УДК 34

Поиск нового подхода в выстраивании уголовно-процессуального доказывания по делам о преступлениях в сфере компьютерной информации

Аникевич Диана Самвеловна

Соискатель ученой степени кандидата юридических наук,
Российский государственный университет правосудия,
117418, Российская Федерация, Москва, ул. Новочеремушкинская, 69;
e-mail: dia.83@list.ru

Аннотация

В статье с опорой на общие доктринальные начала и цели уголовно-процессуального доказывания обосновывается необходимость разработки нового подхода в организации данного процесса по делам о преступлениях в сфере компьютерной информации, поскольку современные тенденции масштабирования цифровой информационной среды и технологий обработки информации, оказавшись в руках правонарушителей приводят к дисбалансу возможностей успешного регулирования и управления негативными процессами, возникающими в цифровой среды, в которой ежедневно совершается множество киберпреступлений. Автором при сравнении процесса уголовно-процессуального доказывания по делам о преступлениях в сфере компьютерной информации с теоретическими положениями базисного закона кибернетики – закона необходимого разнообразия, сформулированного У.Р. Эшби, обосновывается допущение нового подхода в доказывании по данным преступлениям, учитывающего особенности криминогенных факторов цифровой среды.

Для цитирования в научных исследованиях

Аникевич Д.С. Поиск нового подхода в выстраивании уголовно-процессуального доказывания по делам о преступлениях в сфере компьютерной информации // Вопросы российского и международного права. 2025. Том 15. № 7А. С. 119-126.

Ключевые слова

Уголовно-процессуальное доказывание, киберпреступность, компьютерные преступления, информационные технологии, уголовная ответственность, закон необходимого разнообразия.

Введение

Современное уголовное судопроизводство по делам о преступлениях в сфере компьютерной информации сталкивается с новыми вызовами, которые во многом обусловлены природой компьютерной информации, выступающей предметом преступных посягательств, поскольку информация в этой форме обладает уникальными техническими свойствами нематериальности, неочевидной связанности с одним или несколькими материальными носителями, динамичного и трансграничного перемещения и данные свойства следует учитывать при организации процесса доказывания.

Основная часть

Свойства компьютерной информации в зависимости от конкретных обстоятельств дела делают ее как уязвимой, так и практически недосягаемой, что связано с особенностями цифровой среды, техническими характеристиками носителей, участвующих в ее обработке, транспортировке, навыками индивидов, ее создавших и использующих, что в совокупности непосредственным образом влияет на процесс доказывания преступлений в сфере компьютерной информации, требуя междисциплинарных подходов для организации эффективного процесса доказывания.

В научной литературе многократно подчеркнуто, что совершение любого из преступлений, включенных в главу 28 УК РФ, в информационной среде оставляет цифровой след создания, перемещения, удаления и иного действия с компьютерной информацией, однако недостаточно проработаны возможности, которые при правильном подходе позволяют этот след использовать в качестве потенциала для раскрытия и доказывания компьютерных преступлений. В этой связи информационные технологии занимают особую роль в многосложном процессе доказывания.

Цифровые следы, возникающие в цифровой среде в результате совершения компьютерного преступления, в отличие от иных следов, оставляемых при совершении «традиционных» преступлений практически невозможно полностью удалить. Для примера, отпечатки пальцев имеют свойство разлагаться и это может произойти как за 2 часа, так и за 5 суток, в зависимости от поверхности взаимодействия, температуры воздуха, влажности и других факторов.

Понимание конъюнктуры следообразования в цифровой среде более сложное и зависит от многочисленных факторов, получить общее представление о которых возможно получить по описанию, данному А.Г. Волеводзом: «В ходе сеанса связи информация проходит через значительное количество серверов, которые физически могут быть установлены у не меньшего количества провайдеров на значительном географическом пространстве и удалении» [Волеводз, 2002].

Различные трактовки понятия «цифровой след» и отсутствие прямого официального закрепления дефиниции на законодательном уровне отчасти подтверждают многоаспектность явления. Для выработки подходов в доказывании важным выступает взгляд с ракурса изучения возможностей удаления цифрового следа, в части чего существует мнение, что полностью удалить его невозможно, так как информация в том или ином виде будет оставаться в архивах, на сторонних сайтах и в базах данных, могла быть скопирована другими пользователями, сохранена провайдерами.

Выделенные особенности, безусловно проявляются и должны учитываться при организации процесса доказывания, что обуславливает не угасающий интерес научной мысли, направленный

на отыскание механизмов обеспечения электронных доказательств с целью совершенствования процесса доказывания по киберпреступлениям, включая механизмы отыскания источников доказательственной информации, корректного их изъятия и фиксации, производства логически верных выводов на основе полученных данных.

Включаясь в процесс уголовно-процессуального доказывания конкретного преступления, субъект познает событие прошлого, недоступное для непосредственного восприятия, через существенные связи и отношения между объектами, выявляемые через знания и умозаключения, логические операции, устанавливая причинно-следственные связи через внешние проявления, а именно по материальным и идеальным следам вышеуказанных обстоятельств, подлежащих доказыванию.

Тем самым фрагментированная информация об обстоятельствах преступления становится объектом поиска для достижения конкретных целей доказывания по уголовному делу, а процесс доказывания происходит ретроспективно на субъективном уровне и призван по сути реконструировать преступное событие, что в последствии становится основной для принятия итогового процессуального решения по делу после исследования доказательств в судебном заседании (ст. 240 УПК РФ).

Уголовно-процессуальное доказывание, являясь разновидностью процесса познания, тем не менее выстраивает доказывание в строго ограниченной процессуальной форме, только при соблюдении которой, в рамках следственных и иных процессуальных действий должна устанавливаться совокупность определенных обстоятельств: наличие или отсутствие события преступление; время место и способ совершения преступления; лицо, совершившее деяние; форму вины обвиняемого, мотив; наличие или отсутствие обстоятельств, исключающих преступность и наказуемость деяния; наличие обстоятельств, характеризующих личность обвиняемого; характер и размер вреда, причиненного преступлением (ч.1 ст. 73 УПК РФ).

При доказывании большинства из указанных обстоятельств по преступлениям в сфере компьютерной информации необходимо зафиксировать в языковой форме цифровой эквивалент, для названной реконструкции преступного события с необходимостью в дальнейшем формирования внутреннего убеждения суда на основе зачастую сложных, косвенных и технически насыщенных данных, ясность и доступность изложения которых должны объяснить сложную техническую атрибутику понятным для суда языком.

К настоящему времени внедрено множество концептуальных решений в области рассматриваемой проблематики, а также предложено достаточное количество инноваций, однако, присущий данным подходам резко-технологический цифровой эквивалент, меняющие устоявшиеся доктринальные подходы к уголовно-процессуальному доказыванию, подвергается научной критике [Корчагин, Яковенко, 2020; Головко, 2019; Зазулин, 2020] либо предложенные новеллы сталкиваются с организационным, техническим, финансовым и правовым препятствиям на стадии их апробации в современную правоприменительную практику [Федеральный закон № 374-ФЗ, www], оставляя инновационные предложения в теории, что приводит к отставанию имеющихся мер противодействия компьютерным преступлениям от новых вызовов современной компьютерной преступности и ощутимо большему разрыву между результативностью доказательственной деятельности и возможностями средств технологического прогресса в руках правонарушителей.

Вместе с тем имеется также и существенное продвижение возможностей новых технологий в науку и законодательство в области обеспечения безопасности прав граждан в цифровом пространстве, что способствует более эффективной организации процесса доказывания

киберпреступлений.

До недавнего времени в большинстве стран мира, включая Россию на законодательном уровне отсутствовали решения вопросов о том, кто, в течение какого времени и в каком объеме должен хранить электронную информацию, которая зачастую включает и цифровые следы компьютерных преступлений. Однако в последнее время подобным вопросам уделяется больше внимания и в целом прослеживается ужесточение вектора законодательного регулирования.

В 2016 г. большой резонанс в российском обществе вызвало принятие Федерального закона от 6 июля 2016 г. № 374-ФЗ по установлению дополнительных мер противодействия терроризму и обеспечения общественной безопасности, так называемого пакета законов «Яровой-Озерова», поскольку организаторам распространения информации в сети Интернет (в том числе «VKontakte», «WhatsApp», «Telegram», «Viber» и т.д.) согласно указанным законодательным новеллам поставлено в обязанность хранить на территории РФ и предоставлять уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность и обеспечивающим безопасность следующие сведения:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео - или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях, которую требуется хранить в течение одного года;
– текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения, которые необходимо хранить до шести месяцев.
– методанные – информацию о том, кому и когда звонил или пересылал файлы пользователь – в течение трех лет.

Коррелирующие изменения внесены Федеральным законом от 6 июля 2016 г. № 375-ФЗ в УПК РФ, введением части 7 статьи 185 (Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка), в соответствии с которой при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка.

Также широкое применение элементов технологического прогресса внедряется в рамках методов компьютерной (цифровой) криминалистики, называемой форензикой.

Форензика – это компьютерная криминалистика, т.е. прикладная наука о раскрытии и расследовании преступлений в сфере компьютерной информации, связанная с исследованием следообразования цифровых доказательств, а также методов их выявления и различного рода технических средств, используемых в ходе совершения и расследования преступления [Концепция Интернета Вещей, www].

Возможности компьютерной криминалистики позволяют широко использовать в доказывании информацию, хранящуюся в цифровых устройствах при их изъятии, в том числе удаленные данные из смартфонов, ноутбуков, в которых современный человек привычно хранит огромное количество данных, к которым можно получить доступ. В среднем в таких устройствах содержится более 60 000 сообщений, 32 000 изображений и более 1000 видеороликов, широкий спектр приложений и программ, предоставляющих важную информацию для решения конкретных задач, включая PDF-файлы и другие документы, метаданные, информацию из социальных сетей, электронную почту, платформы обмена сообщениями, навигационные приложения и крипто-кошельки.

Облачные хранилища содержат информацию, имеющую потенциал для доказывания несанкционированного доступа к охраняемой компьютерной информации, ее копирования или распространения кражи интеллектуальной собственности. Использование облачных сервисов, таких как «Apple iCloud», «Google Drive», «Dropbox» и т.д., для резервного копирования информации с мобильных устройств и Интернета вещей (IoT) [МВД РФ, www], в том числе помощников по дому, умных часов и автомобилей, используемых 55 % пользователей в качестве основного способа хранения данных может позволить произвести анализ данных, хранящихся в облачных средах для поиска цифровых следов. Данный процесс усложняет трансграничный характер распределения облачных сервисов иногда с участием нескольких юрисдикций.

В целях мониторинга и предупреждения различных угроз общественной безопасности функционируют система «Безопасный город» для наружного видеонаблюдения и встроенными возможностями распознавания лиц с доступом к указанной информации органов внутренних дел. Для их применения при доказывании компьютерных преступлений необходимо получить фотоизображение предполагаемого нарушителя.

Следы преступной деятельности, оставленные с помощью средств мобильной сотовой связи, позволяют установить местонахождение нарушителя, определять маршрут передвижения, получить мультимедийную и иную информацию, передаваемую с помощью мобильного устройства, и установить принадлежность данных конкретному человеку.

Выстраивание уголовно процессуального доказывания по анализируемым составам преступлений будет включать в себя несколько этапов:

Во-первых: определение источников типов данных для сбора (файлы, логи, дампы памяти, сетевой трафик, метаданные) и поиск источников их получения (компьютеры, серверы, мобильные устройства, облачные хранилища, сети).

Во-вторых: сбор данных с сохранением целостности, исследование информации и цифровых носителей, анализ среды и носителей для определения информации, относимой к событию и обстоятельствам преступления.

В-третьих: фиксацию и документирование цифровых доказательств, соблюдая процессуальные требования.

Далее полученная информация должна быть подвергнута проверки и оценке с помощью перекрестного анализа установленных обстоятельств и цифровых следов: журналов событий (логов), который позволит выявить действия пользователей и системных событий; сетевой активности, включая трафик и посещенные сайты; метаданных файлов и других объектов; информации о подборах паролей; исследований памяти (дампов) для выявления текущих процессов и активности; определения хронологии событий и действий в системе.

В результате такого анализа могут быть выявлены обстоятельства незаконного доступа к компьютерной информации, ее изменений, модификации и модели используемых технических устройств нарушителя и т.д., что позволит прийти к определенным выводам, которые необходимы для построения процесса доказывания.

Ключевыми направлениями для дальнейшего развития и совершенствования процесса доказывания по компьютерным преступлениям является область междисциплинарного взаимодействия посредством обмена знаниями и опытом процессуалистов и технических специалистов, которое, на наш взгляд, следует направить на более эффективную организации сбора в информационной среде максимально возможного объема цифровых следов по ранее установленной информации об обстоятельствах преступления, технических средствах,

использованных при его совершении.

Данное взаимодействие на сегодняшний день уже позволило широко вовлечь в доказательственный процесс новые возможности, позволяющие установить связи с конкретным человеком и обстоятельства совершения преступления по техническим сведениям, которые известны каждому процессуалисту: IP-адреса, ICCID сим-карт, IMEI устройств, электронные подписи, логи интернет-ресурсов, свойства файлов, хеширование как цифровой способ фиксации содержания файлов для контроля факта внесения последующих изменений, информацию с жестких дисков компьютера, веб-страниц, сведения о соединениях между абонентами и абонентскими устройствами и т.д.

На сегодняшний день особенности цифровой среды повлияли на изменение УПК РФ в части, касающейся правил изъятия и фиксации электронных носителей информации и порядка производства некоторых следственных действий, что нашло отражение в ст. 164.1, ч. 7 ст. 185, ст. ст. 186, 186.1, 189.1 УПК РФ.

Вместе с тем, на вопрос достаточно ли введенных мер для эффективного доказывания киберпреступлений, отвечают нелицеприятные статистические сведения.

За последние три года в России каждое четвертое преступление совершено с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

В 2022 году доля киберпреступлений в общем объеме совершенных преступлений (1 966 795) составила 522 065 (26,5 %), в 2023 году каждое третье преступление совершено с использованием информационно-телекоммуникационных технологий, их зарегистрировано на 29,7% больше, чем в 2022 году. В 2024 году общее число указанных преступлений увеличилось на 13,1 % по сравнению с предыдущим годом и составило 40 % от всех преступлений [Состояние преступности // Министерство внутренних дел Российской Федерации, www…].

Согласно первому фундаментальному закону кибернетики - закону необходимого разнообразия, сформулированному У.Р. Эшби, разнообразие сложной системы требует сопоставимо разнообразного управления такой системой. Рассматривая используемые преступными элементами огромные объемы цифровой информации и технологии ее обработки по правилам названного закона кибернетики, объемы информации об обстоятельствах совершенного преступления в цифровой среде как внешние раздражители должны поддаваться управлению с помощью уголовно-процессуальных мер, таких как механизмы раскрытия и доказывания преступлений, т.е. контролю за управляющей информацией с помощью мер воздействия, обладающих достаточным разнообразием, чтобы такой контроль осуществлять.

Иными словами, большое количество внешних раздражителей должно быть сопоставимо со способами противодействия им конкретными средствами, что в сфере доказывания может быть достигнуто с помощью увеличения скорости и качества собирания и анализа потенциально доказательственной информации в виде цифровых следов совершения компьютерных преступлений из максимального количества известных источников в цифровой среде, что на достигнутом уровне технологического прогресса возможно посредством создания платформы для использования правоохранительными органами автоматизации указанного процесса.

Заключение

Таким образом, для эффективного процесса доказывания в условиях тотальной цифровизации необходимо максимально широко использовать в доказывании уникальные свойства компьютерной информации в той части, в которой она может быть подвержена

автоматизированному сбору и обработке в целях раскрытия и доказывания киберпреступлений, пополнив арсенал следственных и процессуальных действий, новыми, высокотехнологическими механизмами, которые делали бы возможным единовременное и тотальное получение всего объема цифровой информации по любым известным данным о лице, технических средствах, являющихся орудием преступления и др. при безусловном соблюдении прав человека, что возможно обеспечить посредством получения решения суда для проведения предложенного следственного действия.

Библиография

1. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях / А.Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 4–12.
2. Корчагин А.Г., Яковенко А.А. К вопросу о развитии российской уголовной политики и вызовах современности. Балтийский гуманитарный журнал. 2020. Т. 9. № 4 (33). – С. 375-380; Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция // Вестник экономической безопасности. 2019. № 1. С. 15–25; Зазулин А. И. Функции цифровой информации и технологий в уголовном процессе. Сибирское юридическое обозрение. 2020. Том 17, № 1. С. 75-82.
3. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 6 июля 2016 г. № 374-ФЗ // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/document/0001201607070016 (дата обращения 18.02.2025).
4. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/document/0001201607070042.
5. Федотов Н. Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – С. 11.
6. Главная концепция Интернета Вещей (Internet of Things, IoT) – это среда, в которой вещи имеют способность слушаться управления, а данные о вещах могут быть обработаны для выполнения желаемой задачи посредством обучения устройств.
7. Состояние преступности // Министерство внутренних дел Российской Федерации. – URL: https://xn--b1aew.xn--p1ai/reports/1/ (дата обращения: 02.02.2025).

Search for a New Approach in Structuring Criminal Procedural Evidence in Cases of Computer Information Crimes

Diana S. Anikevich

Applicant for the Degree of Candidate of Legal Sciences,
Russian State University of Justice,
117418, 69 Novocheremushkinskaya str., Moscow, Russian Federation;
e-mail: dia.83@list.ru

Abstract

The article, based on the general doctrinal principles and objectives of criminal procedural evidence, substantiates the need to develop a new approach to organizing this process in cases of computer information crimes. Modern trends in the scaling of the digital information environment and information processing technologies, when in the hands of offenders, lead to an imbalance in the capabilities for successful regulation and management of negative processes arising in the digital

environment, where numerous cybercrimes are committed daily. By comparing the process of criminal procedural evidence in cases of computer information crimes with the theoretical provisions of the fundamental law of cybernetics—the law of requisite variety formulated by W. Ross Ashby—the author justifies the assumption of a new approach to proving such crimes, taking into account the peculiarities of criminogenic factors in the digital environment.

For citation

Anikevich D.S. (2025) Poisk novogo podkhoda v vystraivanii ugolovno-protsessual'nogo dokazyvaniya po delam o prestupleniyakh v sfere komp'yuternoy informatsii [Search for a New Approach in Structuring Criminal Procedural Evidence in Cases of Computer Information Crimes]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (7A), pp. 119-126.

Keywords

Criminal procedural evidence, cybercrime, computer crimes, information technologies, criminal liability, law of requisite variety.

References

1. Volevodz A.G. Traces of crimes committed in computer networks / A.G. Volevodz // Russian investigator. - 2002. – No. 1. – pp. 4-12.
2. Korchagin A. G., Yakovenko A. A. On the development of Russian criminal policy and modern challenges. Baltic Humanitarian Journal. 2020. Vol. 9. No. 4 (33). – pp. 375-380; Golovko L. V. Digitalization in criminal proceedings: local optimization or global revolution // Bulletin of Economic Security. 2019. No. 1. pp. 15-25; Zazulin A. I. Functions of digital information and technologies in criminal proceedings. Siberian Law Review. 2020. Volume 17, No. 1. pp. 75-82.
3. On Amendments to the Federal Law "On Countering Terrorism" and Certain Legislative Acts of the Russian Federation regarding the Establishment of Additional Measures to Combat terrorism and Ensure Public Safety : Federal Law No. 374-FZ of July 6, 2016 // Official Internet Portal of Legal Information. – URL: http://publication.pravo.gov.ru/document/0001201607070016 (accessed 02/18/2025).
4. On amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety : Federal Law // Official Internet Portal of Legal Information. – URL: http://publication.pravo.gov.ru/document/0001201607070042.
5. Fedotov N. N. Forensics – computer criminalistics, Moscow: Yuridicheskiy Mir Publ., 2007, p. 11.
6. The main concept of the Internet of Things (IoT) is an environment in which things have the ability to obey control, and data about things can be processed to perform a desired task through device learning.
7. The state of crime // Ministry of Internal Affairs of the Russian Federation. – URL: https://xn--b1aew.xn--p1ai/reports/1/ (date of access: 02.02.2025).