для их привлечения, найма, развития и удержания В этой связи кадровая стратегия как составной элемент системы корпоративного управления — это процесс самосовершенствования посредством таких действий, как улучшение навыков трудоустройства, повышение сознательности и накопление богатства, что также ведет к саморазвитию персонала.

Список цитируемых источников

1. Цена корпоративного управления. Вестник MacCinsey [Электронный ресурс]. — Режим доступа: http://vestnikmckinsey.ru/organizational-models-and-management-systems/cena-korporativnogo-upravleniya. — Дата доступа: 01.01.2023.

2. ЗАО «Чайна Мерчанте СиЭйчЭн-БиЭлАр Коммерческая и Логистическая Компания» [Электронный ресурс]. — Режим доступа: https://ea-cmcb.com/. — Дата доступа: 13.01.2023.

3. Модель менеджмента в Китае. JobGrade Сайт о труде и менеджменте [Электронный ресурс]. — Режим доступа: https://www.jobgrade.ru/2021/12/11/. — Дата доступа: 23.02.2023.

УДК 336.74

В. В. Лукьянович[1], М. М. Хованская[2]

Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь, [1]lykianovichvladislav@gmail.com, [2]machulj@tut.by

КРИПТОВАЛЮТА: МОШЕННИЧЕСТВО И ВИДЫ

В работе речь пойдет о криптовалюте, популярность которой значительно увеличилась во время пандемии Covid-2019, но вместе с этим вырос и объем мошенничества с ней. Криптомошенничества принимают различные виды, поэтому важно, с одной стороны, точно представлять, как работают новые схемы обмана, а, с другой стороны, предпринимать меры по предупреждению их появления. Для борьбы с криптомошенничеством нужен комплексный подход: повышение финансовой грамотности населения, экономические, правовые и иные меры.

Ключевые слова: криптовалюта; криптомошенничества; виды; блокчейн; майнинг.

V. V. Lukyanovich[1], M. M. Khovanskaya[2]
Baranavichy State University, Baranavichy, the Republic of Belarus,
[1]lykianovichvladislav@gmail.com, [2]machulj@tut.by

CRYPTOCURRENCY: FRAUD AND TYPES

The paper will focus on the cryptocurrency, the popularity of which increased significantly during the Covid-2019 pandemic, but at the same time the volume of fraud with it also increased. There are various types of crypto fraud, so it is important, on the one hand, to understand exactly how new deception schemes work, and, on the other hand, to take measures to prevent their occurrence. To combat crypto fraud, a comprehensive approach is needed: improving the financial literacy of the population, economic, legal and other measures.

Key words: cryptocurrency; crypto fraud; types; blockchain; mining.

Введение. Как только люди начинают использовать и изучать новые денежные механизмы, такие как криптовалюты, они понимают, что все финансовые операции и транзакции связаны с определенными рисками. Интернет, откровенно говоря, является благодатной почвой для мошенничества.

Основная часть. На протяжении многих лет криптовалютам удавалось избегать жестких регулирующих мер, с которыми сталкиваются государства и крупные финансовые учреждения. Несмотря на множество ограничений, связанных с наиболее популярными монетами, в целом децентрализованная экосистема по-прежнему остается достаточно свободным пространством для инвестиций и трейдинга.

С одной стороны, такая ситуация на крипторынке является преимуществом, но, с другой стороны, ее приемлемость и доступность привлекают тысячи криптовалютных «новичков» и мошенников, мечтающих быстро заработать.

В современном мире криптовалюты являются невероятно ценными активами для преступников, потому что это ликвидно, портативно, и после того, как пользователь совершит транзакцию, отменить ее практически невозможно. В связи с этим и родилась совершенно новая волна аферы, охватившая мир цифровых валют. Мошенники появляются там, где есть деньги, а в криптовалютном бизнесе много денег. И всегда будут новички, которые наивно верят в самый простой способ заработка.

Один из распространённых видов мошенничества — это мошенничество в социальных сетях. Для привлечения аудитории и пользователей своих проектов криптостартапы используют социальные сети. Твиттер является самой популярной площадкой для криптоэнтузиастов. Однако мало кто может реально оценивать проект, его фундаментальную и техническую базу, и из-за этого неопытные инвесторы доверяют свои средства «не тем людям». Мошенники могут утраивать гивэвей, разные предложения, где надо будет отправить им всего 1 BNB/BTC/ETH, и они обещают вернуть в 10 раз больше. Это кажется слишком заманчивым, чтобы быть правдой, но новички верят в такие уловки [1].

Также мошенники могут использовать Twitter, чтобы писать посты от имени авторитетных лиц. Боты и фальшивые аккаунты знаменитостей публикуют твиты с привлекательными предложениями многочисленных преимуществ и инвестиций «без проблем». Мошенники создают страницы в одном и том же стиле, как у популярных людей криптоиндустрии с одинаковым изображением профиля и очень похожими никнеймами. Никнеймы выбираются максимально похожими, изменяя буквально пару символов, и при быстром чтении ленты в Твиттере эти изменения можно не заметить. К сожалению, данные махинации являются достаточно распространенными среди мошенников [2].

Среди криптомошенничества набирают популярность такие виды, как фейковые сайты и приложения. Именно на поддельные мобильные приложения попадают многие новички-инвесторы, которые только начинают разбираться в рынке криптовалют. Обычно они размещаются на самых популярных платформах по скачиванию приложений. Хотя такие приложения достаточно быстро распознаются и удаляются, тысячи людей становятся жертвами этой аферы.

Даже если следовать советам опытных пользователей, всегда есть риск посетить поддельные сайты и столкнуться с мошенниками. Сегодня в Интернете довольно много сайтов, которые в точности дублируют самые известные страницы криптопроектов.

Чтобы обнаружить поддельные сайты, нужно внимательно посмотреть на адресную строку. Обычно иконка отображается на официальном сайте в виде ключа. Если адрес страницы не начинается с обычного “https” и не имеет значка, надо насторожиться. И даже если сайт не предупреждает об опасности, пользователь может быть

перенаправлен на совершенно другую платформу во время оплаты, и есть риск потерять вложенные средства.

Еще один из способов мошенничества, который берет свое начало с 90-х, — это финансовая пирамида. Мошеннические схемы с финансовыми пирамидами дошли и до криптовалюты. Финансовые пирамиды — это мошеннические проекты, имитирующие прибыльные инвестиции. Финансирование происходит за счет постоянного привлечения новых участников. Люди вкладывают деньги, привлекают новых людей — пирамида растет. В то же время вершина пирамиды действительно может зарабатывать деньги. А низы ничего не получают — они наивно жертвуют деньги тем, кто на ступеньку выше. Финансовые пирамиды не являются финансовыми организациями, так как не имеют лицензии уполномоченного органа по регулированию и развитию финансового рынка. Они не вправе привлекать инвестиции от обычных людей, не имеют права принимать доверительное управление и осуществлять инвестирование привлеченных средств.

Криптовалютные пирамиды почти ничем не отличаются от классических и имеют узнаваемые характеристики, по которым их можно вычислить:

1. *Гарантия высокой доходности.* 1 % в день, 50 % в неделю это очень много. Реальные инвестиционные проекты такой прибыли не дают. Хотя организаторы финансовых пирамид утверждают обратное. Они обосновывают это уникальностью проекта — своего рода чудо-алгоритмом, позволяющим «обыгрывать» рынок. Но людям, разрабатывающим алгоритмы, быстро разбогатевшие с небольшими вложениями, инвесторы не нужны. Поэтому никогда не стоит доверять свои деньги тому, кто обещает золотые горы с минимальными вложениями.

2. *Привлечение новых пользователей.* Без вкладов инвесторов и постоянного денежного потока финансовая пирамида рухнет. Поэтому, чтобы соблюсти принцип пирамиды, организаторы мошеннических схем стремятся привлечь как минимум 1—2 участников.

3. *Анонимности и лицензии.* Организаторы финансовых пирамид просят пополнять счета через электронные кошельки, где движение средств сложно отследить. Также в интернете нет достоверной информации об организаторах финансовой пирамиды.

Анализируя историю самых известных блокчейн-пирамидах можно отметить 3 проекта.

OneCoin. Общий ущерб — от €4 млрд. до €15 млрд., по разным оценкам. Криптовалюта позиционировалась как «убийца биткойна», которая через три года станет самым популярным способом оплаты на планете. В то же время у проекта не было блокчейна и майнинга. Этим делом занимались сами учредители, а платежи и переводы разрешались только на подконтрольных им площадках. Третий год подряд регуляторы разных стран предупреждают людей о том, что проект имеет все признаки финансовой пирамиды. Основательница проекта Ружа Игнатова внезапно исчезла на четвертом году работы и до сих пор находится в розыске. Были арестованы только главный адвокат и два второстепенных организатора.

PlusToken. Общий ущерб составил $3 млрд. Китайская пирамида рекламировала свой 30 % ежемесячный доход плюс бонусы за привлечение друга. PlusToken залистился на таких криптобиржах, как Bithumb, Huobi, где инвесторы и хранили свои средства. Поиски жертв проводились посредством обучающих занятий для новичков в криптовалюте. Пострадало более 4 млн. человек в Японии, Китае и Европе. Есть подозрение, что основатель манипулировал ценой биткоина благодаря накопленным средствам. Шесть организаторов были задержаны и приговорены к длительным срокам тюремного заключения. Деньги, хранящиеся на криптовалютном кошельке компании, вернуть не удалось. Все аккаунты были опустошены после закрытия проекта неизвестным лицом.

Bitconnect. Нанесенный ущерб — более 1 млрд. долларов. Криптокомпания продвигала децентрализованную одноранговую монету BCC. Инвесторам обещали 90 % годового дохода при депозитах от $10 тыс., заморозку депозита на 300 дней и 40 % в месяц. В 2018 году цена монеты упала на 93 %, поскольку мошенническая деятельность была официально признана регулирующими органами США. В том же году токен был исключен из списка всех бирж, а анонимная команда основателей исчезла вместе со всеми деньгами [3].

Десять крупнейших краж криптоактивов в 2022 году принесли преступникам $4,28 млрд. Первое место занимает Ronin Network (Axie Infinity) — в 2022 году злоумышленники украли цифровых активов на сумму $620 млн. Второе место — Poly Network: эта атака принесла $610 млн., а взлом Binance в октябре 2022 года замкнул тройку лидеров: убытки составили около $570 млн. Четвертое место — инцидент с Coincheck: хакерам удалось украсть активы на сумму

$532 млн. Обанкротившаяся крипто биржа FTX занимает пятое место. Атака принесла киберпреступникам $477 млн. Инцидент с MT Gox занял шестое место и принес убытки в размере $470 млн. В десятка также вошли атаки на Wormhole ($326 млн), KuCoin ($281 млн), PancakeBunny ($200 млн) и BitMart ($196 млн).

В настоящее время крупные государства начинают серьезнее относится к данной сфере и применяют средства защиты информации правовыми методами. Государства могут запрещать или ограничивать использование систем шифрования отдельными лицами, но некоторые документы государственной важности и другая конфиденциальная информация хранятся в зашифрованном виде.

Так в Великобритании необходимо в обязательном порядке сообщить правоохранительным органам свой пароль от своего компьютера или телефона в случае судебного расследования. Отказ в выдаче средства расшифровки является преступлением.

В России использование криптографии ограничено компаниями и индивидуальными предпринимателями. Деятельность по выпуску и продаже программ шифрования требует наличия лицензии.

США включили стандарт AES, который требует, чтобы конфиденциальная правительственная информация хранилась в зашифрованном виде. Спецслужбы могут потребовать от производителей устройств и разработчиков программного обеспечения выдать ключи дешифрования [4].

Пока в Беларуси отсутствует отдельная статья в Уголовном кодексе Республики Беларусь о мошенничестве с криптовалютами, поэтому к этому виду правонарушений применяется статья 212 Хищение имущества путем модификации компьютерной информации, наиболее серьезным наказанием по которой является лишение свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения [5].

Многие схемы криптомошенничества очень сложны и выглядят убедительно с точки зрения пользователя. Надо знать и применять защиту от мошенников. Самое главное, если не понятно, как работает криптовалютный проект, как он устроен, имеет ли он фундаментальную основу и есть сомнения в ее надежности, то лучше потратить время на то, чтобы узнать о проекте больше, прежде чем принимать инвестиционное решение. Криптовалюта несет за собой

много рисков. В связи с тем, что рынки криптовалют являются относительно новыми и менее регулируемыми, чем другие финансовые рынки, они более рискованные и более уязвимы для рыночных манипуляций. Это связано с тем, что существующие криптовалюты не имеют ключевых атрибутов денег, ничем не обеспечены, имеют высокую волатильность, не имеют правовой защиты и обычно необратимы. Глобальные криптовалюты могут подрывать национальный финансовый суверенитет, поэтому необходимо максимально ужесточить правила работы с ними. Так же ввиду усиливающейся роли финансового рынка и усложнением его инструментов необходимо повышение финансовой грамостности населения.

Заключение. Страны постепенно признают правовой статус своих монет и токенов, а Сальвадор делает биткойн своей второй национальной валютой. Через PayPal жители США, Великобритании, а вскоре и всего мира смогут оплачивать регулярные покупки в магазинах, кафе и проезд криптовалютой. Называть все криптовалюты пирамидами также некорректно с юридической точки зрения. Однако мошенники продолжают использовать технологию блокчейн для раскрутки старых и создания новых схем, поэтому важно всегда быть начеку.

Список цитируемых источников

1. Пять распространенных видов мошенничества с криптовалютами и как их избежать [Электронный ресурс]. — Режим доступа: https://vc.ru/crypto/270601. — Дата доступа: 11.03.2023.

2. Виды мошенничества в криптовалютном мире [Электронный ресурс]. — Режим доступа: https://tehnoobzor.com/cryptolife/cryptonews/2329. — Дата доступа: 11.03.2023.

3. Криптовалютные пирамиды [Электронный ресурс]. — Режим доступа: https://finswin.com/kripto/info/kriptovalyuta-piramida.html. — Дата доступа: 11.03.2023.

4. Криптографическая защита информации [Электронный ресурс] // Официальный сайт Serchinform. — 2023. — Режим доступа: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/kriptograficheskaya/. — Дата доступа: 15.03.2023.

5. Уголовный кодекс Республики Беларусь : науч.-практ. коммент. / Т. П. Афонченко [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. — Минск : Нац. центр правовой информ. Респ. Беларусь, 2019. — 1000 с.