: https://practicum.yandex.ru/blog/chto-takoe-blokchain-i-kak-eto-rabotaet. Дата публикации: 27.06.2023.

9. Козин И. С. Метод обеспечения безопасной обработки персональных данных на основе применения технологии блокчейн // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19, № 5. С. 892–900.

10. Stanton Heister, Kristi Yuthas. How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity // Intechopen.com : сайт. URL: https://www.intechopen.com/chapters/75936. Дата публикации: 25.03.2021.

References

1. “On Personal Data”: Federal Law dated July 27, 2006 No. 152-FL: latest edition. ConsultantPlus: site. (In Russ.). Available from: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=lovhelga6k558595471

2. What is personal data? Are the state registration plate and address of the owner personal data? GARANT.RU: Information and legal portal. (In Russ.) Available from: https://www.garant.ru/consult/civil_law/1622422/?ysclid=lopr0bfrlk381642666/. Publication date: May 3, 2023.

3. Russia: leaks of restricted access information in 2022. InfoWatch: site. (In Russ.) Available from: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf?ysclid=lops6ucl7y397651242. Publication date: April 17, 2023.

4. “Code of the Russian Federation on Administrative Offenses” dated December 30, 2001 No. 195-FL. ConsultantPlus: site. (In Russ.). Available from: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=lopticwtlf747464538

5. Fight back against data breaches. IBM: site. URL: https://www.ibm.com/reports/data-breach

6. Leakage of information in government institutions. Blog “Solar Dozor”. (In Russ.). Available from: https://rt-solar.ru/products/solar_dozor/blog/3022/?ysclid=lolhkxefw5932739048. Publication date: September 22, 2022.

7. Trubacheva S. I. Main aspects of personal data protection at an enterprise. *Vestnik Volzhskogo universiteta im. V. N. Tatishheva = Bulletin of the Volga University named after. V. N. Tatishchev.* 2010. (In Russ.). Available from: https://cyberleninka.ru/article/n/osnovnye-aspekty-zaschity-personalnyh-dannyh-na-predpriyatii

8. Connected by one chain: how blockchain protects data. Yandex Practice Blog. (In Russ.). Available from: https://practicum.yandex.ru/blog/chto-takoe-blokchain-i-kak-eto-rabotaet. Publication date: 06/27/2023.

9. Kozin I. S. Method for ensuring secure processing of personal data based on the use of blockchain technology. *Nauchno-texnicheskij vestnik informacionny`x texnologij, mexaniki i optiki = Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*. 2019;19(5):892–900.

10. Stanton Heister, Kristi Yuthas. How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity. Intechopen.com: site. Available from: https://www.intechopen.com/chapters/75936. Publication date: March 25, 2021.

Информация об авторах

Д. В. Клюкина — кандидат экономических наук, доцент;

Ф. К. Романов — аспирант.

Information about authors

D. V. Klyukina — Candidate of Science (Economics), Associate Professor;

F. K. Romanov — a postgraduate student.

Статья поступила в редакцию 23.01.2024; одобрена после рецензирования 15.02.2024; принята к публикации 25.03.2024.

The article was submitted 09.01.2024; approved after reviewing 15.02.2024; accepted for publication 25.03.2024.