ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ МЕЖДУНАРОДНОГО ОБМЕНА ЭЛЕКТРОННЫМИ ДОКАЗАТЕЛЬСТВАМИ В ДЕЛАХ О ТРАНСГРАНИЧНЫХ ЭКОЛОГИЧЕСКИХ ПРЕСТУПЛЕНИЯХ

Гулимова Дилшода Аллоёр кизи
Базовый Докторант кафедры Международного права и прав человека
Ташкентский Государственный Юридический Университет
dilshodaallayarovna@gmail.com
+998996920008

https://doi.org/10.5281/zenodo.20656371

Введение

Трансграничная экологическая преступность в последние годы стала одной из наиболее прибыльных сфер криминальной деятельности, уступая по объемам незаконных доходов лишь торговле наркотиками, контрафактной продукцией и торговле людьми. По данным Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), экологические преступления, включая незаконную вырубку лесов, нелегальную добычу полезных ископаемых и контрабанду диких животных, ежегодно генерируют от 110 до 281 миллиарда долларов США незаконных доходов[1].

В рамках международных конференций и экспертных панелей все чаще подчеркивается, что современные экологические преступления носят ярко выраженный транснациональный и высокотехнологичный характер. Организованные преступные группы (ОПГ) используют сложные логистические цепочки, подставные компании и теневые финансовые схемы, охватывающие юрисдикции десятков государств.

В таких условиях традиционные методы расследования теряют свою эффективность. На передний план выходят электронные (цифровые) доказательства. В отличие от физических улик, которые могут быть легко уничтожены или скрыты, цифровые следы позволяют правоохранительным органам реконструировать события, выявлять организаторов и отслеживать финансовые потоки даже в тех случаях, когда преступники находятся на другом континенте. Электронные письма, данные геолокации, спутниковые снимки и транзакции в криптовалюте становятся ключевыми элементами обвинительной базы в судах[2].

Однако, несмотря на критическую важность таких данных, процесс их получения и легализации на международном уровне сопряжен с серьезными проблемами, которые требуют комплексного обсуждения и выработки новых правовых механизмов.

Специфика электронных доказательств в делах об экологических преступлениях

[1] FATF. (2021). Money Laundering from Environmental Crime. Financial Action Task Force, Paris. URL: www.fatf-gafi.org.

[2] UNODC. (2019). Electronic Evidence: A compilation of cases from the SHERLOC Database. United Nations Office on Drugs and Crime, Vienna.

В ходе экспертных дискуссий было отмечено, что электронные доказательства по экологическим делам имеют свою специфику и классификацию, которая напрямую влияет на методы их трансграничного запроса.

К основным категориям относятся:

1. Данные систем глобального позиционирования и трекинга. Например, Автоматическая идентификационная система (AIS) для судов является важнейшим источником доказательств при расследовании незаконного, несообщаемого и нерегулируемого (ННН) рыбного промысла или сброса токсичных отходов в международных водах. Намеренное отключение AIS-транспондеров (так называемые «темные суда») оставляет цифровые аномалии, которые могут быть проанализированы экспертами[3].

2. Данные дистанционного зондирования Земли (ДЗЗ). Метаданные спутниковых снимков высокого разрешения служат объективным электронным доказательством незаконной вырубки лесов или деградации земель в результате нелегальной добычи ископаемых. Эти файлы содержат точные временные метки (timestamps) и координаты.

3. Коммуникационные данные и электронная коммерция. Незаконная торговля дериватами диких животных (слоновая кость, рог носорога, редкие виды рептилий) активно переместилась на платформы электронной коммерции, в социальные сети и закрытые сегменты интернета (DarkNet). Соответственно, электронная переписка, логи IP-адресов и метаданные профилей пользователей являются ключевыми доказательствами[4].

Сложность заключается в том, что эти данные хранятся на серверах частных технологических компаний (провайдеров услуг), которые, как правило, расположены за пределами юрисдикции государства, на территории которого был причинен экологический ущерб. Это порождает конфликт между национальным суверенитетом и глобальной природой интернета, создавая так называемую проблему «утраты локации» (loss of location).

Правовые и институциональные проблемы обмена

Фундаментальной проблемой, обсуждаемой на международных форумах, является критическое несоответствие между скоростью изменения или удаления электронных данных и медлительностью традиционных правовых инструментов.

Исторически основным инструментом получения доказательств из-за рубежа являлись Договоры о взаимной правовой помощи по уголовным делам (MLAT — Mutual Legal Assistance Treaties). Однако процедура MLAT была разработана для бумажного документооборота. Запрос должен пройти через органы

[3] INTERPOL. (2020).Strategic Analysis Report: Emerging Criminal Trends in the Global Environmental Security Sector. INTERPOL Environmental Security Programme.

[4]UNODC. (2020). World Wildlife Crime Report: Trafficking in protected species. United Nations Office on Drugs and Crime, Vienna, pp. 24-28.

следствия, Генеральную прокуратуру (или Министерство юстиции) запрашивающего государства, затем по дипломатическим каналам поступить в центральный орган запрашиваемого государства, и лишь потом быть переданным для исполнения местным правоохранителям. По оценкам экспертов ООН, исполнение запроса MLAT занимает в среднем от 6 до 24 месяцев[5].

В контексте экологических преступлений такая задержка фатальна. Данные биллинга, IP-логи или записи с камер наблюдения, доказывающие причастность лиц к контрабанде редких видов фауны, могут быть автоматически удалены провайдерами в рамках их политики хранения данных уже через 30–90 дней.

Кроме того, возникает проблема защиты персональных данных. Глобальные провайдеры (Google, Meta, Microsoft и др.) часто отказываются предоставлять электронную информацию по прямым запросам иностранных правоохранительных органов, ссылаясь на строгое национальное и региональное законодательство — например, на Общий регламент ЕС по защите данных или Закон США о хранении сообщений. В результате следствие заходит в тупик из-за юрисдикционных коллизий[6].

Процессуальные трудности: допустимость и целостность данных

Помимо бюрократических барьеров, серьезную проблему представляет процессуальная допустимость электронных доказательств, полученных из-за рубежа. Поскольку уголовно-процессуальные кодексы разных стран не унифицированы, доказательство, собранное с соблюдением всех правил в государстве «А», может быть признано недопустимым в суде государства «Б».

Для того чтобы электронный файл имел юридическую силу, следствию необходимо подтвердить его целостность и аутентичность. В международной практике это обеспечивается механизмом «цепи сохранности» (chain of custody) и криптографическим хешированием (например, алгоритмами MD5 или SHA-256)[7]. Если при передаче данных от иностранного провайдера или зарубежного правоохранительного органа хеш-сумма файла изменится хотя бы на один бит, защита в суде успешно оспорит такое доказательство, заявив о его модификации.

Особая проблема в сфере экологических преступлений заключается в нехватке специализированных кадров. Расследованием незаконной вырубки, браконьерства или загрязнения вод часто занимаются профильные природоохранные инспекции или экологическая полиция. В отличие от подразделений по борьбе с киберпреступностью, экологические инспекторы редко обладают навыками цифровой криминалистики (digital forensics). Они могут неправильно изъять электронный носитель (например, подключить GPS-навигатор браконьеров к компьютеру без использования блокиратора записи),

[5] United Nations Security Council. (2018). CTC/CTED Technical Guide to the implementation of Security Council resolution 2322. Counter-Terrorism Committee Executive Directorate.
[6] Council of Europe. (2021). Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg, p. 12-15.
[7] SWGDE. (2021). SWGDE Best Practices for Computer Forensics. Scientific Working Group on Digital Evidence. Version 3.1.

что приведет к уничтожению метаданных и утрате доказательства для международного суда[8].

Перспективы и новые международно-правовые механизмы

В ответ на вышеуказанные вызовы мировое сообщество разрабатывает инновационные правовые рамки. Ключевой перспективой в области обмена цифровыми доказательствами является применение Второго дополнительного протокола к Будапештской конвенции о киберпреступности, открытого для подписания в 2022 году.

Данный Протокол революционизирует систему: он позволяет правоохранительным органам договаривающихся сторон напрямую запрашивать данные о регистрации (subscriber information) у провайдеров услуг, находящихся в других странах, минуя долгий процесс MLAT. Также вводится механизм ускоренного сохранения данных (expedited preservation of stored computer data) и экстренной взаимной помощи в ситуациях, представляющих непосредственную угрозу (в том числе при масштабных экологических катастрофах)[9].

На региональном уровне перспективы связаны с пакетом законов Европейского Союза об электронных доказательствах (E-evidence package), который внедряет систему Европейских ордеров на предоставление и сохранение данных. Провайдеры обязаны реагировать на такие ордера в срок от 10 дней до 6 часов (в экстренных случаях)[10].

Также огромный потенциал имеет использование технологий распределенного реестра (блокчейн) для фиксации «цепи сохранности» международных доказательств. Интеграция хэш-сумм спутниковых снимков или логов финансовых транзакций в неизменяемый блокчейн позволит судам любой юрисдикции мгновенно верифицировать подлинность электронного документа без необходимости вызова иностранных экспертов.

Заключение

Международный обмен электронными доказательствами становится краеугольным камнем в борьбе с транснациональной экологической преступностью. Текущая система правовой помощи не поспевает за скоростью цифровизации организованных преступных групп. Проблемы юрисдикции, экстерриториальности хранения данных и различия в процессуальных стандартах создают «белые пятна», которыми активно пользуются эко-преступники. Тем не менее, принятие новых международных конвенций (таких как Второй дополнительный протокол) и развитие защищенных каналов связи Интерпола открывают реальные перспективы для ускорения процессов обмена данными.

[8] UNODC. (2019). Data Matters: Practical Guide for Requesting Electronic Evidence Across Borders. United Nations Office on Drugs and Crime.

[9] Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

[10] European Parliament. (2023). Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. Official Journal of the European Union.

На основе проведенного анализа и материалов международных дискуссий предлагаются следующие практические шаги для государств и ведомств:

1. Имплементация международных стандартов: Национальным парламентам рекомендуется ускорить ратификацию Второго дополнительного протокола к Будапештской конвенции и обновить национальные Уголовно-процессуальные кодексы, закрепив в них понятия «электронное доказательство» и процедуры прямого трансграничного запроса к интернет-провайдерам.

2. Создание механизмов экстренного сохранения: Внедрить в национальную практику правовые инструменты для немедленного замораживания (сохранения) электронных данных по запросу иностранного экологического ведомства до направления официального запроса MLAT (data preservation request).

3. Межведомственная интеграция и обучение: Организовать обязательные курсы повышения квалификации по основам цифровой криминалистики (digital forensics) для сотрудников природоохранных прокуратур и экологических инспекций. Целесообразно создание совместных следственных групп (JITs), в которые наряду с экологами будут входить специалисты по кибербезопасности.

4.Технологическая модернизация: Внедрить использование криптографического хеширования и блокчейн-технологий на этапе первоначального сбора цифровых данных (например, при изъятии данных с GPS-устройств браконьеров или получении спутниковых снимков), что гарантирует процессуальную допустимость этих доказательств в зарубежных судах при трансграничном обмене.

Adabiyotlar, References, Литературы:

1. Council of Europe. (2021). Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg. URL: https://rm.coe.int/1680a49c9d

2. Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

3. European Parliament. (2023). Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. Official Journal of the European Union.

4. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543

5. FATF. (2021). Money Laundering from Environmental Crime. Financial Action Task Force, Paris. https://www.fatf-gafi.org/en/publications/Environmentalcrime/Money-laundering-from-environmental-crime.html

6. INTERPOL. (2020). Strategic Analysis Report: Emerging Criminal Trends in the Global Environmental Security Sector. INTERPOL Environmental Security Programme. URL: https://www.interpol.int/Crimes/Environmental-crime (Примечание: полные оперативные отчеты Интерпола доступны только для правоохранительных органов, ссылка ведет на официальный портал программы).

7. SWGDE. (2021). SWGDE Best Practices for Computer Forensics. Scientific Working Group on Digital Evidence. Version 3.1. https://swgde.org/documents
8. United Nations Security Council. (2018). CTC/CTED Technical Guide to the implementation of Security Council resolution 2322. Counter-Terrorism Committee Executive Directorate. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_technical_guide_to_the_implementation_of_scr_2322.pdf
9. UNODC. (2019). Data Matters: Practical Guide for Requesting Electronic Evidence Across Borders. United Nations Office on Drugs and Crime, Vienna.
URL: https://www.unodc.org/unodc/en/cybercrime/data-matters.html
10. UNODC. (2019). Electronic Evidence: A compilation of cases from the SHERLOC Database. United Nations Office on Drugs and Crime, Vienna.
URL: https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence.html
11. UNODC. (2020). World Wildlife Crime Report: Trafficking in protected species. United Nations Office on Drugs and Crime, Vienna. https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf
12. UNODC / CCPCJ. (2022). Resolutions and Decisions of the 31st session of the Commission on Crime Prevention and Criminal Justice. https://www.unodc.org/unodc/en/commissions/CCPCJ/session/31_Session_2022/session-31-of-the-ccpcj.html