ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Курмычкина Альбина Ринат кизи
Магистр права Ташкентского государственного юридического университета
albinaakurmichkina@gmail.com
+998900095772
https://doi.org/10.5281/zenodo.16302325

Аннотация. В статье исследуются специфические особенности доказывания по делам о преступлениях в сфере информационных технологий в контексте современных глобальных вызовов кибербезопасности. Анализируется статистика киберпреступности, показывающая критический рост ущерба до 9,5 триллиона долларов США в 2024 году. Рассматриваются особенности цифровых доказательств, их классификация и критерии допустимости в международной судебной практике. Исследуются процессуальные особенности собирания и исследования электронной информации, включая специфику производства следственных действий и назначения компьютерно-технических экспертиз. Анализируются проблемы международного сотрудничества в рамках Будапештской конвенции 2001 года и новой Конвенции ООН против киберпреступности 2024 года. Выявляется критически низкая раскрываемость IT-преступлений и предлагаются направления совершенствования правовых механизмов доказывания в цифровой среде.

Ключевые слова: киберпреступность, цифровые доказательства, компьютерно-техническая экспертиза, международное сотрудничество, IT-преступления, электронная информация, доказывание, кибербезопасность, транснациональная преступность, взаимная правовая помощь.

I. Введение

Современное общество переживает эпоху глобальной цифровизации, которая коренным образом трансформирует все сферы человеческой деятельности. Одновременно с расширением возможностей информационных технологий наблюдается стремительный рост преступлений, совершаемых в цифровой среде. По данным международных исследований, киберпреступность в 2024 году достигла критических масштабов: глобальный ущерб составил 9,5 триллиона долларов США [1], что превышает ВВП большинства стран мира. Если рассматривать киберпреступность как отдельную экономику, она заняла бы третье место в мире после США и Китая.

Статистика демонстрирует тревожную динамику роста цифровых угроз. В 2024 году средняя стоимость утечки данных в мире достигла рекордных 4,88 миллиона долларов США, что на 10% больше по сравнению с предыдущим годом [2]. По данным ФБР, с момента создания Центра жалоб на интернет-преступность (IC3) ФБР было получено более 7,3 миллиона жалоб, что составляет в среднем 651 800 жалоб в год за последние пять лет [3]. Частота кибератак удвоилась после пандемии COVID-19.

Материальный ущерб от киберпреступности продолжает расти экспоненциально. Согласно исследованиям МВФ, в 2027 году ущерб от киберпреступности в мире составит 23 триллиона долларов, что на 175% больше, чем в 2022 году [4]. Это представляет собой величайший перенос экономического богатства в истории

человечества. Эти цифры превышают ущерб от стихийных бедствий и делают киберпреступность более прибыльной, чем глобальная торговля всеми основными наркотиками вместе взятыми.

Актуальность исследования обусловлена кардинальными особенностями доказывания по IT-преступлениям, которые существенно отличаются от традиционных форм правонарушений. Цифровая природа следов преступной деятельности, их изменчивость и уязвимость к утрате создают принципиально новые вызовы для правоохранительных систем и судебной практики во всем мире.

Цель исследования — выявить и систематизировать специфические особенности процесса доказывания по делам о преступлениях в сфере информационных технологий в контексте международного права и сравнительной правовой практики.

Задачи исследования:

- определить специфику IT-преступлений как объекта доказывания;
- проанализировать особенности предмета доказывания по данной категории дел;
- исследовать процессуальные особенности собирания и исследования доказательств;
- выявить проблемы оценки и использования электронной информации в качестве доказательств.

II. Методология

Методологическую основу исследования составила совокупность общенаучных и частнонаучных методов познания. Применялись диалектический метод как универсальный способ познания правовых явлений в их развитии и взаимосвязи, формально-логический метод для анализа нормативных конструкций, сравнительно-правовой метод для сопоставления различных подходов к регулированию доказывания IT-преступлений, статистический метод для обработки эмпирических данных о состоянии киберпреступности.

Эмпирическую базу составили статистические данные международных организаций (ООН, ФБР, Европол, Интерпол), результаты глобальных исследований в области кибербезопасности за 2023-2024 годы, материалы судебной практики различных юрисдикций, а также данные специализированных исследований в области цифровой криминалистики.

Обзор литературы

Теоретической основой исследования послужили труды ведущих международных специалистов в области уголовного процесса и цифровой криминалистики. Фундаментальные аспекты теории доказательств в цифровую эпоху разработаны в работах Б. Кэрриера [5], К. Кейси [6], С. Гарфинкеля [7]. Проблематика международного сотрудничества в борьбе с киберпреступностью исследована в трудах экспертов Управления ООН по наркотикам и преступности (УНП ООН) [8].

Существенный вклад в разработку проблем квалификации и расследования киберпреступлений внесли международные исследовательские группы, работающие под эгидой Совета Европы и ООН. Вопросы применения специальных знаний при

расследовании IT-преступлений рассмотрены в материалах Научной рабочей группы по цифровым доказательствам (Scientific Working Group on Digital Evidence) [9].

Практические аспекты компьютерно-технической экспертизы освещены в международных стандартах ISO/IEC 27037:2012 и нашли отражение в аналитических материалах ведущих международных экспертных организаций [10].

III. Результаты

1. Специфика преступлений в сфере информационных технологий

Преступления в сфере информационных технологий представляют собой качественно новый вид противоправной деятельности, характеризующийся рядом специфических особенностей, которые кардинально влияют на процесс доказывания. По определению международных конвенций, данные преступления представляют собой противоправные общественно опасные деяния, совершаемые с использованием информационных технологий, информационных систем и информационно-телекоммуникационных сетей.

Современная статистика демонстрирует взрывной рост данной категории преступлений. По данным мирового индекса киберпреступности, опубликованного в 2024 году, наиболее значительными источниками киберпреступности на национальном уровне являются страны с развитой IT-инфраструктурой, но недостаточными мерами кибербезопасности. Исследования показывают, что 47,4% всего интернет-трафика в 2022 году составляли боты, что на 5,1% больше, чем в 2021 году [11].

Структурно преступления в сфере информационных технологий можно классифицировать следующим образом: преступления против безопасности компьютерной информации; преступления в сфере незаконного оборота цифровой информации; преступления в сфере незаконного оборота программных и технических средств; преступления с использованием криптовалют и цифровых финансовых активов.

Особенности следов преступной деятельности в цифровой среде принципиально отличают IT-преступления от традиционных форм правонарушений. Цифровые следы характеризуются высокой изменчивостью, возможностью быстрого уничтожения или модификации, а также способностью к автоматическому воспроизведению и распространению. В отличие от материальных следов, цифровая информация может существовать одновременно в множестве копий, распределенных по различным техническим устройствам и географическим локациям.

Критической особенностью является анонимность субъектов преступления в виртуальной среде. Преступники активно используют средства сокрытия своей личности: анонимные сети (Tor), виртуальные частные сети (VPN), поддельные аккаунты и похищенные идентификационные данные. По данным исследований, средний возраст лица, арестованного за киберпреступление, составляет 19 лет, в то время как средний возраст арестованных за другие преступления — 37 лет [12].

Транснациональный характер киберпреступлений добавляет дополнительные сложности в процесс доказывания. Преступник может находиться в одной стране, использовать серверы в другой, а потерпевшие — в третьей. Это требует

международного сотрудничества и создает юрисдикционные проблемы при собирании доказательств.

2. Особенности предмета доказывания по IT-преступлениям

Предмет доказывания по делам о преступлениях в сфере информационных технологий включает традиционные элементы, но их содержание приобретает специфические черты, обусловленные цифровой природой преступной деятельности.

Цифровые доказательства составляют основу доказательственной базы по IT-преступлениям. Под цифровыми доказательствами понимается информация в электронной форме, имеющая значение для установления обстоятельств, подлежащих доказыванию. Классификация цифровых доказательств включает: данные, содержащиеся на физических носителях информации; информацию, передаваемую по сетям связи; метаданные, характеризующие условия создания, изменения и передачи файлов; логи системных событий и журналы активности пользователей.

Специфика установления обстоятельств, подлежащих доказыванию, проявляется в необходимости реконструкции цифровых процессов. При доказывании события преступления требуется восстановить последовательность действий в информационной системе, определить временные характеристики цифровых операций с учетом возможных манипуляций со временем в компьютерных системах. Установление места совершения преступления осложняется виртуальным характером киберпространства, где физическое местоположение технических средств может не совпадать с юридически значимым местом совершения деяния.

Наиболее сложной задачей является идентификация субъекта преступления в виртуальной среде. Традиционные методы установления личности неприменимы в условиях, когда преступник может использовать чужие учетные записи, поддельные данные или технические средства третьих лиц.

Проблемы идентификации усугубляются использованием средств анонимизации. Современные преступники применяют сложные схемы сокрытия своей личности: многоуровневые системы прокси-серверов, криптографические методы защиты информации, распределенные сети с децентрализованной архитектурой. В таких условиях установление связи между конкретным лицом и совершенным деянием требует применения специальных технических методов и экспертных знаний.

Особое значение приобретает установление способа совершения преступления, который в цифровой среде может включать использование специализированного программного обеспечения, эксплуатацию уязвимостей информационных систем, применение методов социальной инженерии. По статистике, 94% вредоносного программного обеспечения распространяется через электронную почту, а 68% нарушений безопасности связаны с человеческим фактором [13].

Размер ущерба в киберпреступлениях часто носит скрытый характер и может проявляться не сразу. Например, при утечке персональных данных реальный ущерб может возникнуть через длительное время после совершения преступления, когда похищенная информация будет использована для мошенничества. Это создает дополнительные сложности в доказывании причинно-следственной связи между деянием и наступившими последствиями.

3. Процессуальные особенности собирания и исследования доказательств

Расследование IT-преступлений характеризуется существенными процессуальными особенностями, обусловленными спецификой цифровой среды и необходимостью применения специальных технических методов собирания доказательств.

Специальные следственные действия при расследовании IT-преступлений

Традиционные следственные действия при расследовании киберпреступлений приобретают новое содержание и требуют специальных подходов. Осмотр места происшествия в контексте IT-преступлений может включать исследование как физических объектов (компьютерная техника, носители информации), так и виртуальных локаций (веб-сайты, учетные записи в социальных сетях, облачные хранилища).

Особое значение приобретает понятие "цифрового места происшествия", которое может быть территориально распределено по множеству серверов и устройств в различных юрисдикциях. Это создает уникальные проблемы для правоохранительных органов, поскольку традиционные границы юрисдикции становятся размытыми в киберпространстве.

Особенности производства обыска и выемки компьютерной техники

Обыск и выемка компьютерной техники требуют соблюдения строгих процедур для обеспечения сохранности и целостности цифровых доказательств. Основные требования включают: немедленное отключение устройств от сети для предотвращения удаленного уничтожения данных; создание точных побитовых копий носителей информации; документирование всех технических действий; обеспечение неизменности исходных носителей информации.

Критическим фактором является время проведения данных процедур. Цифровые следы могут быть уничтожены за считанные секунды, что требует оперативного реагирования правоохранительных органов. Международная статистика показывает, что среднее время для выявления нарушения безопасности составляет 194 дня, а полный жизненный цикл нарушения от выявления до устранения — 292 дня [13].

Назначение и производство компьютерно-технических экспертиз

Компьютерно-техническая экспертиза (КТЭ) является ключевым инструментом доказывания по IT-преступлениям. В международной практике судебных экспертиз выделяются следующие виды КТЭ:

1. Аппаратно-компьютерная экспертиза — исследование технических средств компьютерной системы, установление их характеристик и функционального назначения;
2. Программно-компьютерная экспертиза — анализ программного обеспечения, выявление его свойств, алгоритмов работы и возможных уязвимостей;
3. Информационно-компьютерная экспертиза — исследование цифровых данных, восстановление удаленной информации, анализ логов системных событий;
4. Компьютерно-сетевая экспертиза — изучение сетевых технологий, анализ сетевого трафика и протоколов передачи данных.

Эффективность КТЭ во многом зависит от квалификации экспертов и технической оснащенности экспертных учреждений. В 2002 году Научная рабочая группа по цифровым доказательствам подготовила документ "Лучшие методы компьютерной криминалистики", за которым в 2005 году последовала публикация стандарта ISO/IEC 17025:2005.

Международное сотрудничество при получении доказательств

Транснациональный характер киберпреступлений делает международное сотрудничество критически важным элементом процесса доказывания. Основными механизмами такого сотрудничества являются:

Взаимная правовая помощь по уголовным делам, осуществляемая на основе двусторонних и многосторонних договоров. Особую роль играет Будапештская конвенция о киберпреступности 2001 года, которая является первым международным договором в данной сфере и устанавливает стандарты международного сотрудничества. В декабре 2024 года была принята Конвенция ООН против киберпреступности — первый всеобъемлющий глобальный договор по этому вопросу.

Экстрадиция киберпреступников, осложненная проблемами юрисдикции и различиями в национальных правовых системах. Традиционные принципы экстрадиции, такие как требование двойной криминализации деяния, могут создавать препятствия в случаях, когда законодательство различных стран по-разному регулирует ответственность за киберпреступления.

Оперативное сотрудничество правоохранительных органов через каналы Интерпола и региональных организаций. Создание специализированных подразделений по борьбе с киберпреступностью в структуре международных правоохранительных организаций способствует повышению эффективности такого взаимодействия.

4. Проблемы оценки и использования цифровых доказательств

Оценка цифровых доказательств представляет собой комплексную проблему, включающую как технические, так и правовые аспекты, которые существенно влияют на эффективность доказывания по IT-преступлениям.

Критерии допустимости цифровых доказательств

Несмотря на отсутствие в большинстве национальных процессуальных законодательств специального понятия "цифровые доказательства", суды активно применяют их при рассмотрении различных категорий дел. Основные критерии допустимости включают: соблюдение процедур получения доказательств; обеспечение неизменности данных в процессе их изъятия и исследования; документирование цепочки обращения с цифровыми носителями; компетентность лиц, осуществляющих работу с цифровыми доказательствами.

В соответствии с международными стандартами, приемлемость цифровых доказательств зависит от инструментов, используемых для их получения. В различных юрисдикциях действуют разные стандарты, но общим требованием является необходимость публикации и рецензирования кода инструментов судебной экспертизы.

Проблемы подлинности и целостности электронной информации

Цифровая информация характеризуется высокой уязвимостью к фальсификации и несанкционированному изменению. Основные проблемы включают: возможность создания поддельных цифровых документов с использованием современных технологий; сложность установления времени создания и модификации файлов; проблемы аутентификации электронных сообщений и цифровых подписей; возможность манипулирования метаданными файлов.

Статистические данные показывают рост использования технологий искусственного интеллекта для создания дипфейков — поддельных аудио- и видеоматериалов, что создает новые вызовы для системы доказывания. По данным аналитических отчетов, в 2024 году существенно увеличилось применение ИИ в мошеннических схемах, включая создание убедительных фишинговых материалов и поддельного контента.

Вопросы анонимности и шифрования как препятствия доказыванию

Широкое использование технологий анонимизации и криптографической защиты информации создает серьезные препятствия для правоохранительных органов. Проблемы включают: применение преступниками анонимных сетей типа Tor для сокрытия своей личности; использование криптовалют для финансовых операций, затрудняющих отслеживание денежных потоков; применение современных алгоритмов шифрования, практически исключающих возможность расшифровки перехваченной информации без ключей.

Согласно международной статистике, только 8% организаций, которые выплачивают выкуп хакерам, получают обратно все свои данные. При этом 75% крупных организаций сталкивались с атаками программ-вымогателей в 2024 году [14], а средняя стоимость восстановления после такой атаки составляет 2,73 миллиона долларов [15].

IV. Обсуждение

Проведенное исследование выявляет системные особенности доказывания по IT-преступлениям, которые кардинально отличают данную категорию дел от традиционных форм правонарушений. Основные выводы включают:

Во-первых, цифровая природа следов преступной деятельности требует принципиально новых подходов к их собиранию, фиксации и исследованию. Традиционные процессуальные механизмы нуждаются в адаптации к реалиям цифровой эпохи.

Во-вторых, критически низкая раскрываемость киберпреступлений свидетельствует о недостаточной эффективности существующих систем правоохранительной деятельности в цифровой сфере. Это обусловлено как объективными сложностями (анонимность, транснациональность, техническая сложность), так и субъективными факторами (недостаточная подготовка кадров, техническое оснащение).

В-третьих, отсутствие в большинстве национальных процессуальных законодательств специального регулирования цифровых доказательств создает правовую неопределенность и препятствует эффективному доказыванию. Принятие в

декабре 2024 года Конвенции ООН против киберпреступности представляет собой важный шаг к гармонизации международных подходов.

В-четвертых, международный характер киберпреступлений требует развития механизмов международного сотрудничества и гармонизации национальных правовых систем в данной сфере.

V. Заключение

Доказывание по делам о преступлениях в сфере информационных технологий характеризуется существенными особенностями, обусловленными цифровой природой преступной деятельности. Стремительный рост киберпреступности (глобальный ущерб 9,5 триллиона долларов США в 2024 году) и прогнозируемое увеличение до 10,5 триллиона к 2025 году делает совершенствование системы доказывания критически важной задачей мирового сообщества.

Основные направления развития включают: законодательное закрепление понятия цифровых доказательств и специальных процедур их получения в национальных правовых системах; совершенствование системы подготовки кадров для правоохранительных органов в области цифровых технологий; развитие технического оснащения экспертных учреждений; расширение международного сотрудничества в борьбе с транснациональной киберпреступностью в рамках новой Конвенции ООН против киберпреступности.

Эффективность противодействия киберпреступности во многом зависит от способности правовых систем адаптироваться к вызовам цифровой эпохи и обеспечить надежную защиту прав и законных интересов граждан в виртуальном пространстве.

References:
Используемая литература:
Foydalanilgan adabiyotlar:

1. Cybersecurity Ventures. "Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024" // Cybersecurity Ventures. 2023. October 25. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
2. IBM. "Cost of a Data Breach Report 2024" // IBM Security. July 30, 2024. URL: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
3. FBI. "Internet Crime Complaint Center Releases 2022 Statistics" // FBI.gov. March 23, 2023. URL: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics
4. SentinelOne. Key Cyber Security Statistics for 2025. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/
5. B. Carrier and E. Spafford, “Getting Physical with the Digital Investigation Process,” International Journal of Digital Evidence, Vol. 2, No. 2, 2003, pp. 1-21.
6. Casey, E. "Digital Evidence and Computer Crime" (2011) https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-

and-computer-crime-third-edition.pdf
7. Garfinkel, S. "Digital Forensics Research: The Next 10 Years" (2010) https://doi.org/10.1016/j.diin.2010.05.009
8. United Nations Convention against Cybercrime. UN General Assembly Resolution 79/243, 2024.
9. Scientific Working Group on Digital Evidence. Best Practices for Computer Forensics. 2002
10. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. (2012).
11. Imperva. (2023). *2023 Bad Bot Report*. Imperva. https://www.imperva.com/resources/resource-library/reports/2023-imperva-bad-bot-report/
12. Cybersecurity Ventures. (2024, November 18). 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybersecurity Ventures. https://cybersecurityventures.com/cybersecurity-almanac-2024/
13. Varonis. (2024, September 13). 157 Cybersecurity Statistics and Trends [updated 2024]. Varonis. https://www.varonis.com/blog/cybersecurity-statistics
14. Sophos. (2024, April). State of Ransomware 2024. Sophos. https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state
15. Help Net Security. (2024, May 2). Ransom recovery costs reach $2.73 million. Help Net Security. https://www.helpnetsecurity.com/2024/05/03/ransom-recovery-costs/