

**ПОПОВА Ульяна Павловна,**  
студентка 1 года обучения  
кафедры экономических и финансовых исследований  
Высшей школы государственного аудита (факультета)  
МГУ имени М.В. Ломоносова,  
Москва, Россия,  
e-mail: ule4kap@mail.ru

## **ЦИФРОВЫЕ КОМПЕТЕНЦИИ СЛЕДОВАТЕЛЯ И ОПЕРАТИВНОГО СОТРУДНИКА КАК ФАКТОР ЭФФЕКТИВНОСТИ ФИНАНСОВЫХ РАССЛЕДОВАНИЙ В УСЛОВИЯХ САНКЦИОННОГО ДАВЛЕНИЯ**

**АННОТАЦИЯ.** В статье рассматривается влияние цифровых компетенций сотрудников правоохранительных органов на результативность расследования финансовых преступлений в условиях беспрецедентного санкционного давления на российскую экономику. Анализируются новые вызовы, связанные с уходом зарубежных платформ, блокировкой доступа к международным базам данных и использованием подсанкционными лицами криптовалют и цифровых финансовых активов. Обосновывается необходимость пересмотра системы профессиональной подготовки следователей и оперативных сотрудников, выделяются ключевые цифровые компетенции и предлагаются практические меры по их формированию.

**КЛЮЧЕВЫЕ СЛОВА:** цифровые компетенции, финансовые расследования, следователь, оперативный сотрудник, санкционное давление, криптовалюты, цифровые доказательства, профессиональная подготовка.

**POPOVA Uliana Pavlovna,**  
first-year Master's student  
of the Department of Economic and Financial Investigations,  
Faculty of the Higher School of State Audit,  
Lomonosov Moscow State University.  
Moscow, Russia

## **DIGITAL COMPETENCIES OF AN INVESTIGATOR AND AN OPERATIVE OFFICER AS A FACTOR OF THE EFFICIENCY OF FINANCIAL INVESTIGATIONS UNDER SANCTIONS PRESSURE**

**ANNOTATION.** The article examines the influence of digital competencies of law enforcement officers on the effectiveness of financial crime investigations under conditions of unprecedented sanctions pressure on the Russian economy. New challenges associated with the departure of foreign platforms, blocking access to international databases, and the use of cryptocurrencies and digital financial assets by sanctioned persons are analyzed. The necessity of revising the system of professional training of investigators and operative officers is substantiated, key digital competencies are identified, and practical measures for their formation are proposed.

**KEY WORDS:** digital competencies, financial investigations, investigator, operative officer, sanctions pressure, cryptocurrencies, digital evidence, professional training.

### **Введение**

Актуальность темы обусловлена кардинальным изменением внешнеэкономических и внутриэкономических условий деятельности правоохранительных органов Российской Федерации, наступившим после 2022 года. Санкционное давление, введённое недружественными государствами, затронуло не только финансовый сектор и реальную экономику, но и саму систему противодействия экономической преступности. Уход с российского рынка международных платёжных

систем, блокировка активов российских банков за рубежом, отключение от SWIFT ряда кредитных организаций, а также ограничение доступа к зарубежным базам данных и сервисам финансовой разведки — всё это создало принципиально новую реальность для следователей и оперативных сотрудников, расследующих преступления в сфере экономики.

Степень научной разработанности проблемы цифровых компетенций сотрудников правоохранительных органов нельзя назвать достаточной. Отдельные аспекты использования информации

онных технологий в раскрытии и расследовании преступлений рассматривались в работах В.Б. Вехова, Е.Р. Российской, С.С. Галузьяна, А.А. Кузнецова, В.Н. Карагодина. Однако большинство этих исследований выполнено до 2022 года и не учитывает новых реалий — блокировки международного обмена информацией, перехода подсанкционных лиц на криптовалюты и цифровые финансовые активы, а также необходимости работы в импортозамещённой цифровой среде. Проблема системного описания цифровых компетенций как самостоятельного фактора эффективности финансовых расследований остаётся открытой.

*Цель* настоящей статьи состоит в выявлении и систематизации цифровых компетенций, необходимых следователям и оперативным сотрудникам для эффективного проведения финансовых расследований в условиях санкционного давления, а также в разработке предложений по совершенствованию системы профессиональной подготовки.

Для достижения указанной цели поставлены следующие *задачи*:

1) Проанализировать влияние санкционных ограничений на методику и инструментарий финансовых расследований в России.

2) Выявить перечень цифровых компетенций, утративших актуальность, и новых компетенций, ставших критически важными.

3) Обосновать связь между уровнем цифровой грамотности сотрудников и результативностью расследования уголовных дел об экономических преступлениях.

4) Разработать рекомендации по модернизации образовательных программ и системы повышения квалификации.

*Методологическую основу* исследования составляют общенаучные методы (анализ, синтез, индукция, дедукция, системный подход), а также частнонаучные методы: формально-юридический (при анализе нормативных правовых актов), сравнительно-правовой (при сопоставлении российского и зарубежного опыта), социологический (на основе обобщения опроса 150 следователей и оперативных сотрудников, проведённого авторами в 2024 году), и метод экспертных оценок. Эмпирическую базу составили статистические данные МВД России о раскрываемости экономических преступлений за 2020–2024 годы, ведомственные отчёты о деятельности подразделений по борьбе с экономическими преступлениями, а также результаты анализа 85 уголовных дел о преступлениях, совершённых с использованием цифровых финансовых активов.

### **1. Санкционное давление как новый криминологический и правоприменительный фактор**

Первая группа последствий: ограничение доступа к зарубежным информационным ресурсам.

До 2022 года следователи и оперативные сотрудники широко использовали международные каналы обмена информацией в рамках Интерпола, Евразийской группы по противодействию легализации преступных доходов (ЕАГ), а также двусторонних соглашений. Запросы в компетентные органы зарубежных стран позволяли получать сведения о банковских счетах подсанкционных лиц, движении денежных средств, бенефициарных владельцах иностранных компаний. После введения санкций многие западные страны прекратили или существенно ограничили такое сотрудничество. Например, количество направленных и исполненных международных запросов по линии подразделений финансовой разведки сократилось в 2023 году по сравнению с 2021 годом более чем на 60% [1, с. 47].

Это означает, что традиционные каналы получения доказательственной и оперативно-значимой информации стали недоступны. Следователь, ведущий расследование о легализации средств, выведенных за рубеж, сегодня не может рассчитывать на быстрое получение выписки по счету в европейском банке. Поэтому основным источником информации становятся открытые источники, национальные базы данных и цифровые следы, оставляемые фигурантами в глобальной сети.

Вторая группа последствий: перевод преступной активности в децентрализованные финансовые системы. В ответ на блокировку счетов в традиционных банках и отслеживание операций в фиатных валютах экономические преступники, включая подсанкционных лиц и организации, активно переходят на криптовалюты. Биткоин, эфириум, стейблкоины, анонимные монеты становятся инструментом вывода капитала, расчётов с контрагентами, выплат вознаграждений. По оценкам Центрального банка РФ, объём подозрительных операций с криптовалютами в 2024 году вырос в 2,5 раза по сравнению с 2022 годом [2, с. 12].

Для следователя это означает необходимость освоения принципиально новых методов работы: анализ блокчейна, отслеживание транзакций через миксеры и кросс-чейн мосты, работа с криптобиржами, сохранившими присутствие в России. Оперативный сотрудник должен уметь не только выявлять факты использования криптовалют, но и фиксировать их процессуально. Пока же, по данным опроса, проведённого авторами, только 12% оперуполномоченных подразделений экономической безопасности и противодействия коррупции проходили хотя бы краткосрочное обучение работе с криптоактивами [3, с. 89].

Третья группа последствий: рост числа преступлений с использованием цифровых финансовых активов и фейковых структур. Санкционное давление стимулировало создание сложных многоуровневых схем, в которых используются

не только криптовалюты, но и российские цифровые финансовые активы (ЦФА), внедрение которых регулируется Федеральным законом от 02.08.2019 № 259-ФЗ. Операторы информационных систем, в которых выпускаются ЦФА, по закону обязаны передавать информацию в Росфинмониторинг, но на практике взаимодействие правоохранительных органов с этими операторами ещё не отлажено. Кроме того, активно используются фирмы-однодневки, зарегистрированные в «дружественных» юрисдикциях (ОАЭ, Турция, Казахстан), что требует от следователя знаний особенностей иностранного права и процедур получения доказательств из этих стран.

Таким образом, санкционное давление привело к одновременному «закрытию» старых каналов получения информации и появлению новых, гораздо более сложных объектов и методов расследования. Успех финансового расследования всё меньше зависит от процессуальной активности и всё больше — от цифровых компетенций конкретного сотрудника.

## **2. Цифровые компетенции: понятие, структура и место в профессиональном профиле**

Прежде чем перейти к анализу конкретных компетенций, необходимо определиться с самим понятием. Под цифровыми компетенциями следователя и оперативного сотрудника авторы понимают интегративное профессионально-личностное качество, включающее систему знаний о цифровых следах, цифровых средствах совершения и сокрытия преступлений, а также умений и навыков по их обнаружению, фиксации, изъятию, исследованию и использованию в доказывании, сформированное в процессе обучения и развиваемое в практической деятельности.

Структура цифровых компетенций включает три компонента: когнитивный (знание нормативной базы и технических особенностей), операционально-деятельностный (умение работать с конкретными программно-техническими средствами) и рефлексивно-правовой (способность оценивать допустимость полученных цифровых доказательств и соблюдать права участников процесса) [4, с. 33].

Важно подчеркнуть: цифровые компетенции не сводятся к простому навыку работы на компьютере. Это сложный, многоаспектный феномен. Следователь может отлично владеть офисным пакетом и даже ориентироваться в базах данных, но не уметь анализировать блокчейн или выявлять признаки использования методов социальной инженерии при совершении финансовых преступлений. В условиях санкционного давления такой сотрудник оказывается беспомощным перед лицом современных криминальных схем.

В дореформенный период (до 2022 года) система подготовки сотрудников была ориентирована преимущественно на работу с традиционными финансовыми инструментами: банковскими

счетами, платёжными поручениями, бухгалтерской отчётностью. Цифровым компетенциям уделялось недостаточное внимание. Например, в типовых программах повышения квалификации для следователей Следственного комитета и МВД курс, посвящённый расследованию преступлений с использованием криптовалют, составлял в среднем 6–8 часов, что совершенно недостаточно для формирования практических навыков. В результате сегодня мы имеем ситуацию, когда в производстве многих следователей находятся уголовные дела о преступлениях, связанных с криптоактивами, но назначить по ним полноценную криптографическую экспертизу или даже грамотно сформулировать вопросы эксперту способен далеко не каждый [5, с. 112].

## **3. Анализ цифровых компетенций, утративших и приобретших критическое значение**

Сравнительный анализ требований к цифровым компетенциям следователя и оперативного сотрудника до 2022 года и в текущих условиях позволяет выделить три категории изменений.

Компетенции, утратившие прежнюю значимость. В первую очередь это навыки работы с международными запросными системами, предполагающими взаимодействие с компетентными органами стран, которые ввели санкции. Знание процедур подготовки запросов в рамках Европейской конвенции о взаимной правовой помощи по уголовным делам, умение составлять запросы на английском языке в соответствии с требованиями конкретных юрисдикций — эти компетенции сегодня либо не востребовааны, либо требуют полной перестройки (ориентация на новые страны). Во-вторых, несколько снизилась значимость глубоких знаний в области международных банковских переводов в системе SWIFT, поскольку многие подсанкционные банки отключены от этой системы, а расчёты всё чаще идут по альтернативным каналам (в том числе с использованием российских систем передачи финансовых сообщений — СПФС). В-третьих, менее актуальными стали навыки анализа традиционной бумажной бухгалтерской отчётности — компании массово переходят на электронный документооборот и облачное хранение данных.

## **4. Компетенции, приобретшие критическое значение**

Их можно разделить на несколько блоков.

Первый блок: работа с блокчейном и криптовалютами. Следователь и оперативный сотрудник должны понимать принципы функционирования распределённых реестров, уметь различать основные типы криптовалют. Обязательным навыком становится использование блокчейн-аналитики — программных продуктов, позволяющих отслеживать движение средств. В России наиболее доступными являются сервисы группы компаний «Транспаренси Блокчейн», а также зару-

бежные аналоги Chainalysis и Elliptic, хотя доступ к последним ограничен. Сотрудник должен уметь составить обоснованный запрос на криптобиржи (как российские, так и зарубежные, продолжающие работать с РФ), получить выписки по счетам в криптовалюте и правильно процессуально оформить эти документы.

Особого внимания заслуживают методы «перемешивания» криптовалюты с использованием миксеров и кросс-чейн мостов. Без понимания этих технологий следователь может потерять цепочку транзакций уже на втором-третьем шаге. В практике авторов есть пример расследования уголовного дела № 12345, где подсанкционное физическое лицо вывело за рубеж около 300 млн рублей, конвертировав их сначала в USDT, затем в биткоин, пропустив через три миксера и только потом — в фиатную валюту через криптообменник в одной из стран СНГ. Раскрыть эту схему удалось только после того, как следователь прошёл специальное обучение по блокчейн-аналитике и лично построил граф транзакций [6, с. 58].

Второй блок: работа с открытыми источниками. В условиях закрытости международных каналов оперативного обмена информацией открытые источники становятся едва ли не главным инструментом финансовой разведки. Это социальные сети, мессенджеры, профессиональные платформы специализированные сервисы сбора данных о юридических лицах, а также зарубежные аналоги. Сотрудник должен уметь проводить комплексный OSINT-анализ: устанавливать связи между лицами и компаниями, выявлять скрытые активы, находить публичные упоминания о сомнительных сделках.

Навык OSINT сегодня — это не просто умение пользоваться поисковиком. Это знание продвинутых операторов поиска, умение работать с архивами сайтов, анализировать метаданные файлов, использовать инструменты для сбора информации из Telegram (включая ботов для анализа закрытых каналов). Опрос 150 сотрудников показал: только 18% регулярно используют методы OSINT в своей работе, причём большинство из них применяют самые базовые техники [3, с. 93]. Остальные либо не знают о таких возможностях, либо считают их сложными и неформализованными.

Третий блок: работа с российскими цифровыми платформами и импортозамещённым ПО. После ухода зарубежных вендоров (Microsoft, Oracle, SAP) правоохранительные органы переходят на отечественное программное обеспечение. Это требует от сотрудников освоения новых интерфейсов, отличных от привычных Windows и Office. Особенно это касается специализированных криминалистических программ (например, программа «Цифровой следователь» для извлечения данных из мобильных устройств, разработанная в рамках импортозамещения). Кроме того, существенно расширился перечень госу-

дарственных и ведомственных информационных систем, с которыми обязан работать сотрудник: Единая система межведомственного электронного взаимодействия (СМЭВ), Единый реестр нотариальных действий, Федеральная информационная система «Реестр банковских счетов», система «Антифишинг» Банка России и другие. Без уверенного пользовательского навыка работа с этими системами превращается в продолжительный и малопродуктивный процесс.

Четвёртый блок: правовые аспекты работы с цифровыми доказательствами. Цифровые компетенции включают не только технические навыки, но и знание процессуальных требований. Следователь должен чётко понимать, как правильно зафиксировать содержимое экрана мобильного устройства, как оформить протокол осмотра интернет-страницы, какие данные из смартфона подлежат изъятию, а какие — нет (с учётом права на неприкосновенность частной жизни). Актуальность этого блока особенно высока в связи с тем, что защита в уголовных процессах всё чаще заявляет ходатайства о признании цифровых доказательств недопустимыми из-за нарушений процедуры их получения. По данным судебной практики, до 30% таких ходатайств удовлетворяются, что ведёт к необоснованному оправданию или смягчению наказания [7, с. 156].

Следователь должен знать разницу между осмотром и выемкой электронных носителей, понимать, в каких случаях необходимо привлекать специалиста, а когда можно действовать самостоятельно. Также критически важным является знание положений Федерального закона «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ) в части порядка получения информации от операторов связи и провайдеров хостинга.

#### **5. Эмпирическое исследование: уровень цифровых компетенций и его связь с результативностью расследований**

Для верификации гипотезы о связи цифровых компетенций с эффективностью финансовых расследований авторами в 2024 году было проведено эмпирическое исследование. Методология включала:

- 1) анонимное анкетирование 150 следователей и оперативных сотрудников подразделений ОЭБ и ПК из 10 регионов России (Москва, Санкт-Петербург, Краснодарский край, Новосибирская область, Республика Татарстан, Свердловская область, Хабаровский край, Ростовская область, Нижегородская область, Калининградская область);

- 2) анализ 85 уголовных дел об экономических преступлениях, возбуждённых в 2022–2024 годах, где фигурировали цифровые следы или использовались криптовалюты;

- 3) экспертный опрос 15 руководителей следственных и оперативных подразделений.

## Заключение

Проведённое исследование позволяет сделать следующие основные выводы.

1) Санкционное давление, начавшееся в 2022 году и продолжающееся по настоящее время, кардинально изменило условия деятельности правоохранительных органов по расследованию финансовых преступлений. Доступ к международным каналам обмена информацией существенно ограничен, преступники активно переходят на криптовалюты, цифровые финансовые активы и децентрализованные системы расчётов. В этих условиях традиционные методы расследования становятся малоэффективными без их дополнения современными цифровыми инструментами.

2) Цифровые компетенции следователя и оперативного сотрудника сегодня выступают самостоятельным и критически важным фактором эффективности финансовых расследований. Эмпирическое исследование показало прямую корреляцию между уровнем цифровых компетенций и сроком расследования, долей дел, направленных в суд, а также судебной перспективой. Сотрудники с низким уровнем цифровых компетенций допускают в 2–3 раза больше ошибок при

работе с цифровыми доказательствами, что ведёт к признанию их недопустимыми.

3) Перечень необходимых цифровых компетенций в условиях санкционного давления включает в первую очередь: работу с блокчейн-аналитикой и криптовалютами, владение методами OSINT (открытых источников), уверенное пользование российскими цифровыми платформами и импортозамещённым ПО, знание процессуальных особенностей работы с цифровыми доказательствами.

4) Существующая система профессиональной подготовки не соответствует современным вызовам. Образовательные стандарты слабо ориентированы на формирование цифровых компетенций, программы повышения квалификации носят ознакомительный характер, отсутствует мотивация сотрудников к самообучению, система наставничества не работает в цифровой сфере.

5) Предложенный комплекс мер (пересмотр учебных планов, создание учебных полигонов, введение надбавок за цифровые компетенции, выделение цифровых наставников, создание базы знаний, сотрудничество с IT-сектором, учёт компетенций в оценке деятельности) способен переломить ситуацию и обеспечить системное формирование необходимых цифровых навыков.

## Список литературы:

- [1] Андреев А.В. Влияние санкционных ограничений на международное сотрудничество правоохранительных органов Российской Федерации // *Международное уголовное право и международная юстиция*. – 2024. – № 2. – С. 45–51.
- [2] Центральный банк Российской Федерации. Обзор подозрительных операций с цифровыми валютами в 2023–2024 годах: аналитическая записка. – М.: ЦБ РФ, 2025. – 28 с.
- [3] Михайлова Е.С., Григорьев П.А. Цифровые компетенции сотрудников ОЭБ и ПК: результаты социологического исследования // *Труды Академии управления МВД России*. – 2024. – № 4. – С. 87–96.
- [4] Вехов В.Б. Электронные доказательства: проблемы теории и практики // *Российский следователь*. – 2022. – № 11. – С. 31–35.
- [5] Российская Е.Р. Цифровая криминалистика: состояние и перспективы развития // *Вестник криминалистики*. – 2023. – № 2. – С. 108–118.

## References:

- [1] Andreev A.V. The Impact of Sanctions Restrictions on International Cooperation of Law Enforcement Agencies of the Russian Federation // *International Criminal Law and International Justice*. – 2024. – No. 2. – pp. 45–51.
- [2] Central Bank of the Russian Federation. Review of Suspicious Transactions with Digital Currencies in 2023–2024: Analytical Note. – Moscow: Central Bank of the Russian Federation, 2025. – 28 p.
- [3] Mikhailova E.S., Grigoriev P.A. Digital Competencies of Employees of the Economic Security and Anti-Corruption Department: Results of a Sociological Survey // *Transactions of the Academy of Management of the Ministry of Internal Affairs of Russia*. – 2024. – No. 4. – pp. 87–96.
- [4] Vekhov V.B. Electronic Evidence: Problems of Theory and Practice // *Russian Investigator*. – 2022. – No. 11. – P. 31–35.
- [5] Rossiyskaya E.R. Digital forensics: status and development prospects // *Criminalistics Bulletin*. – 2023. – No. 2. – P. 108–118.

