

ҚАЗІРГІ ЖЕКЕ ҚҰҚЫҚТЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ
АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОГО ЧАСТНОГО ПРАВА
ACTUAL PROBLEMS OF MODERN PRIVATE LAW
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С ПРИМЕНЕНИЕМ
ТЕХНОЛОГИИ БЛОКЧЕЙН: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРАВОВОГО
РЕГУЛИРОВАНИЯ

*Ильясова Г.А., к.ю.н., профессор-исследователь, Карагандинский Университет
им. академика Е.А.Букетова*

Актуальность темы исследования заключается в том, что защита прав и свобод человека и гражданина при сборе и обработке его персональных данных является не только проблемой одного государства, это проблема мирового масштаба. Поскольку, нарушается право на неприкосновенность частной жизни, в том числе информационное прайвеси, касающееся регулирования сбора и обработки персональных данных, гарантированное Всеобщей Декларацией прав человека, Международным пактом о гражданских и политических правах.

В Республике Казахстан недавно были приняты поправки в законодательство по вопросам информационной безопасности, и они направлены на совершенствование действующего законодательства, введены в закон дополнительные меры защиты персональных данных. Однако, считаем, что законодательные акты не полностью регламентируют правовой механизм обеспечения защиты персональных данных и не соответствуют международным актам, не учитывает теоретические положения регламентации отдельных правовых институтов.

Риски в виде утери данных граждан РК встречались в 2017 году при нарушении правил хранения и утилизации документов, содержащих персональные данные клиентов Qazkom банка, в 2019 году утечки личных данных казахстанцев из баз ЦИК и Генеральной прокуратуры, передачи данных третьим лицам из Медицинской информационной системы «Damimed» и т.д.

По результатам ежегодно проведенных социологических опросов с 2018 по 2023 годы среди граждан в возрасте 18 лет и старше в целях определения уровня осведомленности населения об угрозах информационной безопасности – уровень осведомленности граждан удовлетворительный. Показатели составили за 2018 год – 62,9%, за 2019 год – 73,5%, за 2020 год – 78%, за 2021 год – 75,0%, за 2022 год – 77,4%, за 2023 год – 80,4% [1].

Рисунок 1. Уровень осведомленности граждан об угрозах информационной безопасности с 2018 по 2023 годы



Несмотря на такие показатели, из-за утечки персональных данных граждане чаще стали жертвами мошенников, от имени граждан в банках были получены множество кредитов. По данным МВД РК за последние семь лет более чем в 10 раз выросло количество случаев интернет-мошенничества. Такие преступления составляют 19% от общего количества

зарегистрированных в 2023 году преступлений и 50% от всех мошенничеств. И только за 2023 год причиненный гражданам ущерб составил 21 млрд тенге. При этом, около половины всех эпизодов мошенничества в последние три года совершаются онлайн [2]. Правоохранительные органы не могут эффективно бороться с киберпреступностью.

Следует отметить следующие важные нормативно-правовые акты, регламентирующие правоотношения по сбору, обработке и хранению персональных данных.

- Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года [3];

- Закон Республики Казахстан «О дактилоскопической и геномной регистрации» от 30 декабря 2016 года № 40-VI ЗРК [4];

- Концепция кибербезопасности («Киберщит Казахстана») утверждена постановлением Правительства РК от 30 июня 2017 года №407 [5];

- «Об утверждении Национального плана развития Республики Казахстан до 2025 года». Указ Президента Республики Казахстан от 15 февраля 2018 года № 636 [6].

- Об утверждении Концепции правовой политики Республики Казахстан до 2030 года. Указ Президента Республики Казахстан от 15 октября 2021 года № 674.

- «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы». Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 [7].

Международные правовые акты в сфере обработки и защиты персональных данных:

- Конвенции о защите физических лиц при автоматизированной обработке персональных данных ETS №108 (Страсбург, 28 января 1981 года) [8]. Казахстан не является участником данного международного акта.

Принят Общий регламент по защите данных General Data Protection Regulation (GDPR) Директива ЕС (2016 г.). GDPR усиливает существующие и вводит новые права гражданам ЕС, а также дает гражданам больше контроля над своими личными данными [9]. GDPR гарантирует физическим лицам право контроля над их персональными данными,

В современный период эффективным инструментом обеспечения безопасности персональных данных может стать технология блокчейн.

Блокчейн (blockchain - цепочка блоков) - цепочки взаимосвязанных блоков данных.

То есть это цифровой реестр или база данных, эти данные распределены по всем компьютерам пользователей.

Каждый блок в блокчейне содержит хеш предыдущего блока, поэтому создается надежная цепочка блоков.

В Законе Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК дано следующее определение блокчейна: это «информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования» (статья 1 пункт 38-2) [10].

Различают три типа сетей блокчейна.

Публичный блокчейн — это открытая децентрализованная сеть, доступная всем желающим. Обычно такие сети используют открытый исходный код, действуют прозрачно и не требуют доверия, то есть получить к ним доступ и использовать их может кто угодно. Примерами публичных блокчейнов являются Биткоин и Ethereum.

Приватный блокчейн, как следует из названия, — это закрытая сеть блокчейна. Обычно она находится под контролем одной организации и используется для ее целей и способов применения.

Приватные блокчейны контролируют доступ и устанавливают правила, которые определяют, кто может видеть и записывать транзакции в блокчейне. Они не являются децентрализованными, поскольку в них действует четкая иерархия управления. Однако они могут быть распределенными и поручать многим нодам хранить копию блокчейна на своих компьютерах.

Блокчейн-консорциум — это гибрид публичного и приватного блокчейнов. В блокчейн-консорциуме несколько организаций объединяются для создания общей сети блокчейна, которая управляется и контролируется совместно. В зависимости от потребностей участников такие сети могут быть как открытыми, так и закрытыми.

В отличие от открытой системы, где проверять блоки может любой пользователь, или закрытой системы, где создателей блоков выбирает одна организация, в блокчейн-консорциуме валидаторами выступают несколько одинаково влиятельных сторон [11].

Преимущества технологии блокчейн для защиты данных.

Технология блокчейн предлагает несколько значительных преимуществ в области защиты данных, которые делают ее привлекательной для использования в этом контексте:

Конфиденциальность: Блокчейн обеспечивает высокий уровень конфиденциальности путем шифрования данных и управления доступом к ним. Персональные данные могут быть доступны только тем, кому это разрешено, что снижает риск утечек.

Неизменность данных: Информация, размещенная в блокчейне, не может быть изменена без согласия всех участников сети. Это гарантирует целостность информации, что особенно важно для персональных данных.

Децентрализация: Блокчейн не имеет центрального управления, что делает его менее уязвимым для хакерских атак, поскольку злоумышленники должны были бы взломать множество устройств одновременно.

Прозрачность: Все транзакции в блокчейне являются открытыми и доступными для просмотра всех участников. Это обеспечивает прозрачность и возможность проверки всех действий, что способствует доверию.

Безопасные транзакции: Благодаря использованию криптографии и децентрализации, транзакции с персональными данными могут быть выполнены без участия посредников, что снижает риск хакерских атак.

Устойчивость к отказам: Блокчейн-сети продолжают работать, даже если часть узлов выходит из строя, что делает их надежными и устойчивыми к сбоям.

Безопасность: Сильное шифрование и электронные подписи делают транзакции в блокчейне безопасными и защищенными.

В децентрализованной сети блокчейна нет центрального органа или посредника, контролирующего поток данных или транзакций. Технология блокчейна позволяет совершать прозрачные транзакции, которые проверяются и подтверждаются самими участниками сети без навязанных посредников с помощью электронных цифровых подписей. Личная информация будет храниться под защитой, обеспеченной методами криптографического шифрования. Например, вместо того, чтобы вводить логин и пароль, пользователь может использовать свой цифровой ключ, который будет храниться в блокчейне.

В блокчейне можно создать систему, которая будет контролировать доступ к информации и отслеживать все изменения. Это позволит быстро обнаруживать и предотвращать утечки данных, а также установить ответственность за них.

После того как данные о транзакции формируются в блоки, они проходят криптографическую верификацию и записываются в базу данных. Вся информация, связанная с технологией блокчейн, хранится в хорошо защищенной децентрализованной сети. Доступ к ней открывается с помощью специальных криптографических ключей. Благодаря этому, подделать информацию, которая хранится в сети, нельзя.

Эти преимущества делают технологию блокчейн мощным инструментом для защиты данных, включая персональные данные, и объясняют ее растущую популярность в этой области.

Проблемы применения технологии блокчейн для обеспечения защиты персональных данных.

1. Дорогая технология и программа, защита блокчейна от различных кибератак.

Использование блокчейна для хранения данных, также защита блокчейна от различных кибератак, гораздо дороже использования других типов баз данных.

2. После добавления данных их очень сложно изменить и удалить.

При использовании любых типов баз данных необходимо соблюдение требований законодательства, действующего на территории конкретного государства. Например, при сборе и обработке персональных данных лиц, находящихся на территории Европейского Союза необходимо обеспечить соблюдение GDPR (General Data Protection Regulation). Принцип работы блокчейна может привести к нарушению многих правил и требований защиты персональных данных, предусмотренных GDPR, так как:

- персональные данные часто передаются через государственные границы, но при этом не всегда возможно соблюдение требований GDPR к трансграничной передаче данных;
- неправильные или устаревшие данные невозможно исправить (право на исправление);
- обработка данных не прекращается по достижении целей обработки (принцип минимизации и право на возражение);
- данные невозможно удалить ("право на уничтожение персональных данных"). В соответствии с Регламентом Европейского Союза и национальным законодательством существует возможность обратиться к контролирующему органу с требованием уничтожения персональных данных. Однако, данное положение неприменимо к средствам, основанным на блокчейн-технологии, поскольку эта технология характеризуется неизменностью и сохраняет первоначальную информацию для гарантии целостности данных.

3. Хранение.

Реестры блокчейна могут сильно увеличиться со временем. В настоящее время блокчейн Биткойна требует около 200 ГБ дискового пространства. Увеличение размера блокчейна, очевидно, опережает увеличение емкости жестких дисков, и сеть рискует потерять ноды, если реестр станет слишком большим для загрузки и хранения пользователями.

4. Нехватка IT специалистов.

Несмотря на конфликт блокчейна с правами по защите данных, все так и технология блокчейн развивается, и, надеемся, она в будущем будет развиваться в соответствии с законодательством. Эксперты полагают, что создание частного блокчейна может сделать его совместимым с законодательством. Частная или разрешенная система, также называемая закрытой системой, не использует открытые ноды для сохранения данных. Вместо этого они хранят информацию на локальных машинах. Таким образом, легче удалить информацию по чьей-либо просьбе

Таким образом, с точки зрения безопасности хранения персональных данных, блокчейн является целесообразным и эффективным решением, однако при этом необходимо учитывать экономические аспекты и правовые ограничения, которые накладывает технология.

Опыт зарубежных стран по обеспечению защиты персональных данных с помощью технологии блокчейн.

Швейцария. Швейцарские медицинские учреждения применяют блокчейн для хранения медицинских данных пациентов. Это позволяет пациентам иметь полный контроль над своими данными и обеспечивает их конфиденциальность.

США. В Соединенных Штатах блокчейн нашел применение в банковской сфере. Здесь он используется для обеспечения безопасности финансовых транзакций и защиты личных данных клиентов.

Великобритания. Блокчейн также используется для усиления безопасности и прозрачности в сфере образования, особенно при проверке академических достижений и выдаче дипломов.

Германия. В Германии блокчейн активно применяется в здравоохранении для создания электронных здравоохранительных записей (EHR), где пациенты могут контролировать доступ к своим медицинским данным и делиться ими с врачами по необходимости.

Швеция. Шведское правительство использует блокчейн для регистрации земельных прав и недвижимости, что повышает прозрачность и уменьшает возможность мошенничества в этой сфере.

Канада. В Канаде проводятся исследования по использованию блокчейна для обеспечения безопасности источников воды и контроля за их качеством, что имеет большое значение для общественного здоровья.

Австралия. Блокчейн применяется в австралийском правительстве для обеспечения целостности и прозрачности бюджетных транзакций и расходов государства.

Чтобы обеспечить максимальную безопасность защиты персональных данных, думаем, необходимо применить современные инновационные технологии - технологию блокчейн, которая не использует централизованное хранилище или сервер. осуществляет все транзакции через децентрализованную систему между каждым участником лично, подключенную к одной сети блокчейн.

Правовые аспекты использования технологии блокчейн в зарубежных странах.

Регулирование данных. Страны, такие как Германия и Швеция, строго регулируют хранение и передачу персональных данных. При использовании блокчейна для хранения и обработки таких данных, необходимо соблюдать соответствующие нормы безопасности данных и приватности.

Смарт-контракты. США и Великобритания разрабатывают законодательство и нормы для смарт-контрактов, которые являются ключевым элементом блокчейн-платформ. Это включает в себя признание смарт-контрактов как правовых документов и регулирование их исполнения.

Финансовое регулирование. Многие страны смотрят на блокчейн в контексте финансовых операций и криптовалютного рынка. Поэтому, они разрабатывают законодательство для регулирования криптовалютных обменов, ICO (Initial Coin Offerings) и соблюдения AML (Anti-Money Laundering) и KYC (Know Your Customer) правил.

Земельные права. В случае использования блокчейна для регистрации земельных прав, как в Швеции, необходимо создать законодательные рамки для признания электронных записей блокчейна в качестве юридически обязательных документов.

Общественные консультации. В некоторых случаях, внедрение блокчейна важно согласовать с общественностью и законодательными органами, чтобы обеспечить прозрачность и доверие.

Германия. Закон о защите данных (BDSG) и Общее правило по защите данных ЕС (GDPR) регулируют обработку персональных данных. При использовании блокчейна для хранения и обработки таких данных необходимо соблюдать эти нормы.

Смарт-контракты и их правовой статус еще активно обсуждаются в контексте германского права.

Швеция. Закон о персональных данных (Personuppgiftslagen) и Закон о медицинской информации (Patientdatalagen) регулируют обработку медицинских и персональных данных. При использовании блокчейна в здравоохранении, необходимо соблюдать вышеуказанные законы.

Регистрация земельных прав с использованием блокчейна также требует законодательной поддержки.

США. Федеральное и штатное законодательство регулирует использование блокчейна в различных областях, включая финансы, страхование и здравоохранение.

SEC (Комиссия по ценным бумагам и биржам) и CFTC (Комиссия по торговле товарными фьючерсами) разрабатывают правила для криптовалют и ICO.

Смарт-контракты и их юридический статус обсуждаются на уровне штатов и федерального правительства.

Великобритания. GDPR применяется в Великобритании, и она разрабатывает свои нормативные акты для адаптации к этому закону. Британский правительственный орган, Her

Majesty's Land Registry, рассматривает блокчейн для регистрации земельных прав и работает над законодательной базой для этого.

Австралия. Австралийское законодательство о защите данных требует соблюдения стандартов конфиденциальности при использовании блокчейна. Финансовые организации подвержены регулированию со стороны Австралийской комиссии по ценным бумагам и инвестициям (ASIC) и других финансовых регуляторов.

Заклучение

В заключение можно сказать, что технология блокчейн играет важную роль в защите персональных данных и обеспечении безопасности в различных аспектах жизни и бизнеса.

Преимущества блокчейна в области защиты данных включают в себя безопасное хранение и передачу информации, невозможность фальсификации данных и улучшение прозрачности.

В целом, блокчейн представляет собой эффективную технологию для защиты персональных данных, и его роль в этой области будет продолжать расти по мере развития технологии.

Статья подготовлена в рамках выполнения научного исследования по заказу Комитета науки Министерства науки и высшего образования Республики Казахстан грантового финансирования по научным и (или) научно-техническим проектам на 2023-2025 годы по теме проекта ИРН 19679658 «Правовое регулирование применения технологии блокчейн в Республике Казахстан: теория и практика».

Список литературы

1 Вопросы обеспечения кибербезопасности. Рекомендации - [Электронный ресурс]. - Режим доступа: <https://www.gov.kz/memleket/entities/mdai/press/article/details/109499?lang=ru>

2 Кудряшова О. Утечка персональных данных казахстанцев: какими последствиями это чревато для граждан. 07.03.2024 г. // [Zakon.kz](https://www.zakon.kz/finansy/6426850-utechka-personalnykh-dannykh-kazakhstantsev-kakimi-posledstviyami-eto-chrevato-dlya-grazhdan.html) - [Электронный ресурс]. - Режим доступа: <https://www.zakon.kz/finansy/6426850-utechka-personalnykh-dannykh-kazakhstantsev-kakimi-posledstviyami-eto-chrevato-dlya-grazhdan.html>

3 О персональных данных и их защите. Закон Республики Казахстан от 21 мая 2013 года N 94-V. - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/Z1300000094>

4 О дактилоскопической и геномной регистрации. Закон Республики Казахстан от 30 декабря 2016 года № 40-VI ЗРК. - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/Z1600000040>

5 Концепция кибербезопасности («Киберщит Казахстана») утверждена постановлением Правительства РК от 30 июня 2017 года №407 - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/P1700000407>

6 Об утверждении Национального плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан. Указ Президента Республики Казахстан от 15 февраля 2018 года № 636. - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/U1800000636>

7 Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269. - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/P2300000269>

8 Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января, 1981 г.) (с изменениями от 15 июня 1999 г.) - [Электронный ресурс]. - Режим доступа: https://online.zakon.kz/Document/?doc_id=1034061&pos=1;-12#pos=1;-12

9 Общий регламент по защите данных General Data Protection Regulation (GDPR). Постановление 2016/679 - [Электронный ресурс]. - Режим доступа: <https://ogdpr.eu/ru>

10 Об информатизации. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК. - [Электронный ресурс]. - Режим доступа: <https://adilet.zan.kz/rus/docs/Z1500000418>

11 Что такое блокчейн и как он работает. - [Электронный ресурс]. - Режим доступа: <https://academy.binance.com/ru/articles/what-is-blockchain-and-how-does-it-work>

CURRENT TRENDS IN THE DEVELOPMENT OF ENVIRONMENTAL LAW IN GLOBALIZATION

Bondar I. A., Ph.D. of Economics, Associate Professor, Head of the Department of Aviation Management Flight Academy of the National Aviation University, Kropyvnytskyi, Ukraine

Shvydanenko D.V., head of the sector of economic research of the Department of the National Institute of Public Health and the Kirovohrad Scientific Research Unit, expert forensic center of the Ministry of Internal Affairs of Ukraine, Kropyvnytskyi, Ukraine

The modern world is at a crossroads where the development of society is inevitably intertwined with the growth of environmental challenges. Above all, globalization appears to be a determining factor influencing the development of environmental law. Climate change, loss of biodiversity, environmental pollution - these problems do not stop at the borders of countries and require international cooperation and regulation.

Modern trends in the development of environmental law indicate the search for new approaches and tools to ensure sustainable development and preservation of natural resources. Global problems require global answers, and that is why the development of environmental law is gaining more and more importance in the conditions of globalization.

In this scientific study, we will try to consider the main directions of the modern development of environmental law in the context of globalization. We will investigate the influence of global processes on the formation of environmental law at various levels - from international to national. We will also consider the key challenges faced by modern environmental legislation and ways to solve them.

It is necessary to take into account that effective regulation of environmental issues requires not only the adoption of new legislative acts, but also the development of international cooperation mechanisms, the involvement of target groups of the public, and the creation of conditions for environmental education and awareness.

In this context, the analysis of modern trends in the development of environmental law in the context of globalization becomes a relevant and important task, which will allow more effective response to the challenges facing modern society.

Environmental and legal problems of society attract the attention of government representatives, scientists, practical workers and others. The essence of the rule of law is that it ensures the honor and dignity, personal and property security of citizens, their rights and freedoms. And in particular, it is about the constitutionally enshrined environmental rights of citizens.

According to forecasts, the coming years for Ukraine, as well as for the whole world, will be years of various kinds of disasters and ecological cataclysms. All countries have entered an era of crisis, which is associated with the availability of a limited amount of natural resources, the deterioration of the ecological situation, climate change and many other problems of both an objective and subjective nature.

To eliminate these and many other problems, as well as to form a system of effective legal regulation in the field of effective use of natural resources and protection of the natural environment, as well as ensuring environmental safety, such a legal branch as environmental law of Ukraine is called.

Environmental legislation of Ukraine today represents a multi-sectoral system of regulatory acts of different legal force, which complicates their use and leads to numerous contradictions between them or inconsistency of individual acts, duplication. The presence of regulations in a large