

но включать одновременное развитие и внедрение информационных технологий, разработку и создание экспертных систем – специальных аналитических программ (программных продуктов) с использованием знаний в области финансов, судебной бухгалтерии, криминалистики, оперативно-розыскной деятельности, основанных на общем анализе финансово-хозяйственной деятельности субъектов хозяйствования, состояния бухгалтерского учета и финансовой отчетности организации, которые позволят выявлять определенные индикаторы, свидетельствующие о возможных нарушениях, пресекать финансовые преступления на ранних стадиях их совершения, а в комплексе успешно противодействовать преступности в финансовой сфере.

УДК 343.9

Т.И. Дудко

ПРЕСТУПЛЕНИЯ В СФЕРЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Начиная как проект крипто-энтузиастов, система Bitcoin, основанная на технологии цепочки блоков и распределенных реестров (блокчейн) с используемой одноименной расчетной единицей, коренным образом изменила представления общества о существующей финансовой системе. Биткойн превратился из первоначально ничем не обеспеченного продукта в серьезный инвестиционный актив, позволяющий выполнять ряд функций: средства обмена, платежа, накопления и меры стоимости.

Дальнейшая реализация в рассматриваемой области человеком своего «преобразующего потенциала» привела к появлению блокчейн-индустрии, без которой уже сложно представить современное информационное общество. Из этого следует, что массовый интерес к блокчейн-технологии и к криптовалютам определяется самим научно-техническим прогрессом, а также стремлением человека быстро и легко извлекать материальную выгоду, посредством использования и трансформации накопленных знаний об информационных технологиях.

Несмотря на то что блокчейн-технология и криптовалюты достаточно недавно привлекли внимание широкой общественности, первым, кто по достоинству оценил преимущества криптовалют (такие как быстрота, анонимность, надежность, дешевизна и транснациональность транзакций), стал преступный мир. Привлекательность использования криптовалюты в преступных целях обусловлена равным образом уникальными свойствами архитектуры блокчейна: децентрализованным характером

сети и наличием криптографических средств защиты данных в ней, что в значительной степени затрудняет процесс идентификации владельца криптовалюты, а также возможность изъятия ее из криптокошелька.

Нацеленность на применение инновационных решений преступниками приводит к возникновению и развитию преступных посягательств, совершаемых ранее неизвестными способами и с использованием ранее неизвестных средств и связанных в рассматриваемом нами случае с использованием блокчейн-технологии и криптовалюты.

Одной из первых и наиболее востребованных сфер использования криптовалюты в преступных целях стала наркоторговля. О криптовалюте, в частности биткойне, как надежном платежном средстве при расчетах за наркотики заговорили еще в 2013 г. в связи с делом Silk Road (анонимной интернет-площадки, действовавшей в теневого интернете и занимавшейся распространением наркотиков, порнографии, персональных данных, оружия, контрафактов продукции) [1, с. 9]. Сегодня схема продажи не только наркотиков, но и иных запрещенных к обороту предметов с использованием в качестве средства оплаты криптовалюты детально проработана преступниками и широко применяется ими во всем мире. Согласно данным Интерпола, с 2010 по 2016 г. оборот от реализации запрещенных предметов в теневого интернете составил свыше 2 млрд долларов США исключительно в криптовалюте [2].

На фоне роста капитализации криптовалют и в условиях отсутствия должного правового регулирования данной сферы, позволяющего определить параметры безопасности выпуска и оборота криптовалюты, отмечается тенденция постепенной переквалификации преступников с хищения денежных средств на хищение криптовалюты в различных формах проявления: взлом кошельков криптобирж и отдельных пользователей; вымогательство криптовалюты; реализация мошеннических ICO и др. [3–5]. По экспертным оценкам, только за первое полугодие 2018 г. посредством модификаций технологических средств для совершения преступлений в криптоиндустрии преступникам удалось похитить около 1,1 млрд долларов США в криптовалюте [6].

Наглядным примером развития способов совершения преступных посягательств в отношении криптовалюты с использованием сетевых технологий, основанных на удаленном доступе, является появление скрытого майнинга или криптоджекинга. Основная цель криптоджекинга заключается не в похищении данных, а в использовании стороннего оборудования для добычи криптовалюты, ведь чем больше производственные мощности аппаратных средств, тем выше шанс получить вознаграждение в виде криптовалюты. В то же время использование вычислительных мощностей сторонних сервисов может нанести суще-

ственный вред не только интересам отдельных граждан и организаций, но и интересам отдельных государств.

Для преступников сфера оборота криптовалюты предоставила широкие возможности по легализации (отмыванию) доходов, полученных преступным путем. Особенности архитектуры блокчейна и отсутствие соответствующих рекомендаций Международной группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) по выявлению сомнительных операций с криптовалютой фактически исключают возможность достоверно установить участников преступных схем [7, с. 151]. На практике встречаются способы легализации преступных доходов через криптовалюты посредством использования нелегальных обменных сервисов и криптоавтоматов, криптомиксеров и азартных онлайн-игр [1, с. 12; 7, с. 151–152]. Согласно отчету аналитической компании CipherTrace, в период с 2017 г. по первое полугодие 2018 г. было легализовано преступных доходов при помощи криптовалюты свыше 1,2 млрд долларов США [6].

Широкое распространение в открытом доступе интернета информации об алгоритмах разработки вредоносного программного обеспечения и подробных инструкциях по осуществлению, например, криптоджекинга в совокупности с существующими в теневом интернете 12 000 запросами и 34 000 предложениями, связанными с хищением криптовалюты [5], позволяет нам сделать вывод, что для совершения большинства преступных посягательств в сфере криптоиндустрии не требуется наличие специального образования, а лишь наличие специальных технических навыков, полученных посредством изучения и использования соответствующих ресурсов интернета.

Таким образом, можно констатировать, что преступники, имея более высокий уровень подготовки в сфере инновационных технологий, используют все более изощренные способы совершения преступлений. Для эффективного противодействия данным преступлениям необходимо оперативное реагирование правоохранительных органов, которое невозможно без соответствующей подготовки сотрудников в области информационных технологий, в частности блокчейн-технологий и оборота криптовалют.

1. Сидоренко Э.Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2.

2. Ларина Е., Овчинский В. Криптовалюта, блокчейн и преступность [Электронный ресурс] // Завтра: блоги и сообщества. URL: http://zavtra.ru/blogs/kriptovalyuta_blokchejn_i_prestupnost (дата обращения: 25.09.2018).

3. Wall Street Journal: мошеннические ICO уже принесли своим создателям свыше \$1 млрд [Электронный ресурс] // ForkLog. URL: <https://forklog.com/wall-street-journal-moshennicheskie-ico-uzhe-prinesli-svoim-sozdatelyam-svyshe-1-mlrd> (дата обращения: 25.09.2018).

4. С начала этого года преступники похитили \$1,1 млрд в криптовалюте [Электронный ресурс]. URL: <https://cryptonews.one/kriptovaluta/s-nachala-ehotogo-goda-prestupniki-pokhitili-11-mlrd-v-kriptovaljute> (дата обращения: 08.10.2018).

5. Group-IB: Хакерские группировки променяли банки на рынок криптовалют [Электронный ресурс]. URL: <https://coinspot.io/technology/bezopasnost/group-ib-hakerskie-gruppirovki-promenyali-banki-na-rynok-kriptovalyut> (дата обращения: 08.10.2018).

6. Исследование: в 2018 году через криптовалюту отмоют около \$1,5 млрд [Электронный ресурс]. URL: <http://hodlweek.com/news/issledovanie-v-2018-godu-cherez-kriptovaliutu-otmoiut-okolo-15-mlrd> (дата обращения: 08.10.2018).

7. Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. № 6.

УДК 343.982.323

В.И. Елётнов

ОПРЕДЕЛЕНИЕ ПОЛОВОЙ ПРИНАДЛЕЖНОСТИ ЧЕЛОВЕКА В КРИМИНАЛИСТИЧЕСКОЙ ПРАКТИКЕ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ТРАНСГЕНДЕРНЫХ ЯВЛЕНИЙ

С 1 января 2019 г. в штате Нью-Йорк США вступит в силу закон, официально разрешающий жителям данной территории указывать в свидетельстве о рождении третий пол, обозначаемый как пол «X» [1]. Аналогичные законопроекты утверждены или находятся на стадии рассмотрения и в некоторых других штатах США (Калифорнии, Орегоне, Вашингтоне и Нью-Джерси), в Германии, Австрии, Австралии, Новой Зеландии, Канаде, Индии, Пакистане и Непале [2]. Мировое сообщество постепенно узаконивает интерсексуальность – различные комбинации мужских и женских половых признаков, которые не вписываются в традиционную бинарную систему, меняя традиционные представления о биологическом поле.

В контексте обозначенной тенденции отдельным пунктом стоит необходимость овладения сотрудниками правоохранительных органов терминами, обозначающими новые вариации половой принадлежности современного человека, визуальной диагностики их признаков.

Признавая существование третьего пола, законодатели и научное сообщество в первую очередь имеют в виду людей, которые родились с определенными физическими или биологическими половыми особенностями (например, гермафродитов, сочетающих в себе физиологические признаки обоих полов (в Беларуси гермафродитизм относят к гене-