Вестник Сибирского юридического института МВД России

УДК 343.98 : 004.7

**Павел Викторович ГАЛУШИН,**
доцент кафедры информационно-правовых дисциплин и специальной техники Сибирского юридического института МВД России (г. Красноярск),
кандидат технических наук
*galushin@gmail.com*

# СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ ЗНАНИЯ В ОБЛАСТИ ЦИФРОВОЙ ВАЛЮТЫ И МАЙНИНГА, НЕОБХОДИМЫЕ СОТРУДНИКАМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ДЛЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

# SPECIAL TECHNICAL KNOWLEDGE IN THE FIELD OF DIGITAL CURRENCY AND MINING, WHICH ARE NECESSARY FOR LAW ENFORCEMENT OFFICERS TO INVESTIGATE CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

В статье рассматривается вопрос о том, какие специальные технические знания в области цифровой валюты и майнинга необходимы для раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий. На примерах выявляется особая роль фундаментальной подготовки в освоении передовых технологий, а также целесообразность включения соответствующих тем в образовательный процесс вузов правоохранительных органов.

The article considers the issue of what special technical knowledge in the field of digital currency and mining is necessary to solve and investigate crimes committed using information and communication technologies. The examples highlight the special role of fundamental training in mastering advanced technologies, as well as the advisability of including relevant topics in the educational process at law enforcement educational institutions.

**Ключевые слова:** специальные знания, цифровая валюта, криптовалюта, майнинг, расследование и раскрытие преступлений.

***Keywords:*** *special knowledge, digital currency, cryptocurrency, mining, crime investigation.*

Преступления, совершаемые с использованием информационно-коммуникационных технологий, остаются одним из самых распространенных и быстро растущих категорий преступлений. Из всех преступлений, совершенных в России в 2023 г., каждое третье было совершено с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Подобных уголовно наказуемых деяний в 2023 г. было зарегистрировано на 29,7% больше, чем в 2022 г. Раскрыто преступлений в данной сфере было на 21% больше, чем в 2022 г.[1] Таким образом, раскрываемость преступлений, совершаемых с использованием информационно-коммуникационных технологий, снизилась. Можно констатировать, что их общественная опасность продолжает возрастать.

1 Состояние преступности в России за январь-декабрь 2023 года. URL: мвд.рф/reports/item/47055751/ (дата обращения: 09.02.2023).

Одной из самых современных информационно-коммуникационных технологий, используемых для совершения преступлений, является криптовалюта. Использование криптовалют при организации преступной деятельности существенно повышает степень конспирации злоумышленников, например в сфере незаконного оборота наркотиков. Однако за последние годы использование криптовалют и лежащей в основе их функционирования технологии блокчейн вышло за пределы исключительно преступной деятельности в данной сфере.

18 марта 2019 г. был принят Федеральный закон N 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», который ввел в ГК РФ понятие «цифровые права», родственное понятию токена в криптовалютах.

Федеральный закон от 31 июля 2020 г. N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» ввел понятие «цифровая валюта», под которое попадают существовавшие на тот момент криптовалюты.

Федеральным законом от 24 июля 2023 г. N 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» была введена новая форма российского рубля – цифровой рубль, основанная на ряде технологий, некоторые из которых используются в криптовалютах.

При реализации дистанционного электронного голосования в Российской Федерации используется технология блокчейн («цепочка блоков», п. 17 ст. 64.1 Федерального закона от 12 июня 2002 г. N 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»).

Криптовалюта сегодня не только используется при совершении преступлений как средство повышение конспирации, но и сама стала объектом преступных посягательств. Майнинг криптовалюты, в свою очередь, зачастую совершается с нарушением законодательства: хищением электроэнергии, распространением вредоносного программного обеспечения, неуплатой налогов от реализации криптовалюты.

Таким образом, криптография, технология блокчейн и криптовалюты сегодня становятся объектами рассмотрения гражданского, налогового, административного, уголовного и даже конституционного права.

Эффективная борьба с правонарушениями во всех перечисленных областях невозможна без хотя бы поверхностного понимания принципов функционирования соответствующих информационно-коммуникационных технологий. Например, определение наиболее подходящего правового механизма обеспечения сохранности криптовалюты в ходе расследования уголовного дела базируется на понимании того, что дает возможность распоряжаться счетом в криптовалюте [подр.: 3].

Данный тезис подтверждается проникновением упоминания конкретных технологий в тексты федеральных законов. Так, уже упоминавшийся Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» включает термин «цепочка блоков» (то есть технологии блокчейн) и ключей зашифрования и расшифрования (то есть несимметричной криптографии).

Кроме того, в гражданском праве в связи с введением понятия «цифровые права» появилась конструкция «в соответствии с правилами информационной системы». На наших глазах происходит смыкание понятия «доказательства» в математике и юриспруденции.

Таким образом, в некоторых фундаментальных для функционирования государства сферах информационно-коммуникационные технологии перестают быть для юриспруденции «черным ящиком», детали функционирования которого можно оставить техническим специалистам.

Одним из барьеров, затрудняющих понимание современных информационно-коммуникационных технологий специалистами в иных предметных областях (в том числе –

юриспруденции), является их очень динамичное развитие и постоянное появление новых технологий. Угнаться за всеми ними одному человеку просто невозможно. На сегодняшний день не существует специалистов в информационно-коммуникационных технологиях вообще, эта сфера дробится на области, которые все больше изолируются друг от друга. Это приводит к необходимости каждому человеку выбирать, какие конкретные информационно-коммуникационные технологии осваивать.

Одним из соображений, позволяющих осуществить такой выбор, является изучение таких технологий, польза от которых для профессиональной деятельности непосредственно очевидна. Однако для новых технологий степень полезности оценить практически невозможно: раз технология новая, то отсутствует опыт ее применения.

Но при таком подходе человек действует реактивно: он пассивно реагирует на происходящее. При таком подходе правоохранительные органы будут на позиции догоняющего в освоении информационно-коммуникационных технологий по сравнению с преступниками. Для того чтобы быть готовыми к появлению новых информационно-коммуникационных технологий, которые могут быть использованы при совершении преступлений, требуется проактивный подход.

Наблюдается так называемый эффект Линди [7]: чем дольше существует технология, тем больше вероятность, что она продолжит существовать. Иными словами, вероятность исчезнуть у технологии убывает со временем, то есть к ним неприменима логика жизненного цикла живых существ, у которых смертность растет с возрастом.

Эффект Линди приводит к парадоксальному выводу: для того чтобы быть успешным в информационно-коммуникационных технологиях, нужно не гнаться за «модными новинками», а изучать фундаментальные закономерности, лежащие в основе сразу большого класса подобных новинок.

Естественно, речь не идет о том, что новые технологии изучать бессмысленно вообще. Дело именно в выборе фокуса: на изучение чего специалисту нужно сделать ставку. Новые технологии можно и даже нужно изучать. Ведь даже проверенные временем к сегодняшнему дню технологии когда-то были новыми. Но при этом всегда нужно иметь в виду, что новое может потерять популярность так же быстро, как привлекло к себе внимание при появлении. По-настоящему же сосредоточиться стоит на технологиях и знаниях, которые существуют долго.

Рассмотрим, насколько высказанные соображения применимы к сфере цифровой валюты и майнинга. В основе криптовалюты лежит ряд технологий, которые одновременно появились достаточно давно, сохраняют актуальность и поныне, а также имеют широкий спектр приложений.

Для подтверждения права распоряжения кошельком криптовалюты используется электронная подпись, которая, в свою очередь, основана на несимметричной криптографии, а для связи блоков в блокчейне без существенного разрастания их объема используются хэш-функции.

И несимметричная криптография, и хэш-функции используются не только в цифровых валютах. Упрощенный аналог хэш-функции используется в номерах банковских карт для уменьшения вероятности случайной ошибки при их передаче. Последняя цифра номера карты является контрольной, то есть зависит от всех предыдущих. Значит, если при вводе номера карты допустить ошибку в одной цифре, то факт наличия ошибки можно обнаружить.

Несимметричная криптография применяется сегодня очень широко в силу того, что она позволяет организовать защищенный канал передачи информации поверх незащищенного, например по сети Интернет. Поэтому ее используют для авторизации и передачи данных онлайн-банки, социальные сети и вообще любые сайты, предусматривающие обмен с пользователями конфиденциальной информацией.

Кроме того, только несимметричная криптография позволяет организовать дис-

танционное электронное голосование с сохранением всех избирательных прав граждан Российской Федерации: «неизменности сохраняемых результатов волеизъявления избирателей, участников референдума и соблюдения тайны голосования, а также невозможности установления связи между персональными данными избирателя, участника референдума и результатом его волеизъявления».

Несимметричная криптография базируется на достижениях теории чисел, которые были получены в XVII-XVIII вв. (малая теорема Ферма и теорема Эйлера). В свою очередь, корни теории чисел могут быть легко прослежены и до нашей эры (понятие простого числа). Все упомянутые результаты по сложности не выходят за рамки школьной программы по математике.

Конкретная разновидность несимметричной криптографии, используемой в криптовалюте биткойн, основана на использовании так называемых эллиптических кривых. Соответствующие методы криптографии были предложены в 1985 г. [1], при этом изучение эллиптических кривых активно велось в XIX в., некоторые результаты, используемые в эллиптической криптографии, принадлежат Ньютону, а первое известное рассмотрение подобных кривых приведено в «Арифметике» Диофанта, написанной в III в. нашей эры.

Безусловно, разработка первой криптовалюты (биткойн) является блестящим достижением, а ее создатель или создатели были гениями сразу в нескольких областях. Но для того чтобы разобраться в принципах функционирования криптовалюты, нет необходимости быть настолько же гениальным: существуют полные описания функционирования биткойна, предназначенные для школьников [5].

Таким образом, несмотря на весьма недавнее появление криптовалют (2009 г. – появление биткойна, массовая известность среди широких слоев населения – 2017 г.), их принципы базируются на фундаментальных результатах, появившихся задолго до XXI в. и достаточно широко представленных в литературе. Таким образом, роль фундаментальных знаний для информационно-коммуникационных технологий на примере криптовалют подтверждается.

Одной из распространенных разновидностей преступлений, связанных с криптовалютой, в последние годы стало хищение электроэнергии для майнинга. Дело в том, что для зрелых криптовалют майнинг требует большого количества вычислительных ресурсов, а следовательно, и затрат на электроэнергию.

При расследовании таких преступлений актуальными для сотрудников органов внутренних дел становятся знания в области электротехники. Например, по количеству криптовалюты, полученной в результате майнинга, может быть оценен объем похищенной электрической энергии.

Беглый поиск по разделу «Юридическая пресса» справочной правовой системы «КонсультантПлюс» позволяет обнаружить несколько публикаций, в которых в качестве единицы измерения объема потребленной или произведенной электроэнергии ошибочно указан «киловатт в час» или «кВт/ч». В действительности, киловатт – это единица измерения мощности, то есть расхода энергии в единицу времени. Соответственно, единицей измерения электрической энергии может быть «киловатт-час» по аналогии с такой единицей измерения рабочего времени, как «человеко-год».

Некоторое знакомство с электротехникой и физикой позволило бы избежать подобных досадных ошибок. В случае научных публикаций их непосредственный вред невелик, но в случае юридически значимых документов ситуация может быть хуже: от ущерба репутации органов власти до признания недействительными протоколов следственных действий. Подчеркнем, что здесь снова идет речь о фундаментальном факте, не зависящем от новых моделей оборудования для майнинга.

Расследование преступлений, совершаемых с использованием криптовалюты или посягающих на счета в криптовалюте, является крайне сложным в силу анонимности кошельков. Однако обмен криптовалюты на материальные ценности (что и является конечной це-

лью большинства преступлений в этой сфере) в основном проходит через сайты-обменники или биржи, так как достаточно трудно найти контрагента, который бы согласился принять криптовалюту в качестве оплаты.

Это означает, что вопрос определения личности владельца кошелька криптовалюты сводится к отслеживанию цепочки транзакций, ведущих к кошельку на бирже или обменнике. Учет криптовалют децентрализован и информация обо всех транзакциях в криптовалюте доступна в открытых источниках, например сайтах бирж. Однако ручное отслеживание цепочек транзакций в реальных условиях требует много времени и чревато ошибками. Для автоматизации подобных действий были разработаны системы блокчейн-анализа, например «Прозрачный блокчейн», используемая Федеральной службой по финансовому мониторингу Российской Федерации [2].

Одной из основ систем блокчейн-анализа является теория графов: раздел математики, изучающий структуру связей объектов произвольной природы. В случае блокчейн анализа объектами выступают кошельки криптовалюты, а связями – переводы между кошельками.

Истоки теории графов восходят к античности: философ и математик Порфирий использовал изображение дерева как иллюстрацию дихотомического деления в работе «Введение» для классификации философского понятия материи [6], а дерево может быть рассмотрено как одна из разновидностей графов. Подлинное научное изучение графов началось, когда Леонард Эйлер в статье, изданной Петербургской академией наук, о решении знаменитой задачи о кенигсбергских мостах [4], датированной 1736 г., первым применил идеи теории графов при доказательстве некоторых утверждений. В XIX в. теория графов применялась в электротехнике и органической химии.

На сегодняшний день эта математическая теория очень активно применяется на практике, так как с помощью графов можно описывать компьютерные и социальные сети. Такое направление, как «анализ социальных сетей», может быть в значительной степени охарактеризовано как прикладная теория графов. Анализ социальных сетей может быть использован в раскрытии и расследовании преступлений, так как позволяет извлекать информацию, хранящуюся в сети Интернет в неявной форме.

Из сказанного видно, что в основе блокчейн-анализа, который появился относительно недавно, необходимого для раскрытия и расследования преступлений, совершаемых с использованием криптовалют, лежит теория графов, появившаяся в XVIII в. и окончательно сформировавшаяся в середине XX в. При этом данное научное направление имело правоохранительные приложения и до появления криптовалют. Специалисты, изучившие элементы теории графов для использования при анализе социальных сетей, получили определенное преимущество при изучении блокчейн-анализа.

Мы снова видим, что фундаментальные факты, установленные задолго до появления компьютеров, оказываются полезными с точки зрения изучения самых современных информационно-коммуникационных технологий.

Таким образом, современные тенденции в развитии информационно-коммуникационных технологий и их проникновение непосредственно в сферу правового регулирования общественных отношений на уровне федеральных законов требует совершенствования подготовки сотрудников органов внутренних дел. Это может происходить как на уровне высшего ведомственного образования, так и дополнительного профессионального образования (повышения квалификации).

При этом применительно к информационно-коммуникационным технологиям, связанным с цифровой валютой и блокчейн-технологиями, необходимо ориентироваться на сочетание фундаментальной подготовки и полезности преподаваемого материала для профессиональной служебной деятельности.

**Библиографический список**

1. Болотов, А.А. Элементарное введение в эллиптическую криптографию : протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: URSS, 2006. – 274 с. – ISBN 5-484-00444-6. – EDN QMQFVJ.

2. Бутенко, О.С. Криптовалюты как общественно-экономическое явление и объект криминалистического анализа / О.С. Бутенко // Бизнес. Образование. Право. – 2021. – N 4(57). – С. 217-222. – DOI 10.25683/VOLBI.2021.57.412. – EDN LOFGPY.

3. Карлов, А.Л. Процессуальные средства обеспечения сохранности криптовалюты в ходе расследования уголовного дела (на примере биткоина) / А.Л. Карлов, П.В. Галушин // Современное право. – 2020. – N 7. – С. 110-114. – DOI 10.25799/NI.2020.34.65.017. – EDN DCHTTG.

4. Мациевский, С.В. К истории теории графов. Зарождение / С.В. Мациевский, Г.В. Квитко // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. – 2021. – N 4. – С. 23-33. – EDN KUQQVZ.

5. Пошерстник, Б.Е. Биткоин. Блокчейн. Криптовалюты : лекции для старшеклассников / Б.Е. Пошерстник, М.Я. Пратусевич. – СПб: СМИО Пресс, 2023.

6. Проскурин, С.Г. Древо Порфирия и картина мира / С.Г. Проскурин // Идеи и идеалы. – 2017. – Т. 2. – N 2(32). – С. 132-139. – DOI 10.17212/2075-0862-2017-2.2-132-139. – EDN YUHGFH.

7. Талеб, Н.Н. Рискуя собственной шкурой: Скрытая асимметрия повседневной жизни / Н.Н. Талеб ; пер. с англ. Н. Караева. – М.: Азбука, 2018.