

ния «Концепции...» также следует дополнить четкими показателями, характеризующими формирование механизмов высокотехнологичного надзора (например, удельный вес мер прокурорского реагирования, реализованных в электронной среде).

### СПИСОК ИСТОЧНИКОВ

1. Федеральный закон от 17 января 1992 года № 2202-1 (ред. от 11.06.2022) «О прокуратуре Российской Федерации» // Ведомости СНД и ВС РФ. 1992. № 8. Ст. 366.

2. Приказ Генеральной прокуратуры РФ от 14 сентября 2017 г. № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Информационно-правовая система «Законодательство России». URL: <http://pravo.gov.ru/> (дата обращения: 25.07.2022).

3. Зенин С. С. Нормативно-правовое обеспечение деятельности органов государственной власти в условиях пандемии Covid-19 // Lex Russica. 2021. № 6. С. 66–70.

4. Иванченко Е. А. Организация деятельности прокуратуры в условиях дальнейшего научно-технического прогресса и цифровизации общества // Основы экономики, управления и права. 2020. № 5. С. 178–183.

5. Стрельников В.В. Проблемы информационного обеспечения в органах прокуратуры Российской Федерации // Правовое государство: теория и практика. 2020. № 6. С. 141–145.

УДК 343

**Шулякова Мария Владимировна**

студент, Ростовский институт (филиал)

ВГУЮ (РПА Минюста России)

г. Ростов-на-Дону, Российская Федерация

*mari.shulyakova.99@inbox.ru*

**Алибеков Шахизин Ильмутдинович**

доктор экономических наук, профессор

Ростовский институт (филиал)

ВГУЮ (РПА Минюста России)

г. Ростов-на-Дону, Российская Федерация

**Расследования криптовалютных преступлений,  
основанных на блокчейне**

*В данной статье автор затрагивает механизмы передачи зашифрованной информации технологии блокчейна. В связи с передачей и хранением различных данных, в том числе конфиденциальной информации при использовании криптовалюты, становится все чаще*

*и прощя совершение преступлений в этой сфере, таких как: приобретение оружия, мошенничество в крупных размерах, наркотических средств, легализации преступных доходов, преступления против государственной безопасности и ряд других. Рассмотрим, как исследуют «следы» в данных информационных, киберпреступлениях с использованием криптовалюты в криминальных целях, а также алгоритмы расследования и обработки ключевых данных для дальнейшей возможности привлечения к уголовной ответственности.*

***Ключевые слова:** блокчейн, криптовалюта, расследование киберпреступлений, информационно-телекоммуникационные технологии, биткоин-кошелек, транзакции.*

### **Shulyakova Maria Vladimirovna**

student, Rostov Institute (branch)

VSU (RPA of the Ministry of Justice of Russia)

Rostov-on-Don, Russian Federation

### **Alibekov Shakhizin Ilmutdinovich**

doctor of economics, professor

Rostov Institute (branch)

VSU (RPA of the Ministry of Justice of Russia)

Rostov-on-Don, Russian Federation

## **Investigations of cryptocurrency, crimes based on blockchain**

*In this article, the author touches upon the mechanisms for transferring encrypted information to blockchain technology. In connection with the transfer and storage of various data, including confidential information when using cryptocurrency, it is becoming more and more common to commit crimes in this area, such as: acquisition of weapons, large-scale fraud, narcotic drugs, money laundering, crimes against state security and a number of others. Let's consider how the «traces» in these informational, cybercrimes using cryptocurrency for criminal purposes are investigated, as well as algorithms for investigating and processing key data for the further possibility of bringing to criminal responsibility.*

***Keywords:** blockchain, cryptocurrency, cybercrime investigation, information and telecommunication technologies, bitcoin wallet, transactions.*

Блокчейн можно представить как непрерывную последовательную цепочку блоков, выстроенную на основе определенных правил, содержащую информацию. Связь между такими блоками цепи обеспечивается как определенной нумерацией, так и тем, что отдельный блок содержит свою собственную хеш-сумму и хеш-сумму блока, стоящего перед ним. Любое изменение в блоке изменит и информацию о его хеш-сумме [8, с. 2]. И если после изменяемого блока уже было создано продолжение цепи, то изменение станет весьма сложным. Все дело в том, что обычно копии таких цепочек хранятся на множестве компьютеров, которые независимы друг от друга, именно поэтому представляет широкий спектр возможностей для расследования преступлений и предупреждения киберпреступлений. Такие технологии позволяют отслеживать подозрительные транзакции, блокировать движение средств на счета потенциальных преступников и связанных с ними лиц. А также необходимые данные расследования (данные о самом преступном деянии и связанных с ним действий, био-

метрические данные граждан и лиц без гражданства, сведения о судимости, списки разыскиваемых лиц и прочее) сохраняются, в том числе в ряде баз данных судебной экспертизы, посредством чего становятся более доступными и безопасными.

Появились случаи угроз террористических группировок с требованиями криптовалюты, что в свою очередь отразило ей некую негативную сторону, как дополнительный предмет криминальных посягательств. Изначально криптовалюта не имели никаких границ обращения, что создает огромные риски в контроле и соответственно безопасности [2, с. 1]. Из-за этого ряд стран запрещают или ограничивают использование криптовалюты на своей территории. Сейчас появились различные компании, активно работающие над блокчейн-технологиями для борьбы с отмыванием денег.

Сегодня часто мы слышим о взломе и краже персональных данных, а также интеллектуальной собственности. И зачастую в раскрытии таких преступлений правоохранительные органы недостаточно подготовлены и оснащены. Охват таких преступлений велик, ведь они могут происходить как на местном уровне, например, взлом Yahoo, посягательство на 3 миллиарда учетных записей пользователей, а также участились случаи международного уровня, где правительство одной страны обвиняет во взломе другую, или ряд стран, что влияет на международные отношения в целом [3, с. 3].

Интеллектуальный уровень преступности растет прямо пропорционально развитию цифрового пространства. В даркнете возможно даже получить платную юридическую консультацию, т. е. существуют юристы, которые за биткоины проконсультируют вас, как выдать себя, не оставив следы, используя криптовалюту в криминальных целях. Существуют и другие виды организованной преступности, в которой задействованы профессиональные хакеры со всего мира. Криптокриминал стал частью реального мира преступности, людей похищают и требуют передачи адресов криптовалютных кошельков под угрозой смерти или причинения различного вида ущерба. Однако вернемся к тому, что биткоин-транзакции записываются в блокчейне, соответственно их можно отслеживать, в том числе доходы, полученные незаконным путем [4, с. 2]. Любой может загрузить историю транзакций биткоина и проверить ее, либо использовать один из ряда сервисов, чтобы проверить транзакцию онлайн.

Тщательно исследовав процессы блокчейна, можно установить учетные записи, которые, очевидно, относятся к одному биткоин-кошельку, а значит, регулируются одним и тем же пользователем. Описанное получило название кластеризации. Другим моментом, на который стоит обратить внимание, – остаток после первичной биткоин-транзакции направляют обратно на счет, но отличный от счета отправителя, начавшего данный финансовый процесс [5, с. 276]. И когда мы выявили, что несколько учетных записей связаны с одним субъектом, мы можем приступать к выявлению данного субъекта, а именно установлению его личности. Что опять же говорит о реальной работе блокчейн-расследования.

Из-за указанных ограничений конфиденциальности биткоина многие, и конечно же криминальные личности, переходят на новые криптовалюты, на-

пример Z-кэш и Монэро, которые создают минимум следов после транзакций. Названные криптовалюты, конечно, ставят конфиденциальность на планку значительно выше. Однако и здесь есть свои возможности для расследования. Группа исследователей Принстонского университета во главе с Мальтом Мозером посредством анализа и исследований доказали, что даже в отношении таких новых криптовалют можно установить более 60 % необходимых данных о транзакциях [6, с. 189].

Говоря об опыте нашей страны, в России уже почти 2 года существует сервис «Прозрачный блокчейн», который был создан Росфинмониторингом для отслеживания транзакций криптовалюты [7, с. 3]. Эта технология направлена не только на анализ самих транзакций, но и на выявление признаков преступных действий, благодаря чему постепенно нарабатывается практика расследований, а также судебная практика по таким делам. Более того, ранее отраженные особенности технологий блокчейна могут действительно содействовать в расследовании преступлений с криптовалютой. Наибольший уклон здесь не на установление личности преступника, в первую очередь необходимо установить все движения его средств и связь между ними, именно поэтому правоохранительным органам стоит взаимодействовать с криптовалютными компаниями для выявления и пресечения криминальной деятельности посредством блокчейн-технологий. Важно создание специальных групп для мониторинга с целью выявления подозрительной активности и блокировки таких незаконных финансовых операций [8, с. 2]. Разумеется, решение этой важной и сложной проблемы носит комплексный характер, и требует постоянного исследования и развития для усиления контроля и пресечения преступных финансовых обращений криптовалюты, в том числе для большего доверия в сфере безопасного пользования ею внутри стран и на международном уровне.

### СПИСОК ИСТОЧНИКОВ

1. Посиделки с кибер-детективами: расследуем преступления с криптовалютами // Безопасность. URL: <https://hub.forklog.com/posidelki-s-kiber-detektivami-rassleduem-prestupleniya-s-kriptovalyutami/> (дата обращения: 25.11.2022).

2. Возможности блокчейна в расследовании уголовных дел // Блокчейн. URL: <https://ru.bitcoinethereumnews.com/blockchain/opportunities-for-blockchain-in-police-investigations/> (дата обращения: 25.11.2022).

3. Журнал о блокчейне. URL: <https://blockchain24.pro/o-blokchejn-rassledovaniyah-i-specifike-kriptovalyutnyh-prestuplenij-s-georgiem-rahaevym> (дата обращения: 25.11.2022).

4. Крипто. URL: <https://www.rbc.ru/crypto/news/602fb2449a7947f67080807f> (дата обращения: 25.11.2022).

5. Мельников В. Ю. Уголовная ответственность за преступления : учеб. пособие. Ростов н/Д : Ростовский институт (филиал) ВГУЮ (РПА Минюста России, 2022. 565 с.

6. Проблемы реализации уголовной политики на современном этапе развития российского общества : монография. Ростов н/Д : ВГУЮ (РПА Минюста России), Ростовский институт (филиал), 2020. 270 с.

7. Сервисы для отслеживания блокчейн и их значение. URL: <https://cryptonews.net/ru/news/blockchain/5555673/> (дата обращения: 25.11.2022).

8. Умная безопасность. URL: <https://dzen.ru/media/id/5c88926728941b00b4b27d1a/prestuplenie-i-blokchein-instrumenty-analiza-blokcheinov-i-otslejivaniia-tranzakcii-v-rukah-pravoohranitelnyh-organov-5c88af0943a7b600b05bcb1f> (дата обращения: 25.11.2022).

УДК 343.98

**Яркова Елизавета Сергеевна**

студент, Костромской государственной университет  
г. Кострома, Российская Федерация  
*liza.yar@bk.ru*

**Галичева Анастасия Сергеевна**

студент, Костромской государственной университет  
г. Кострома, Российская Федерация  
*galicheva.anastasya@yandex.ru*

**Евстегнеев Алексей Сергеевич**

кандидат юридических наук, доцент  
Костромской государственной университет  
г. Кострома, Российская Федерация  
*vse-evstegneev@yandex.ru*

**Цифровизация деятельности следователя  
при раскрытии и расследовании преступлений**

*В данной статье авторы рассматривают вопросы использования следователями средств цифровизации в процесс раскрытия преступлений и расследования уголовных дел. Ими обращено внимание на широкое применение компьютерных и им подобных технических средств при производстве следственных действий. Также авторами рассмотрены проблемы, связанные с отсутствием, в действующем уголовно-процессуальном законодательстве России, норм, регулирующих порядок их использования в уголовном судопроизводстве, следовательно, не урегулирован вопрос признания полученных результатов доказательствами по уголовному. В связи с этим, в статье обосновывается целесообразность внесения дополнений и изменений в действующий Уголовно-процессуальный кодекс Российской Федерации, что позволило бы следователю, на законном основании, использовать средства цифровизации в его деятельности и снять вопросы о признании доказательствами результатов их применения в процессе расследования уголовных дел.*