УДК 349

# *ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СМИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ*

***Коньшина Н.С.***

*студент,*

*Белгородский государственный национальный исследовательский университет*

*Белгород, Россия*

***Федорова В.А.***

*студент,*

*Белгородский государственный национальный исследовательский университет*

*Белгород, Россия*[1]

**Аннотация:** В статье рассматриваются организационные аспекты расследования преступлений, совершаемых с использованием средств массовой информации и информационно-телекоммуникационных сетей. Автор анализирует специфику объекта и предмета расследования, проблемы межведомственного и международного взаимодействия, кадрового обеспечения и собирания электронных доказательств. Отмечается, что традиционные криминалистические методики плохо работают в цифровой среде, а существующие механизмы правовой помощи не рассчитаны на скорость цифровых процессов. На основе доктринальных позиций и складывающейся практики предлагаются направления совершенствования: формирование специализированных следственных подразделений, разработка типовых алгоритмов действий, упрощение процедур получения данных от операторов связи и интернет-провайдеров, переход к

[1]**Научный руководитель:** Ярощук И.А., доцент кафедры судебной экспертизы и криминалистики, Юридический институт НИУ «БелГУ», Белгород, Россия

оперативным каналам международного обмена информацией. Делается вывод о том, что ключевым фактором остаётся человеческий — следователь, способный мыслить в цифровых категориях, и организация, способная обеспечить ему условия для такой работы.

**Ключевые слова:** организация расследования, средства массовой информации, информационно-телекоммуникационные сети, электронные доказательства, киберпреступность, трансграничность, межведомственное взаимодействие, специализация следователей, цифровая платформа, международная правовая помощь.

## *ORGANIZATIONAL ASPECTS OF INVESTIGATING CRIMES COMMITTED USING THE MEDIA AND INFORMATION AND TELECOMMUNICATION NETWORKS*

***Konshina N.S.***
*student,*
*Belgorod State National Research University*
*Belgorod, Russia*

***Fedorova V.A.***
*student,*
*Belgorod State National Research University*
*Belgorod, Russia*[2]

**Annotation:** The article examines the organizational aspects of investigating crimes committed using mass media and information and telecommunications networks. The author analyzes the specifics of the object and subject of the investigation, the problems

[2] **Scientific supervisor:** Yaroshchuk I.A., Associate Professor at the Department of Forensic Science and Criminalistics, Law Institute, Belgorod State National Research University, Belgorod, Russia

of interdepartmental and international cooperation, staffing, and the collection of electronic evidence. It is noted that traditional forensic methods do not work well in a digital environment, and existing legal assistance mechanisms are not designed to cope with the speed of digital processes. Based on doctrinal positions and existing practice, the following areas for improvement are proposed: the formation of specialized investigative units, the development of standard action algorithms, the simplification of procedures for obtaining data from telecommunications operators and internet service providers, and the transition to operational channels for international information exchange. It is concluded that the key factor remains the human element — an investigator capable of thinking in digital terms, and an organization capable of providing them with the conditions for such work.
**Keywords:** investigation organization, mass media, information and telecommunications networks, electronic evidence, cybercrime, cross border nature, interdepartmental cooperation, specialization of investigators, digital platform, international legal assistance.

Преступления, совершаемые с использованием средств массовой информации и информационно-телекоммуникационных сетей, перестали быть экзотикой. Сегодня это рутина - ежедневная, массовая, плохо поддающаяся традиционным криминалистическим методикам. Следователь, привыкший работать с материальными следами, вдруг оказывается в ситуации, где «место происшествия» - это сервер в другой юрисдикции, а «потерпевший» и «подозреваемый» никогда не встречались в реальном мире. Организация расследования таких деяний требует перестройки привычных алгоритмов, и перестройка эта идёт медленно и болезненно.

Первое, с чем сталкивается следователь, - это размытость границ преступного деяния. Если при «обычной» краже есть физическое место, время и очевидцы, то при преступлении в сети всё это либо отсутствует, либо существует в виде цифровых артефактов, которые ещё нужно найти и зафиксировать. Как отмечает

В.В. Поляков, «Особенности компьютерных преступлений часто проявляются в технически сложных способах их совершения и оставляемой при этом специфической следовой картине, включающей особый вид следов - электронно-цифровых. Обстановка совершения таких преступлений также весьма необычна, поскольку объективная сторона преступной деятельности разворачивается в кибернетическом пространстве» [1].

СМИ как инструмент совершения преступления добавляют ещё один слой сложности. Публикация в газете или на новостном портале - это одновременно и способ совершения деяния (например, клеветы или разжигания ненависти), и доказательство. Организация расследования требует взаимодействия со редакциями, а это - отдельная процессуальная процедура, где нужно балансировать между интересами следствия и гарантиями свободы массовой информации, закреплёнными в Законе РФ «О средствах массовой информации».

Преступления в сети почти всегда выходят за пределы одного региона, а часто - и одного государства. Сервер может находиться в Нидерландах, платёжная система - в США, а исполнитель - в соседнем субъекте Федерации. Особенностью всех компьютерных преступлений является транснациональность (трансграничность), ответственность за эти деяния предусмотрена законодательством различных государств. Именно трансграничность преступных деяний значительно усложняет установление места совершения преступлений, затрудняет их раскрытие, расследование и профилактику совершения. Преступления в сфере компьютерной информации могут начаться на территории одного государства, а продолжаться и закончиться на территории других государств. Кроме того, последствия, наступившие на территории одного государства, могут отражаться на территориях, находящихся под юрисдикцией других государств. Расстояния, пограничный контроль, равно, как и необходимость физического присутствия в таких ситуациях неважны.

На национальном уровне ситуация усложняется тем, что разные ведомства обладают разной компетенцией. МВД, ФСБ, Роскомнадзор, Банк России — каждый

работает в своей нише, и координация между ними оставляет желать лучшего. Концепция государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий, утверждённая распоряжением Правительства РФ от 30 декабря 2024 г. № 4154-р, прямо предусматривает создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком РФ, кредитными организациями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети «Интернет» и иных информационных технологий (за исключением компьютерных атак и компьютерных инцидентов) [2]. Это шаг в правильном направлении, но пока - только на бумаге.

Международное взаимодействие ещё сложнее. Запрос о правовой помощи в «цифровом» деле может идти месяцами, а данные на серверах зарубежных провайдеров за это время неоднократно перезаписываются. К.К. Клевцов отмечает, «К процессуальным трудностям также стоит отнести длительные сроки получения электронной информации, необходимой для расследования обозначенных выше преступлений, в рамках исполнения запроса об оказании правовой помощи. В основном это связано с отсутствием в многосторонних и двусторонних документах обязательства предоставлять ответ в течение определенного срока» [3].

Организация расследования немыслима без людей, которые понимают, что делают. Следователь, не разбирающийся в сетевых протоколах, логах и криптовалютах, обречён на поверхностное расследование. Между тем специализация в этой сфере идёт трудно. С одной стороны, создаются специализированные подразделения (как того требует упомянутая Концепция), с другой - их комплектование сталкивается с объективными трудностями: техническая грамотность стоит дорого, а конкурентная среда в IT-сфере предлагает специалистам куда более привлекательные условия.

Ю.В. Волкова ещё несколько лет назад предупреждала: «Высокие технологии развиваются такими темпами, что отставание будет, и, прежде всего в сферах далеких от технологий, таких как юриспруденция. Специалисты не появятся сами по себе, их необходимо готовить, а для правовой сферы специально и постоянно. Кроме того, необходимо совершенствовать уже работающих специалистов» [4]. Эта оценка остаётся актуальной и сегодня.

Организационно эта проблема выглядит наиболее остро. Электронные доказательства нестабильны: их легко изменить, удалить, подделать. Процедура изъятия должна быть выстроена так, чтобы обеспечить их целостность и допустимость. На практике же нередки случаи, когда следователь ограничивается распечаткой страницы сайта, не фиксируя метаданные, или изымает жёсткий диск без надлежащего описания его состояния.

А.И. Туршин подчёркивает, «Обычный осмотр электронного документа без предварительной фиксации его содержимого не позволяет достоверно установить, были ли внесены в него какие-либо изменения. Правило о возможности подтвердить целостность электронного доказательства при помощи цифровых технологий: видеозаписи процесса собирания доказательства, прикрепления к процессуальным документам хеш-значения (контрольной суммы) электронного доказательства либо электронной подписи. Такое требование, по сути, придаёт произвольной электронной информации процессуальный статус полноценного электронного документа, а затем и доказательства, поскольку она наделяется рядом реквизитов, которые могут иметь процессуальное значение для подтверждения целостности и достоверности данных в ходе их копирования и длительного хранения» [5]. Организационно это означает необходимость участия специалиста на всех этапах - от осмотра до экспертизы, а не только на финальной стадии.

Что можно предложить? Во-первых, необходимо ускоренное формирование специализированных следственных подразделений с чёткой вертикалью подчинения и едиными методическими стандартами. Во-вторых, требуется разработка типовых алгоритмов действий для наиболее распространённых

категорий дел - от фишинга до распространения запрещённого контента через СМИ. В-третьих, назрела необходимость упрощения процедур получения данных от операторов связи и интернет-провайдеров - в разумных пределах, с сохранением судебного контроля. Наконец, в-четвёртых, международное сотрудничество в цифровой сфере должно перейти от громоздких запросов о правовой помощи к оперативным каналам обмена, что требует как политической воли, так и технологической инфраструктуры.

Организация расследования преступлений, совершаемых с использованием СМИ и информационно-телекоммуникационных сетей, - это вызов, на который система пока отвечает реактивно. Создание специализированных подразделений, разработка платформ обмена информацией и совершенствование законодательства - всё это необходимые, но недостаточные меры. Ключевым остаётся человеческий фактор: следователь, способный мыслить в цифровых категориях, и организация, способная обеспечить ему условия для такой работы. Без этого любые концепции останутся декларациями.

**Библиографический список:**

1. Поляков, В. В. Основы методики расследования компьютерных преступлений : учебное пособие / В. В. Поляков ; Алтайский государственный университет. — Барнаул : Изд-во АлтГУ, 2024. — 121 с. — Текст : непосредственный. URL: https://epk.asu.ru/wp-content/uploads/2024/11/Итог_Уч.-пособ-Основы-методики-расследования-КП-2.pdf

2. О Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р // Собрание законодательства Российской Федерации. — 2025. — № 2. — Ст. 76. URL: https://www.law.ru/npd/doc/docid/1310847113/modid/99

3. Клевцов К. К. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕС КИБЕРПРЕСТУПНОСТЬЮ В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ НОВЫМ ВЫЗОВАМ И УГРОЗАМ // Вестник СПбГУ. Серия 14. Право. 2022. №3. URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbes-kiberprestupnostyu-v-kontekste-protivodeystviya-novym-vyzovam-i-ugrozam

4. Ю. В. Волкова О подготовке следственных работников и об эффективности расследования компьютерных преступлений (впервые опубликована: Волков Ю. В. Вопросы эффективного расследования компьютерных преступлений // Проблемы профилактики и противодействия компьютерным преступлениям: материалы Междунар. науч.-практ. конференции. Челябинск, 2008. С. 42–48. URL: https://telecomlaw.ru/articles/v_edu_invest_staff.pdf

5. Туршин А.И. Электронные доказательства в уголовном процессе: опыт зарубежных стран и российские перспективы // Юридические исследования. 2025. № 9. С. 1-11. DOI: 10.25136/2409-7136.2025.9.75764 EDN: YGMMIK URL: https://nbpublish.com/library_read_article.php?id=75764