YURIDIK FANLAR AXBOROTNOMASI

ВЕСТНИК ЮРИДИЧЕСКИХ НАУК

REVIEW OF LAW SCIENCES

huquqiy ilmiy-amaliy jurnal

правовой научно-практический журнал

legal scientific-practical journal

2024-yil 2-son

VOLUME 8 / ISSUE 2 / 2024

DOI: 10.51788/TSUL.ROLS.2024.8.2.

ISSN 2181-919X

E-ISSN 2181-1148

DOI: 10.51788/TSUL.ROLS

Crossref Content Registration

MUASSIS: TOSHKENT DAVLAT YURIDIK UNIVERSITETI

"Yuridik fanlar axborotnomasi – Вестник юридических наук – Review of law sciences" huquqiy ilmiy-amaliy jurnali O'zbekiston matbuot va axborot agentligi tomonidan 2020-yil 22-dekabrda 0931-sonli guvohnoma bilan davlat ro'yxatidan o'tkazilgan. Jurnal O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi jurnallari ro'yxatiga kiritilgan.

Sotuvda kelishilgan narxda.

Muharrirlar:
Y. Yarmolik, Y. Mahmudov,
E. Mustafayev, K. Abduvaliyeva,
F. Muhammadiyeva

Musahhih:
S. Rasulova

Texnik muharrir:
U. Sapayev

Dizayner:
D. Rajapov

Tahririyat manzili:
100047. Toshkent shahar,
Sayilgoh ko'chasi, 35.
Tel.: (0371) 233-66-36 (1169)

Veb-sayt: review.tsul.uz
E-mail: reviewjournal@tsul.uz
Obuna indeksi: 1385.

Jurnal 24.06.2024-yilda tipografiyaga topshirildi. Qog'oz bichimi: A4.
Shartli 18,6 b.t. Adadi: 100.
Buyurtma raqami: 87.

TDYU tipografiyasida chop etildi.

E-ISSN 2181-1148
ISSN 2181-919X

УЧРЕДИТЕЛЬ: ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

Правовой научно-практический журнал «Вестник юридических наук – Yuridik fanlar axborotnomasi – Review of Law Sciences» зарегистрирован Агентством печати и информации Узбекистана 22 декабря 2020 года с удостоверением № 0931.
Журнал включён в перечень журналов Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан.

Реализуется по договорной цене.

Редакторы:
Е. Ярмолик, Й. Махмудов,
Э. Мустафаев, К. Абдувалиева,
Ф. Мухаммадиева

Корректор:
С. Расулова

Технический редактор:
У. Сапаев

Дизайнер:
Д. Ражапов

Адрес редакции:
100047. Город Ташкент,
улица Сайилгох, 35.
Тел.: (0371) 233-66-36 (1169)

Веб-сайт: review.tsul.uz
E-mail: reviewjournal@tsul.uz
Подписной индекс: 1385.

Журнал передан в типографию 24.06.2024.
Формат бумаги: А4.
Усл. п. л. 18,6. Тираж: 100 экз.
Номер заказа: 87.

Отпечатано в типографии ТГЮУ.

FOUNDER: TASHKENT STATE UNIVERSITY OF LAW

"Yuridik fanlar axborotnomasi – Вестник юридических наук – Review of law sciences" legal scientific-practical journal was registered by Press and Information Agency of Uzbekistan on December 22, 2020, with certificate number 0931.
The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

Agreed-upon price.

Editors:
Y. Yarmolik, Y. Makhmudov,
E. Mustafaev, K. Abduvalieva,
F. Mukhammadieva

Proofreader:
S. Rasulova

Technical editor:
U. Sapaev

Designer:
D. Rajapov

Publishing department addess:
100047. Tashkent city,
Sayilgokh street, 35.
Phone: (0371) 233-66-36 (1169)

Website: review.tsul.uz
E-mail: reviewjournal@tsul.uz
Subscription index: 1385.

The journal is submitted to the printing house on 24.06.2024.
Paper size: A4.
Cond. p.p.18,6. Unit: 100.
Order: 87.
Published in printing house of TSUL.

MUNDARIJA

СОДЕРЖАНИЕ

CONTENTS

Kelib tushgan / Получено / Received: 24.04.2024
Qabul qilingan / Принято / Accepted: 03.06.2024
Nashr etilgan / Опубликовано / Published: 24.06.2024

DOI: 10.51788/tsul.rols.2024.8.2./RJOF6571
UDC: 347:004(045)(575.1)

ЗАЩИТА ЦИФРОВЫХ АКТИВОВ: ИМПЕРАТИВЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЭКОСИСТЕМЫ КРИПТОБИРЖ УЗБЕКИСТАНА

Гулямов Саид Саидахрарович,
доктор юридических наук, профессор,
заведующий кафедрой «Киберправо»
Ташкентского государственного юридического университета
ORCID: 0000-0002-2299-2122
e-mail: said.gulyamov1976@gmail.com

Рустамбеков Исламбек Рустамбекович,
доктор юридических наук, профессор кафедры
«Международное частное право», врио ректора
Ташкентского государственного юридического университета
ORCID: 0000-0002-8869-8399
e-mail: i.rustambekov@tsul.uz

Аннотация. *Анализируя сложный ландшафт кибербезопасности криптобирж Узбекистана, статья подчёркивает важность разработки и внедрения политики и нормативной базы в области кибербезопасности. В статье выявлены наиболее актуальные и развивающиеся цифровые угрозы, а также оценивается эффективность передовых мер по смягчению последствий. Кроме того, исследован трансформационный потенциал инновационных правовых и технологических инструментов, таких как верификация личности на основе блокчейна, доказательства с нулевым разглашением и безопасные многосторонние вычисления. В статье представлены углублённый анализ действующего законодательства, регулирующего практику кибербезопасности в криптовалютной экосистеме Узбекистана, и идеи относительно перспектив будущего развития. Для обеспечения всестороннего анализа ситуации в области кибербезопасности в индустрии криптовалютных бирж используется обширный обзор научных публикаций, отраслевых отчётов и официальных документов, касающихся кибербезопасности на рынке криптовалют. Кроме того, статья включает тематические исследования известных инцидентов кибербезопасности, связанных с криптобиржами. Анализируя примеры из реальной жизни, исследователи попытались обеспечить более детальное понимание проблем кибербезопасности, с которыми сталкиваются криптобиржи, и эффективности различных мер по их смягчению. В заключении статьи даны практические рекомендации по созданию безопасной, надёжной инновационной среды для пользователей криптовалют в Узбекистане.*

Ключевые слова: *кибербезопасность, криптобиржи, Узбекистан, нормативно-правовой ландшафт, технологические инновации.*

RAQAMLI AKTIVLARNI HIMOYA QILISH: O‘ZBEKISTON KRIPTOBIRJALARI EKOTIZIMI UCHUN KIBER XAVFSIZLIK IMPERATIVLARI

Gulyamov Said Saidaxrarovich,
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi mudiri,
yuridik fanlar doktori, professor

Rustambekov Islombek Rustambekovich,
Toshkent davlat yuridik universiteti rektori v.v.b,
Xalqaro xususiy huquq kafedrasi professori,
yuridik fanlar doktori

Annotatsiya. *Maqolada O‘zbekiston kriptobirjalari kiberxavfsizligining murakkab landshafti tahlil qilinib, kiberxavfsizlik siyosati va tartibga solish asoslarini ishlab chiqish hamda ularni amalga joriy etishning ahamiyati ta’kidlanadi. Unda dolzarb va rivojlanayotgan raqamli tahdidlar aniqlangan, shuningdek, ilg‘or yumshatish choralarining samaradorligi baholangan. Bundan tashqari, blokcheyn asosida shaxsni tasdiqlash, nol bilimli dalillar va ko‘p tomonlama xavfsiz hisob-kitoblar kabi innovatsion huquqiy va texnologik vositalarning transformatsion salohiyati o‘rganilgan. Muallif O‘zbekistonning kriptovalyutaviy ekotizimidagi kiberxavfsizlik amaliyotini tartibga soluvchi amaldagi qonunchilikni chuqur tahlil qiladi va kelajakdagi rivojlanish istiqbollariga oid mulohazalarini bildiradi. Kriptovalyuta birjalari sanoatida kiberxavfsizlik holatini har tomonlama tahlil qilishni ta’minlash uchun kriptovalyuta bozoridagi kiberxavfsizlik bilan bog‘liq ilmiy nashrlar, sanoat hisobotlari va ularning keng qamrovli sharhi bayon qilinadi. Bundan tashqari, maqolada kriptovalyuta birjalari bilan bog‘liq kiberxavfsizlik bo‘yicha tadqiqot olib borilgan. Maqolada tadqiqotchilar tomonidan voqelikda kuzatilayotgan misollar tahlil qilinib, kiberxavfsizlik muammolari haqida batafsilroq ma’lumot berishga harakat qilingan. Maqola yakunida O‘zbekistonda kriptovalyuta foydalanuvchilari uchun xavfsiz, ishonchli va innovatsion muhitni yaratish bo‘yicha amaliy tavsiyalar taqdim etiladi.*

Kalit so‘zlar: *kiberxavfsizlik, kriptobirjalar, O‘zbekiston, huquqiy tartibga solish, texnologik innovatsiyalar.*

PROTECTING DIGITAL ASSETS: CYBERSECURITY IMPERATIVES FOR UZBEKISTAN’S CRYPTO EXCHANGE ECOSYSTEM

Gulyamov Said Saidakhrarovich,
Tashkent State University of Law,
Head of the Department of Cyber law,
Doctor of Science in Law, Professor

Rustambekov Islambek Rustambekovich,
Acting Rector of Tashkent State University of Law,
Professor of the Department of Private International Law,
Doctor of Science in Law

Abstract. *Analyzing the complex cybersecurity landscape of Uzbekistan’s crypto exchanges, the article emphasizes the importance of developing and implementing cybersecurity policies and regulatory frameworks. The article identifies the most pressing and evolving digital threats and evaluates the effectiveness of advanced mitigation measures. Furthermore, it explores the transformative potential of innovative legal and technological tools, such as blockchain-based identity verification, zero-knowledge proofs, and secure multi-party computation. The article provides*

an in-depth analysis of the current legislation governing cybersecurity practices within Uzbekistan's crypto ecosystem and offers insights into future development prospects. To provide a comprehensive analysis of the cybersecurity situation in the cryptocurrency exchange industry, an extensive review of academic publications, industry reports and official documents related to cybersecurity in the cryptocurrency market is used. In addition, the article includes case studies of known cybersecurity incidents related to cryptocurrency exchanges. By analyzing real-life examples, the researchers aim to provide a more detailed understanding of the cybersecurity challenges faced by cryptocurrency exchanges and the effectiveness of various mitigation measures. Ultimately, the article presents practical recommendations for creating a secure, trustworthy, and innovation-driven environment for cryptocurrency users in Uzbekistan.

Keywords: *cyber security, crypto exchanges, Uzbekistan, legal regulation, technological innovations.*

Введение

История растущей важности кибербезопасности в индустрии криптовалютных бирж

Быстрый рост рынка криптовалют и растущая популярность криптовалютных бирж выдвинули кибербезопасность на передний план проблем отрасли. Поскольку число пользователей и объём транзакций на криптобиржах продолжают расти, растёт и привлекательность этих платформ для киберпреступников. Криптобиржи, которые служат посредниками при покупке, продаже и обмене криптовалютами, хранят огромные объёмы цифровых активов и конфиденциальной пользовательской информации, что делает их главной мишенью для кибератак. Децентрализованный характер криптовалют и отсутствие единой нормативной базы в разных юрисдикциях ещё больше усугубляют проблемы, с которыми сталкиваются криптобиржи при обеспечении безопасности своей инфраструктуры и защите активов своих пользователей.

Последствия нарушений кибербезопасности в индустрии криптовалютных бирж могут быть серьёзными и привести к потере цифровых активов на миллионы долларов, компрометации личной информации пользователей и подрыву доверия к рынку криптовалют в целом. Громкие хакерские атаки, такие как взлом Mt. Gox в 2014 году [1] и атака Coincheck в 2018 году [2], подчеркнули уязвимость криптобирж перед киберугрозами и необходимость принятия надёжных мер кибербезопасности. Поскольку индустрия обмена криптовалют продолжает развиваться и взрослеть, решение проблем кибербезопасности становится решающим для обеспечения долгосрочной стабильности и роста рынка криптовалют.

Целью этой статьи является предоставление всестороннего обзора текущих и ожидаемых угроз кибербезопасности, с которыми сталкиваются криптобиржи, обсуждение эффективности различных мер по смягчению последствий и подчёркивание необходимости разработки и внедрения надёжных политик кибербезопасности. В статье будут рассмотрены правовые и технологические инструменты, доступные криптовалютным биржам для повышения уровня кибербезопасности, с особым акцентом на перспективы регулирования в Республике Узбекистан.

Анализируя ситуацию с кибербезопасностью в индустрии криптовалютных бирж, эта статья призвана внести свой вклад в продолжающуюся дискуссию о важности кибербезопасности на рынке криптовалют и предоставить ценную информацию для криптобирж, политиков

E-ISSN 2181-1148
ISSN 2181-919X

и исследователей. В статье будут рассмотрены уникальные проблемы, связанные с децентрализованным характером криптовалют, а также необходимость сбалансированного подхода, который способствует инновациям, обеспечивая при этом безопасность и целостность инфраструктуры обмена криптовалютами.

Материалы и методы

Чтобы обеспечить всесторонний анализ ситуации в области кибербезопасности в индустрии криптовалютных бирж, в этой статье используется многогранная методология исследования. Основной подход включает в себя обширный обзор научных публикаций, отраслевых отчётов и официальных документов, касающихся кибербезопасности на рынке криптовалют. Этот обзор помогает определить текущее состояние знаний, наиболее актуальные угрозы кибербезопасности и новые тенденции в этой области.

Помимо обзора литературы, статья включает тематические исследования известных инцидентов кибербезопасности, связанных с криптобиржами. Эти тематические исследования дают ценную информацию о тактике, используемой киберпреступниками, уязвимостях и уроках, извлечённых из каждого инцидента. Анализируя примеры из реальной жизни, статья стремится обеспечить более детальное понимание проблем кибербезопасности, с которыми сталкиваются криптобиржи, и эффективности различных мер по их смягчению.

Результаты исследования

Текущие и ожидаемые угрозы кибербезопасности, с которыми сталкиваются криптобиржи

Криптобиржи сталкиваются с широким спектром угроз кибербезопасности, которые могут поставить под угрозу безопасность их инфраструктуры и активов их пользователей. Одной из наиболее распространённых угроз являются попытки взлома, когда киберпреступники стремятся использовать уязвимости в программном обеспечении или сети биржи для получения несанкционированного доступа к учётным записям пользователей и кражи средств [3]. Хакеры могут использовать различные методы, такие как социальная инженерия, внедрение вредоносного ираммного обеспечения или использование уязвимостей нулевого дня, чтобы взломать защиту биржи.

Ещё одна серьёзная угроза, с которой сталкиваются криптобиржи, – фишинговые атаки, когда киберпреступники создают поддельные веб-сайты или рассылают мошеннические электронные письма, чтобы обманом заставить пользователей раскрыть свои учётные данные для входа или закрытые ключи [4]. Фишинговые атаки могут быть очень сложными и трудными для обнаружения, часто с использованием методов социальной инженерии для манипулирования доверием пользователей и их недостаточной осведомлённости о кибербезопасности.

Инсайдерские угрозы представляют собой ещё один серьёзный риск для криптовалютных бирж, поскольку злонамеренные сотрудники или подрядчики, имеющие доступ к конфиденциальной информации, могут злоупотреблять своими привилегиями для кражи средств или компрометации учётных записей пользователей [5]. Внутренние угрозы может быть особенно сложно обнаружить и предотвратить, поскольку они часто затрагивают людей, которым организация доверяет и которые имеют законный доступ к критически важным системам.

Помимо этих угроз, криптобиржи также сталкиваются с технологическими уязвимостями, возникающими из-за сложности их инфраструктуры и быстрого развития криптовалютного ландшафта. Эти уязвимости могут включать ошибки смарт-контрактов, недостатки механизма

консенсуса или недостатки криптографических алгоритмов, используемых для защиты учётных записей пользователей и транзакций [6].

В будущем ситуация с кибербезопасностью для криптовалютных бирж, вероятно, станет ещё более сложной, поскольку рынок криптовалют продолжает расти и привлекать всё больше участников. Растущая ценность цифровых активов и растущая изощрённость киберпреступников, вероятно, приведут к более частым и серьёзном кибератакам, нацеленным на криптовалютные биржи [7]. Более того, появление квантовых вычислений может представлять собой долгосрочную угрозу безопасности существующих криптографических алгоритмов, требуя от криптобирж внедрения постквантовой криптографии для поддержания целостности своей инфраструктуры [8].

Эффективность различных мер по смягчению последствий

Для устранения разнообразного спектра угроз кибербезопасности, с которыми сталкиваются криптобиржи, необходим комплексный подход, включающий множество мер по смягчению последствий. Одной из наиболее эффективных мер является внедрение многофакторной аутентификации (MFA) для учётных записей пользователей [9]. MFA требует, чтобы пользователи предоставили две или более формы идентификации, такие как пароль и биометрический фактор, для доступа к своим учётным записям, что значительно снижает риск несанкционированного доступа.

Ещё одной важной мерой по смягчению последствий является использование аппаратных модулей безопасности (HSM) для хранения и управления закрытыми ключами [10]. HSM – это специализированные устройства, которые обеспечивают безопасную среду для криптографических операций, гарантируя, что закрытые ключи никогда не попадут в сеть или программное обеспечение биржи. Используя HSM, криптобиржи могут минимизировать риск кражи закрытого ключа и несанкционированных транзакций.

Системы мониторинга в режиме реального времени также необходимы для своевременного обнаружения и реагирования на инциденты кибербезопасности. Эти системы используют расширенную аналитику и алгоритмы машинного обучения для выявления аномальных действий, таких как необычные попытки входа в систему или подозрительные транзакции, и предупреждают команду безопасности биржи для дальнейшего расследования [11]. Благодаря постоянному мониторингу инфраструктуры биржи эти системы могут помочь предотвратить или смягчить последствия кибератак.

Регулярные проверки безопасности и тестирование на проникновение являются ещё одной важной мерой по смягчению последствий для криптобирж. Эти оценки включают систематическую оценку инфраструктуры, политик и процедур биржи для выявления уязвимостей и слабых мест [12]. Проводя регулярные проверки и внедряя рекомендуемые улучшения безопасности, криптобиржи могут активно устранять потенциальные угрозы и поддерживать надёжную кибербезопасность.

В дополнение к этим техническим мерам криптобиржи также должны уделять приоритетное внимание обучению своих сотрудников и пользователей передовым методам кибербезопасности. Сюда входит предоставление рекомендаций по созданию надёжных паролей, выявлению попыток фишинга и безопасному управлению закрытыми ключами [13]. Развивая культуру осведомлённости о кибербезопасности, криптобиржи могут снизить риск человеческих ошибок и атак социальной инженерии.

Важность разработки и реализации комплексной политики кибербезопасности

E-ISSN 2181-1148
ISSN 2181-919X

Разработка и внедрение комплексных политик кибербезопасности имеет решающее значение для криптовалютных бирж, поскольку они обеспечивают последовательный и эффективный подход к управлению рисками кибербезопасности. Эти политики должны определять цели безопасности биржи, определять роли и обязанности сотрудников, а также устанавливать чёткие процедуры для предотвращения, обнаружения и реагирования на инциденты кибербезопасности [4].

Ключевым компонентом комплексной политики кибербезопасности является система управления рисками, которая позволяет бирже выявлять, оценивать и определять приоритетность рисков кибербезопасности на основе их потенциального воздействия и вероятности возникновения. Эта структура также должна включать стратегии по снижению выявленных рисков, такие как внедрение мер безопасности, приобретение страховки кибербезопасности или партнёрство со сторонними поставщиками услуг безопасности [15].

Реагирование на инциденты и планирование непрерывности бизнеса также являются важнейшими элементами комплексной политики кибербезопасности. Криптовалютные биржи должны иметь чётко определённые процедуры реагирования на инциденты кибербезопасности, включая процессы сдерживания, расследования и восстановления [16]. Кроме того, биржи должны разрабатывать и регулярно тестировать планы обеспечения непрерывности бизнеса, чтобы гарантировать, что они смогут поддерживать основные операции и защищать активы пользователей в случае серьёзных сбоев.

Соблюдение соответствующих законодательных и нормативных требований является ещё одним важным аспектом комплексной политики кибербезопасности. Криптовалютные биржи должны гарантировать, что их политика и практика соответствуют применимым законам и правилам, таким как Общий регламент по защите данных (GDPR) в Европейском союзе или Закон об обмене информацией о кибербезопасности (CISA) в США. Несоблюдение этих требований может повлечь за собой значительные финансовые санкции и репутационный ущерб.

Регулярный пересмотр и обновление политик кибербезопасности необходимы для обеспечения их эффективности и актуальности перед лицом развивающихся угроз и меняющихся требований бизнеса. Криптовалютные биржи должны установить процесс периодической оценки эффективности своей политики и внесения необходимых изменений на основе новых отраслевых стандартов, передового опыта и уроков, извлечённых из инцидентов кибербезопасности.

Юридические и технологические инструменты для повышения кибербезопасности, доступные криптобиржам

Криптовалютные биржи могут использовать ряд юридических и технологических инструментов для повышения своей кибербезопасности и защиты пользовательских активов. Одним из многообещающих инструментов является проверка личности на основе блокчейна, которая использует децентрализованные протоколы идентификации для безопасного хранения и управления идентификационной информацией пользователя [17]. Используя проверку личности на основе блокчейна, криптобиржи могут снизить риск кражи личных данных и мошеннического создания учётных записей, предоставляя пользователям больший контроль над своими личными данными.

Доказательства с нулевым разглашением (ZKP) – ещё один мощный технологический инструмент, который может помочь криптобиржам повысить конфиденциальность и безопасность. ZKP позволяют пользователям доказывать достоверность

заявления или транзакции, не раскрывая лежащие в основе данные, обеспечивая безопасные и конфиденциальные процессы аутентификации и проверки [18]. Интегрируя ZKP в свою инфраструктуру, криптобиржи могут защитить конфиденциальность пользователей, сохраняя при этом целостность своих операций.

Безопасные многосторонние вычисления (MPC) – это криптографический метод, который позволяет нескольким сторонам совместно вычислять функцию на основе своих входных данных, не раскрывая эти входные данные друг другу. MPC может использоваться криптобиржами для безопасной обработки транзакций и выполнения операций управления ключами, не раскрывая конфиденциальные данные потенциальным злоумышленникам [19]. Используя MPC, криптобиржи могут повысить безопасность и отказоустойчивость своей инфраструктуры, сохраняя при этом конфиденциальность пользовательской информации.

С юридической точки зрения криптобиржи могут использовать договорные соглашения и условия обслуживания для установления чётких ожиданий и обязательств в отношении кибербезопасности. В этих соглашениях могут быть указаны меры безопасности, которые будет реализовывать биржа, обязанности пользователей по защите своих учётных записей и ответственность биржи в случае инцидента кибербезопасности [20]. Чётко определив эти условия, криптобиржи могут снизить риск юридических споров и обеспечить большую прозрачность для своих пользователей.

Криптовалютные биржи также могут использовать страхование кибербезопасности для передачи некоторых финансовых рисков, связанных с инцидентами кибербезопасности. Полисы страхования кибербезопасности могут покрывать ряд расходов, включая судебно-медицинские расследования, восстановление данных, судебные издержки и компенсацию клиентам [21]. Получив соответствующее страховое покрытие кибербезопасности, криптобиржи могут снизить потенциальные финансовые последствия успешной кибератаки и продемонстрировать свою приверженность защите активов пользователей.

Текущее состояние правил кибербезопасности для криптобирж в Республике Узбекистан и возможные будущие изменения

Нормативно-правовая база для криптовалютных бирж в Республике Узбекистан пока ещё развивается, и правительство предпринимает шаги по созданию комплексной базы криптовалютной индустрии. В 2018 году Президент Узбекистана подписал Указ «О мерах по развитию цифровой экономики в Республике Узбекистан», который заложил основу правового признания и регулирования криптовалют и технологии блокчейн [22].

В соответствии с этим указом Национальному агентству проектного управления при Президенте Республики Узбекистан (НАПУ) поручено разработать нормативную базу криптовалютной индустрии. В 2019 году НАПУ выпустило свод правил и положений для криптовалютных бирж, работающих в Узбекистане, который включал требования по лицензированию, мерам по противодействию отмыванию денег (ПОД) и финансированию терроризма (ПФТ), а также стандарты кибербезопасности [23].

Согласно этим правилам, криптобиржи в Узбекистане должны получить лицензию НАПУ и внедрить надёжные меры ПОД/ФТ и кибербезопасности. Биржи также должны соблюдать международные стандарты, такие как рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (FATF), и сотрудничать с правоохранительными органами в случае инцидента

E-ISSN 2181-1148
ISSN 2181-919X

кибербезопасности или подозрительной деятельности [24].

В дополнение к конкретным правилам криптовалютных бирж Узбекистан также принял более широкий закон о кибербезопасности – Закон Республики Узбекистан «О кибербезопасности», который вступил в силу в 2019 году. Этот закон устанавливает общие рамки обеспечения безопасности информационных систем и сетей в стране, включая меры по предотвращению, обнаружению и реагированию на угрозы кибербезопасности. Однако закон не затрагивает напрямую конкретные проблемы и риски, связанные с криптовалютами и криптобиржами, что оставляет место для дальнейшей разработки целевых правил в этой области.

Кроме того, Правительство Узбекистана приняло долгосрочный стратегический план, известный как Стратегия «Цифровой Узбекистан – 2030», в котором изложено видение страны в области цифровой трансформации и технологического развития [25]. Стратегия признаёт потенциал технологии блокчейна и криптовалют в стимулировании инноваций и экономического роста и подчёркивает необходимость создания благоприятной нормативной среды, которая уравновешивает преимущества и риски этих технологий. В рамках этой стратегии правительство выразило намерение продолжить разработку и совершенствование нормативной базы для криптовалютной индустрии в соответствии с передовой международной практикой и меняющимися потребностями рынка.

Хотя эти правила представляют собой значительный шаг на пути к созданию безопасной и совместимой с требованиями индустрии криптовалютных бирж в Узбекистане, есть возможности для дальнейшего развития и совершенствования. Поскольку рынок криптовалют продолжает развиваться и появляются новые угрозы кибербезопасности, нормативно-правовую базу необходимо адаптировать, чтобы обеспечить её эффективность в защите пользователей и поддержании целостности отрасли.

Потенциальные будущие изменения в сфере регулирования криптовалютных бирж в Узбекистане могут включать создание специальной структуры кибербезопасности для криптовалютной индустрии, аналогичной системе кибербезопасности Национального института стандартов и технологий (NIST) в США [26]. Такая структура могла бы обеспечить более комплексный и стандартизированный подход к управлению рисками кибербезопасности и продвижению лучших практик среди криптовалютных бирж.

Ещё одной областью потенциального развития является содействие более тесному сотрудничеству и обмену информацией между криптобиржами, регулирующими органами и правоохранительными органами. Создав формальные каналы для обмена информацией об угрозах и передовым опытом, отрасль сможет разработать более скоординированный и эффективный ответ на инциденты кибербезопасности и возникающие угрозы [27].

Наконец, поскольку криптовалютная индустрия в Узбекистане продолжает расти и развиваться, может возникнуть необходимость в более специализированных и адаптированных правилах для устранения уникальных рисков и проблем, с которыми сталкиваются криптобиржи. Это может включать разработку руководящих принципов по безопасному хранению цифровых активов, установление стандартов совместимости сетей блокчейнов и создание нормативной «песочницы» для тестирования новых технологий и практик кибербезопасности [28].

Сравнение ситуации с кибербезопасностью криптобирж в Республике Узбекистан с ситуацией в других странах

Сравнение кибербезопасности криптобирж в Республике Узбекистан с ситуацией в других странах выявляет как сходства, так и различия. Как и многие другие юрисдикции, Узбекистан признал необходимость нормативной базы, которая учитывала бы уникальные риски и проблемы, связанные с криптовалютами, и предпринял шаги по установлению руководящих принципов безопасной работы криптобирж.

Однако подход к регулированию в Узбекистане всё ещё находится в относительно зачаточном состоянии по сравнению с подходом на более зрелых рынках, таких как США, Япония или Сингапур [9]. Эти страны разработали более полные и подробные правила кибербезопасности для криптовалютной индустрии, включая конкретные требования к оценке рисков, отчётности об инцидентах и сторонним аудитам.

Одним из заметных отличий является упор на сотрудничество и обмен информацией между участниками отрасли. В таких странах, как США и Япония, существуют хорошо зарекомендовавшие себя механизмы криптобирж для обмена информацией об угрозах и лучшими практиками, такие как Стандарт безопасности криптоактивов (CCSS) в Японии и Совет по рейтингам криптовалют (CRC) в США [30]. Эти инициативы помогают развивать совместный и упреждающий подход к кибербезопасности, что имеет важное значение для борьбы с быстроменяющимся ландшафтом угроз.

Ещё одна область, где Узбекистан мог бы перенять опыт других стран, это разработка специализированных рамок и руководств по кибербезопасности для криптовалютной индустрии. Например, Национальный институт стандартов и технологий (NIST) в США разработал структуру кибербезопасности, которая обеспечивает общий язык и набор лучших практик для управления рисками кибербезопасности в различных отраслях, включая сектор криптовалют [31].

Несмотря на эти различия, проблемы кибербезопасности, с которыми сталкиваются криптобиржи в Узбекистане, во многом аналогичны проблемам, с которыми сталкиваются биржи в других странах. Попытки взлома, фишинговые атаки и инсайдерские угрозы – это универсальные проблемы, которые требуют сочетания технического контроля, вмешательства в человеческий фактор и нормативного надзора для эффективного смягчения последствий.

Выводы

Краткое изложение основных выводов и важности надёжных мер и политики кибербезопасности

В ходе данного исследования был проведён всесторонний анализ ситуации в области кибербезопасности в индустрии криптовалютных бирж с упором на текущие и ожидаемые угрозы, меры по их смягчению, правовые и технологические инструменты, а также изменения в сфере регулирования в Республике Узбекистан. Результаты подчёркивают исключительную важность надёжных мер и политики кибербезопасности для криптобирж для защиты их инфраструктуры и пользовательских активов от растущего спектра киберугроз.

Для криптовалютных бирж важно сделать кибербезопасность приоритетом в качестве основного компонента своей бизнес-стратегии и выделить достаточные ресурсы для внедрения и поддержания эффективных мер безопасности. Это включает в себя инвестиции в передовые технические средства контроля, регулярное обучение и подготовку сотрудников и пользователей, а также активное участие в разработке отраслевых стандартов и лучших практик. Криптовалютные биржи также должны стремиться сотрудничать с другими участниками отрасли, ре-

E-ISSN 2181-1148
ISSN 2181-919X

гулирующими и правоохранительными органами для обмена информацией об угрозах и координации реагирования на возникающие угрозы.

Работая вместе над решением сложных проблем, связанных с кибербезопасностью в индустрии криптовалютных бирж, заинтересованные стороны в Республике Узбекистан могут внести свой вклад в развитие более безопасной, отказоустойчивой и заслуживающей доверия экосистемы криптовалют. Это в свою очередь будет способствовать долгосрочному росту и внедрению криптовалют и технологии блокчейн как в Узбекистане, так и во всём мире.

REFERENCES

1. Mcmillan R. The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. *Business*, 2014, March 3. Available at: https://www.wired.com/2014/03/bitcoin-exchange/

2. Japanese cryptocurrency exchange loses more than $500 million to hackers. CNBC. Available at: https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html

3. Houben R., Snyers A. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament, 2018.

4. Dion-Schwarz C., Manheim D., Johnston P.B. Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats. Rand Corporation, 2019.

5. Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. Where is current research on blockchain technology? A systematic review. *PloS One*, 2016, vol. 11 (10).

6. Feder A., Gandal N., Hamrick J., Moore T. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity,* 2018, vol. 3 (2), pp. 137–144.

7. Vasek M., Moore T. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2015, pp. 44–61.

8. Dasgupta D., Shrein J.M., Gupta K.D. A survey of blockchain from security perspective. *Journal of Banking and Financial Technology*, 2019, vol. 3 (1), pp. 1–17.

9. Conti M., Kumar E.S., Lal C., Ruj S. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20 (4), pp. 3416–3452.

10. Li X., Jiang P., Chen T., Luo X., Wen Q. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 2020, no. 107, pp. 841–853.

11. Taylor P.J., Dargahi T., Dehghantanha A., Parizi R.M., Choo K.K.R. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 2020, vol. 6 (2), pp. 147–156.

12. Homoliak I., Venugopalan S., Hum Q., Szalachowski P. A security reference architecture for blockchains. *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 390–397.

13. Mosakheil J.H. Security threats classification in blockchains. *Culminating Projects in Information Assurance*, 2018, p. 48.

14. Alkhalifah A., Ng A., Kayes A., Chowdhury J., Alazab M., Watters P. A taxonomy of blockchain threats and vulnerabilities. *Blockchain Cybersecurity, Trust and Privacy*. Springer, Cham, 2020, pp. 3–26.

15. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on ethereum smart contracts (sok). *Proceedings of the International conference on principles of security and trust.* Springer, Berlin, Heidelberg, 2017, pp. 164–186.

16. Meng W., Tischhauser E.W., Wang Q., Wang Y., Han J. When intrusion detection meets blockchain technology: A review. *IEEE Access*, 2018, no. 6, pp. 10179–10188.

17. Ye C., Li G., Cai H., Gu Y., Fukuda A. Analysis of security in blockchain: Case study in 51%-attack detecting. *Proceedings of the 2018 5th International Conference on Dependable Systems and Their Applications (DSA).* IEEE, 2018, pp. 15–24.

18. Saad M., Spaulding J., Njilla L., Kamhoua C., Shetty S., Nyang D., Mohaisen A. Exploring the attack surface of blockchain: A systematic overview. 2019. arXiv preprint arXiv:1904.03487

19. Liang X., Zhao J., Shetty S., Liu J., Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *Proceedings of the 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE, 2017, pp. 1–5.

20. Kiran P., Kavya N.P. A survey on methods and challenges of crypto currency transactions. *Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT).* IEEE, 2020, pp. 852–857.

21. Chicarino V.R., Jesus E.F., Albuquerque C., Rocha A.A.D.A. On the detection of selfish mining and stalker attacks in blockchain networks. *Annals of Telecommunications,* 2020, vol. 75 (3), pp. 143–152.

22. Gervais A., Karame G.O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S. On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016, pp. 3–16.

23. Harz D., Boman M. The scalability of trustless trust. 2018. arXiv preprint arXiv:1801.09535

24. Bonneau J., Miller A., Clark J., Narayanan A., Kroll J.A., Felten E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings of the 2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 104–121.

25. Androulaki E., Barger A., Bortnikov V., Cachin C., Christidis K., De Caro A., Muralidharan S. Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the thirteenth EuroSys conference.* 2018, pp. 1–15.

26. Lin I.C., Liao T.C. A survey of blockchain security issues and challenges. *International Journal of Network Security*, 2017, vol. 19 (5), pp. 653–659.

27. Eyal I., Sirer E.G. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 2018, vol. 61 (7), pp. 95–102.

28. Karame G. On the security and scalability of bitcoin's blockchain. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 1861–1862.

29. Dinh T.T.A., Wang J., Chen G., Liu R., Ooi B.C., Tan K.L. Blockbench: A framework for analyzing private blockchains. *Proceedings of the 2017 ACM International Conference on Management of Data,* 2017, pp. 1085–1100.

30. Karame G. O., Androulaki E., Capkun S. Double-spending fast payments in bitcoin. *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 906–917.

31. Liu J., Liu Z., Zhang Z. A survey on consensus mechanisms and mining strategy management in blockchain networks. 2019. arXiv preprint arXiv:1908.08316

32. Cai C.W. Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain. *Accounting & Finance*, 2018, vol. 58 (4), pp. 965–992.

33. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 2017, vol. 41 (10), pp. 1027–1038.

34. Gulyamov S., Rustambekov I., Narziev O., Xudayberganov A. Draft Concept of the Republic of Uzbekistan in the Field of Development Artificial Intelligence for 2021–2030*. Jurisprudence*, 2021, no. 1, pp. 107–121.

E-ISSN 2181-1148
ISSN 2181-919X