Международный журнал прикладных наук и технологий "Integral"

Научная статья

Original article

УДК 338.24

DOI 10.55186/27131424_2023_5_3_3

ВЛИЯНИЕ ЦИФРОВЫХ ВАЛЮТ И КИБЕРПРЕСТУПНОСТИ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ СТРАНЫ

THE IMPACT OF DIGITAL CURRENCIES AND CYBERCRIME ON ECONOMIC SECURITY OF THE COUNTRY

Белов Максим Алексеевич, студент 3-го курса ФГБОУ ВО «Пензенский государственный технологический университет» (440039, Пензенская область, г. Пенза, проезд Байдукова/ул. Гагарина, д. 1 «а»/11), тел. 8(937) 415-08-82 belov.maxim02@gmail.com

Тарасова Татьяна Викторовна, доцент кафедры экономики и управления, ФГБОУ ВО «Пензенский государственный технологический университет» (440039, Пензенская область, г. Пенза, проезд Байдукова/ул. Гагарина, д. 1 «а»/11), тел. 8(963) 100-99-01, rabota13a@yandex.ru

Maxim A. Belov, 3rd year student Penza state technological university (1 «a» /11 Baidukova passage/ Gagarina st., Penza, 440039 Russia), tel. 8(937) 415-08-82, belov.maxim02@gmail.com

Tatyana V. Tarasova, associate professor of the department of economics and management, Penza state technological university (1 «a» / 11 Baidukova passage / Gagarina st., Penza, 440039 Russia), tel. 8(963) 100-99-01, rabota13a@yandex.ru

Аннотация. В статье рассматривается влияние цифровых валют и киберпреступности на экономическую безопасность страны. Исследованы основные виды киберпреступлений, цели и их последствия для экономики страны. Также, рассматривается связь цифровых средств оплаты с теневой экономикой и ростом киберпреступности. Определены способы защиты экономической безопасности страны и борьбы с киберпреступлениями, включая внедрение новых технологий и политических мер. Особое внимание уделяется технологии *blockchain*, как одному из способов предотвращения киберпреступлений. Исследован алгоритм работы *blockchain*, а также определены основные преимущества использования данной технологии для защиты экономической безопасности.

Abstract. The article examines the impact of digital currencies and cybercrime on the economic security of the country. The main types of cybercrimes, goals and their consequences for the country's economy are investigated. Also, the connection of digital means of payment with the shadow economy and the growth of cybercrime is considered. The ways of protecting the country's economic security and combating cybercrime, including the introduction of new technologies and policy measures, have been identified. Particular attention is paid to blockchain technology as one of the ways to prevent cybercrimes. The algorithm of blockchain operation is investigated, and the main advantages of using this technology to protect economic security are determined.

Ключевые слова: экономическая безопасность, информационные технологии, интернет-преступления, платежная система, криптовалюта, блокчейн.

Keywords: economic security, information technology, internet crimes, payment system, cryptocurrency, blockchain.

Цифровая экономика стала неотъемлемой частью нашей жизни, и вместе с ней появились новые формы экономической преступной деятельности. Современные технологии позволяют преступникам работать анонимно и в международных масштабах, что делает борьбу с ними очень непростой задачей.

Международные организации, правительства и компании всего мира ведут активную борьбу с экономическими преступлениями, включая киберпреступления. Использование новых технологий, таких как блокчейн, помогает повысить эффективность борьбы с данными преступлениями.

В современном мире экономические преступления включают в себя такие виды как отмывание денег, коррупция, налоговые мошенничества и финансовые махинации. Киберпреступления же включают в себя кражу личной информации, кражу денег с банковских счетов, кибершпионаж, кибертерроризм и другие виды преступлений, совершаемых через сеть Интернет.

Правительства и компании всего мира активно работают над созданием новых мер по борьбе с экономической преступностью, которая включает в себя улучшение законодательства, обмен информацией между различными организациями и странами, а также создание новых технологических решений для защиты данных и мониторинга ситуации в режиме реального времени.

Борьба с экономической преступностью – это задача, требующая международного сотрудничества и координации усилий всех заинтересованных сторон. Только таким образом появляется возможность защитить экономику и обеспечить устойчивое развитие в будущем [2].

В отличие от других преступлений, киберпреступления в настоящее время самый быстрорастущий сегмент. Любые IT инновации создают условия для появления новых вариантов киберпреступности и способов кражи персональных данных, финансов и секретных документов или разработок какой-либо компании. Основная цель этих преступников – это государственные учреждения, медицинская деятельность и крупные промышленные компании [7].

Цифровые средства оплаты также привлекают теневую экономику. Тема электронных валют тесно взаимосвязана с преступностью, которая растет значительными темпами. Сотрудниками правоохранительной деятельности на территории России в 2020 году было установлено 517722 случая киберпреступлений. Для сравнения, в сфере незаконного оборота наркотических средств установлено 51 495 случаев правонарушений [3].

Новейшие IT-разработки для киберпреступников являются легкой добычей, так как еще нет действенных методов защиты, иначе говоря, возможно наличие непредусмотренных вариантов обхода системы защиты. Киберпреступник крадет документы, файлы, активы и зачастую переводит их в другую страну, тем самым уменьшая шансы быть пойманным. Подобные ситуации мешают развитию экономики создавая угрозы экономической безопасности. Кибератаки зачастую остаются нераскрытыми. Большая часть киберпреступлений осуществляется с помощью сети *Deepweb*, вход осуществляется исключительно с помощью особого ПО или в дело вступают анонимные браузеры, например браузер *TOR*, или программы-анонимайзеры, предоставляющие скрытие *IP*-адреса и геолокацию. Кроме того, при осуществлении интернет-преступлений на замену преступных групп выходит новая форма взаимодействия – криминальные макросети и их соучастниками являются посетители открытых чатов, форумных сайтов и закрытых сообществ. А чтобы стать одним из участников данных макросетей, нужно получать доверие и определенный статус, из-за остается открытым вопрос, являются ли макросети менее устойчивыми, нежели преступные группировки в традиционном понимании [4].

В наше время никто не может быть в полной безопасности, даже наличие тостера в доме уже подвергает нас риску взлома, не говоря уже о персональных компьютерах и телефонах. Через телефонные *SMS*-сообщения и социальную инженерию мошенники могут получать доступ к нашим финансам и документам. Также стоит учесть то, что киберпреступления постоянно совершенствуются. Появление криптовалют открыло много возможностей киберпреступникам и развязало многим из них руки [5].

Одним из способов предотвращения киберпреступлений в Российской Федерации является полная легализация криптовалют имеющих прозрачную систему, где можно видеть все переводы и тем самым взять под контроль сферу криптовалют. Таким образом, легализация криптовалют может помочь уменьшить возможности для киберпреступников использовать криптовалюты для скрытного проведения преступных операций.

Любая криптовалюта основана на технологии *blockchain*.

Blockchain – это распределенная книга данных, которая обеспечивает безопасный обмен информацией между участниками сети. Эта технология дает возможность выбранным участникам обмениваться данными без посредников. Облачные сервисы *blockchain* упрощают сбор и интеграцию данных из разных источников, а также их обмен. Данные разбиваются на блоки, которые связываются друг с другом уникальными идентификаторами в виде криптографических хеш-функций [6].

Рассмотрим алгоритм работы *blockchain*:

1) Сеть опирается на определенные рекомендации и процедуры для своих узлов для подтверждения новых транзакций. Только если транзакция аутентифицирована, она становится частью нового блока. Этот блок связан с предыдущим с помощью хэша, и его уникальный хэш зависит от его содержимого и хэша предыдущего блока.

2) Чтобы сохранить точность при добавлении новых блоков в цепочку, *blockchain* использует механизм консенсуса между сетевыми узлами. Одним из таких механизмов является *Proof-of-Work*, используемый биткойнами. Этот механизм требует, чтобы узлы решили сложную математическую задачу, и, если узлу это удалось, он оповещает другие узлы, которые могут оценить точность решения. Как только решение проверено, новый блок можно безопасно добавить в цепочку [8].

Blockchain технологии могут помочь сократить количество киберпреступлений, поскольку они предоставляют более безопасные и прозрачные способы хранения, передачи и обработки данных.

Безопасная передача данных. Благодаря криптографическим протоколам, которые используются в *blockchain*, данные могут быть безопасно переданы между участниками сети без риска их изменения или подмены. Это может снизить риск кибератак, таких как хакерские атаки или фишинг, которые могут привести к утечке данных и другим негативным последствиям для организаций и частных лиц. Таким образом, технология *blockchain* может быть использована для обеспечения

безопасности обмена данных в различных областях, включая финансы, медицину, правительство и технологические инновации.

Идентификация и аутентификация. *Blockchain* может использоваться для создания безопасных систем идентификации и аутентификации, которые могут помочь предотвратить утечки данных и злоупотребление информацией. Таким образом, *blockchain* может использоваться для создания цифровых идентификаторов, которые могут быть проверены без необходимости раскрытия личных данных.

Сокращение или устранение лишних посредников. *Blockchain* может убрать посредников в процессе совершения транзакций и обмена информацией с помощью децентрализованной сети, в которой каждый участник владеет доступом к одному и тому же *blockchain*. Благодаря этому, он может аутентифицировать транзакции без участия посредника.

Blockchain, действительно, полезный инструмент для борьбы с киберпреступлениями, но не может являться универсальным решением. Киберпреступники могут использовать разные способы и технологии для обхода защиты информации. По этой причине, *blockchain* не может гарантировать полную безопасность данных. Помимо данной технологии, необходимо соблюдать другие меры безопасности, такие как использование двухфакторной аутентификации, сложных паролей. Кроме этого, нужно регулярно обновлять программное обеспечение, разработчики используют современные технологии, которые усиливают меры безопасности в своих приложениях.

Литература

1. Арефьева, А. С. Перспективы внедрения технологии блокчейн / А. С. Арефьева, Г. Г. Гогохия // Молодой ученый. – 2017. – № 15 (149). – С. 326–330. [Электронный ресурс]. – URL: https://moluch.ru/archive/149/42071/ (дата обращения: 08.05.2023).
2. Пахарев А.В. Влияние цифровых валют и киберпреступности на экономическую безопасность страны // Экономическая безопасность. – 2022.

– Том 5. – № 2. – С. 457–472 [Электронный ресурс]. – URL: https://1economic.ru/lib/114692 (дата обращения 19.04.2023)

3. Потеряйко А. Цифровизация и киберпреступность против человека [Электронный ресурс]. – URL: https://regnum-ru.turbopages.org/regnum.ru/s/news/3384903.html (дата обращения 19.04.2023).
4. Противодействие киберпреступности в сфере цифровой экономики: проблемы и перспективы. [Электронный ресурс]. – URL: https://bstudy.net/788271/ekonomika/protivodeystvie_kiberprestupnosti_sfere_tsifrovoy_ekonomiki_problemy_perspektivy (дата обращения 19.04.2023)
5. Цифровая экономика: от цифровых активов к криптовалютам. [Электронный ресурс] – URL: https://bstudy.net/624487 (дата обращения 19.04.2023).
6. Что такое блокчейн? [Электронный ресурс] – URL: https://www.oracle.com/cis/blockchain/what-is-blockchain/ (дата обращения 19.04.2023).
7. Что такое киберпреступность? Защита от киберпреступности. [Электронный ресурс] – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения 19.04.2023).
8. Что такое технология блокчейн? [Электронный ресурс] – URL: https://aws.amazon.com/ru/what-is/blockchain (дата обращения 19.04.2023).

References

1. Arefyeva, A. S. Prospects for the introduction of blockchain technology / A. S. Arefyeva, G. G. Gogokhia // Young Scientist. – 2017. – № 15 (149). – p. 326–330. [electronic resource]. – URL: https://moluch.ru/archive/149/42071 / (accessed: 08.05.2023).
2. Pakharev A.V. The impact of digital currencies and cybercrime on the economic security of the country // Economic security. – 2022. – Volume 5. – № 2. – p. 457–472 [Electronic resource]. – URL: https://1economic.ru/lib/114692 (accessed: 19.04.2023)

3. Poteryaiko A. Digitalization and cybercrime against man [Electronic resource]. – URL: https://regnum-ru.turbopages.org/regnum.ru/s/news/3384903.html (accessed: 19.04.2023).
4. Countering cybercrime in the digital economy: problems and prospects. [electronic resource]. – URL: https://bstudy.net/788271/ekonomika/protivodeystvie_kiberprestupnosti_sfere_tsifrovoy_ekonomiki_problemy_perspektivy (accessed: 19.04.2023)
5. Digital economy: from digital assets to cryptocurrencies. [Electronic resource] – URL: https://bstudy.net/624487 (accessed: 19.04.2023).
6. What is blockchain? [Electronic resource] – URL: https://www.oracle.com/cis/blockchain/what-is-blockchain / (accessed: 19.04.2023).
7. What is cybercrime? Protection against cybercrime. [Electronic resource] – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (accessed 19.04.2023).
8. What is blockchain technology? [Electronic resource] – URL: https://aws.amazon.com/ru/what-is/blockchain (accessed 19.04.2023).

Для цитирования: Белов М.А., Тарасова Т.В. ВЛИЯНИЕ ЦИФРОВЫХ ВАЛЮТ И КИБЕРПРЕСТУПНОСТИ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ СТРАНЫ// Международный журнал прикладных наук и технологий "Integral" №3/2023