УДК 343.98.062

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Воинский Владислав Александрович
студент магистратуры
Московский государственный университет
технологий и управления им. К.Г. Разумовского (ПКУ)
Москва, Россия

ОСНОВНЫЕ НАПРАВЛЕНИЯ И СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация

Рассматриваются вопросы интеграции современных информационных и цифровых технологий в деятельность правоохранительных органов по раскрытию и расследованию преступлений. Проводится анализ текущего состояния нормативно-правового и технического обеспечения следственной работы в условиях цифровизации криминальной среды, включая специфику работы с электронными следами, биометрическими данными и виртуальным пространством. Результатами исследования являются разработанные теоретические и практические предложения по совершенствованию механизмов фиксации доказательств и превентивного выявления преступлений. Предложено внедрение ведомственной децентрализованной платформы на базе технологии блокчейн для обеспечения целостности цифровых улик, а также создание адаптивных нейросетевых модулей предиктивной аналитики для борьбы с латентной киберпреступностью. Сделан вывод о необходимости системной трансформации подходов к расследованию, включающей создание гибридных следственных инструментов и адаптацию образовательных стандартов для формирования междисциплинарных компетенций у сотрудников правоохранительных органов.

Ключевые слова: раскрытие преступлений, компьютерные технологии, электронные следы, цифровые доказательства

Стремительная цифровизация всех сфер общественной жизни привела к качественной трансформации криминальной среды, порождая новые виды противоправных деяний и видоизменяя традиционные составы преступлений. Современная правоохранительная деятельность сталкивается с необходимостью не просто адаптации к цифровым реалиям, но и опережающего внедрения высокотехнологичных инструментов. Актуальность темы обусловлена тем, что информационное пространство становится одновременно и средой совершения преступлений, и источником доказательственной информации.

Эффективность работы следственных органов сегодня находится в прямой зависимости от степени интеграции специализированного программного обеспечения, алгоритмов искусственного интеллекта и методов анализа больших данных в повседневную практику. Рассматриваемая проблематика охватывает широкий спектр вопросов: от фиксации электронных следов до применения биометрической идентификации личности.

Первостепенное значение приобретает анализ роли информационных технологий как инструмента повышения качества следственной работы. Н. А. Милов

справедливо отмечает, что перспективы использования таких средств позволяют существенно оптимизировать процесс сбора доказательств и сократить сроки расследования [3, с. 218]. Внедрение автоматизированных рабочих мест, баз данных и аналитических систем создает фундамент для перехода от интуитивного поиска к научно обоснованному алгоритму выявления преступных связей. Цифровая трансформация уголовного судопроизводства требует пересмотра традиционных тактических приемов, поскольку объект посягательства и орудия преступления все чаще имеют виртуальную природу.

Особое внимание следует уделить феномену электронных следов. В отличие от материальных объектов, цифровая информация обладает свойствами легкой копируемости, модифицируемости и возможности удаленного уничтожения. Д. А. Влезько и В. В. Онипко указывают, что использование современных методов для работы с такими следами становится обязательным условием успешного расследования [2, с. 38]. К данной категории относятся не только файлы на носителях, но и лог-файлы серверов, метаданные, следы сетевой активности и транзакции в блокчейн-сетях. Работа с названными объектами требует привлечения специалистов, обладающих глубокими познаниями в области компьютерной криминалистики, способных обеспечить целостность и неизменность изымаемых данных для их последующего признания допустимыми доказательствами в суде.

Специфика современной преступности характеризуется активным использованием информационно-телекоммуникационных сетей для совершения мошеннических действий, распространения запрещенной информации и координации преступных групп. М. А. Нуров подчеркивает, что актуальные проблемы раскрытия таких деяний связаны с анонимностью пользователей, трансграничным характером сетей и использованием средств шифрования [4, с. 675]. Правоохранительные органы вынуждены противостоять технически подкованным злоумышленникам, применяющим VPN-сервисы, прокси-серверы и теневой сегмент интернета DarkNet. В сложившейся ситуации традиционные оперативно-разыскные мероприятия должны дополняться высокотехнологичной разведкой на основе открытых источников (OSINT) и специализированным мониторингом закрытых каналов связи.

Отдельным вектором развития выступает применение цифровых инструментов в расследовании преступлений против личности, в том числе половой неприкосновенности. Ф. А. Вестов и Д. Д. Карпова анализируют практику

использования технологий в раскрытии половых преступлений, не связанных с насилием, акцентируя внимание на анализе переписки в социальных сетях и мессенджерах [1, с. 57]. Выявление «груминга» и иных форм дистанционного психологического воздействия на жертву становится возможным благодаря семантическому анализу текстовых сообщений и восстановлению удаленных диалогов. Указанный подход позволяет формировать доказательную базу даже при отсутствии физического контакта между преступником и потерпевшим, основываясь на цифровых следах коммуникации.

Биометрические технологии представляют собой еще один значимый сегмент технических средств, кардинально меняющий тактику розыска. А. Д. Чайка рассматривает возможности биометрии, включая распознавание лиц, голоса и походки, как действенный механизм установления личности подозреваемых [7, с. 630]. Системы видеонаблюдения, интегрированные с базами данных розыска, позволяют в режиме реального времени фиксировать перемещение интересующих лиц. Однако применение биометрии сопряжено с необходимостью обеспечения высокой точности алгоритмов и исключения ошибок идентификации, что требует постоянного совершенствования нейросетевых моделей, лежащих в основе таких систем. Развитие геномной регистрации и создание федеральных баз данных ДНК также относится к сфере высокотехнологичного обеспечения расследования, позволяя связывать разрозненные эпизоды преступной деятельности в единую серию.

Комплексное применение компьютерных технологий невозможно без соответствующего нормативного и организационного обеспечения. К. И. Озеров указывает на необходимость адаптации уголовно-процессуального законодательства к реалиям цифровой эпохи, предлагая рассматривать цифровые данные как самостоятельный вид доказательств [5, с. 55]. Процессуальное оформление изъятия электронной информации, осмотр веб-сайтов и облачных хранилищ требуют четкой регламентации для исключения возможности оспаривания полученных результатов стороной защиты.

Вместе с тем, Д. В. Теткин и И. С. Воронина обращают внимание на перспективу применения совершенно новых компьютерных технологий, таких как виртуальная и дополненная реальность, для реконструкции обстановки места происшествия [6, с. 84]. Моделирование событий преступления в виртуальном пространстве позволяет проводить следственные эксперименты с высокой степенью детализации, проверять

показания участников и наглядно демонстрировать механизм совершения деяния суду и присяжным заседателям. Подобная визуализация способствует лучшему восприятию сложной технической информации участниками процесса, не обладающими специальными познаниями.

Несмотря на очевидный прогресс, практика выявляет ряд существенных затруднений. М. В. Шматов анализирует проблемы раскрытия преступлений в сфере компьютерной информации, указывая на дефицит квалифицированных кадров и отставание технического оснащения подразделений от уровня оснащенности киберпреступников [8, с. 199]. Скорость появления новых вредоносных программ и схем хищения средств опережает темпы разработки антивирусного ПО и методик расследования. Критическим фактором становится время реакции на инцидент: чем быстрее происходит фиксация цифрового следа, тем выше вероятность успешного раскрытия, однако бюрократические процедуры зачастую замедляют данный процесс.

На основании проведенного анализа литературы и текущего состояния практики, представляется необходимым предложить собственные методы улучшения и совершенствования деятельности по раскрытию преступлений с использованием IT-технологий. Выявленные проблемы фрагментарности используемого софта и сложности в процессуальном закреплении цифровых доказательств требуют системного решения.

Предлагается разработка и внедрение единой децентрализованной платформы фиксации цифровых доказательств на основе технологии распределенного реестра (блокчейн). Суть предложения заключается в создании закрытой ведомственной сети, куда загружаются хеш-суммы всех изымаемых цифровых объектов (образы жестких дисков, дампы памяти, скриншоты переписок) непосредственно в момент их обнаружения. Такой подход гарантирует неизменность данных: любая попытка модификации файла приведет к несовпадению хеш-суммы, что будет зафиксировано в реестре. Внедрение указанной системы позволит исключить обвинения в фальсификации доказательств со стороны защиты и повысит доверие суда к материалам, полученным электронным путем. Техническая реализация возможна путем создания специализированного программно-аппаратного комплекса для следователей, автоматически генерирующего и отправляющего метаданные в блокчейн при проведении осмотра.

Вторым направлением совершенствования должна стать разработка адаптивного нейросетевого модуля предиктивной аналитики для выявления латентных киберпреступлений. Существующие системы часто работают постфактум, реагируя на уже совершенные деяния. Предлагаемый метод заключается в создании ИИ-агентов, способных анализировать большие массивы неструктурированных данных в открытом сегменте сети и даркнете для выявления паттернов подготовки к преступлению. Модуль должен обучаться на базе данных раскрытых дел, выявляя неочевидные корреляции в поведении пользователей, специфическом сленге и транзакционной активности. Отличительной чертой данной разработки должна стать способность к семантическому анализу контекста, что позволит отличать реальные угрозы от информационного шума. Например, в контексте половых преступлений, упоминаемых Вестовым и Карповой [1], нейросеть могла бы выявлять паттерны «груминга» на ранних стадиях по лингвистическим маркерам манипуляции, передавая сигналы оперативным подразделениям для превентивного вмешательства.

Третьим предложением является внедрение технологии «виртуального полигона» для автоматизированного моделирования векторов кибератак. При расследовании инцидентов, связанных с неправомерным доступом к компьютерной информации, следователю часто сложно понять механизм взлома. Предлагаемая система будет создавать изолированную виртуальную копию инфраструктуры потерпевшего и в автоматическом режиме симулировать возможные сценарии атаки, используя известные методы эксплойтов. Результатом работы системы станет вероятностная карта уязвимостей, использованных преступником, что сузит круг подозреваемых до лиц, обладающих конкретными техническими компетенциями. Такой метод позволит перевести техническую экспертизу на новый уровень, предоставляя эксперту не просто статичные логи, а динамическую модель инцидента.

Реализация представленных предложений потребует не только значительных финансовых вложений, но и пересмотра образовательных стандартов подготовки сотрудников правоохранительных органов. Необходимо введение междисциплинарных курсов, объединяющих юриспруденцию и программирование, для формирования компетенций «цифрового следователя». Только синтез глубоких правовых знаний и продвинутых технических навыков позволит эффективно противостоять современной преступности.

Интеграция компьютерных технологий в следственную деятельность представляет собой необратимый процесс, определяющий будущее криминалистики. Рассмотренные в статье направления – от анализа больших данных до использования биометрии – демонстрируют, что технологии перестали быть вспомогательным средством и превратились в системообразующий фактор раскрытия преступлений.

Предложенные методы использования блокчейна для фиксации доказательств и нейросетевой предиктивной аналитики направлены на решение ключевых проблем: обеспечение достоверности данных и переход от реактивной модели расследования к проактивной.

Дальнейшее развитие указанной сферы должно идти по пути создания интегрированных интеллектуальных систем, способных обрабатывать колоссальные объемы информации, освобождая человеческий ресурс для принятия ключевых процессуальных решений. Успех в борьбе с высокотехнологичной преступностью зависит от способности правоохранительной системы опережать криминальный мир в скорости освоения и внедрения инноваций.

Список использованных источников

1. Вестов, Ф. А. Использование правоохранительными органами цифровых технологий в предупреждении, раскрытии и расследовании половых преступлений, не связанных с насилие / Ф. А. Вестов, Д. Д. Карпова // The Newman in Foreign Policy. – 2023. – Т. 2, № 71(115). – С. 56-60. – EDN LXGSQQ.

2. Влезько, Д. А. Использование современных методов и технологий для раскрытия и расследования преступлений, оставленных электронными следами / Д. А. Влезько, В. В. Онипко // Тенденции развития науки и образования. – 2024. – № 107-5. – С. 37-40. – DOI 10.18411/trnio-03-2024-221. – EDN LHQSTS.

3. Милов, Н. А. Перспективы использования информационных технологий в раскрытии и расследовании преступлений / Н. А. Милов // Инновации. Наука. Образование. – 2022. – № 52. – С. 217-221. – EDN JEAFZP.

4. Нуров, М. А. К вопросу об актуальных проблемах раскрытия и расследования преступлений совершаемых с использованием информационно-телекоммуникационных технологий / М. А. Нуров // Флагман науки. – 2023. – № 11(11). – С. 674-676. – EDN SYRGVV.

5. Озеров, К. И. Использование современных цифровых технологий в раскрытии и расследовании преступлений / К. И. Озеров // Научно-техническое обеспечение уголовного судопроизводства: Материалы научно-практической конференции, Москва, 10 июля 2024 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2024. – С. 54-57. – EDN BESHUO.

6. Теткин, Д. В. Современная перспектива применения новых компьютерных технологий при выявлении, раскрытии и расследовании преступлений / Д. В. Теткин, И. С. Воронина // Право: история и современность. – 2023. – Т. 7, № 1. – С. 82-89. – DOI 10.17277/pravo.2023.01.pp.082-089. – EDN FMSFDX.

7. Чайка, А. Д. Использование биометрических технологий в процессе раскрытия и расследования преступлений / А. Д. Чайка // Проблемы совершенствования российского законодательства: Сборник тезисов Всероссийской научно-практической конференции курсантов, слушателей и студентов, Барнаул, 10–12 апреля 2024 года. – Барнаул: Барнаульский юридический институт МВД России, 2024. – С. 629-631. – EDN URIKWJ.

8. Шматов, М. В. О некоторых проблемах раскрытия преступлений в сфере компьютерной информации и с использованием компьютерных технологий / М. В. Шматов // Актуальные проблемы уголовного процесса и криминалистики: сборник научных статей X Международной заочной научно-практической конференции, Могилев, 30 апреля 2024 года. – Могилев: Учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь», 2024. – С. 198-201. – EDN PNBUUE.