

УДК 343.98:336.7

DOI 10.33244/2617-4154.3(24).2026.303-313

G. O. Panasenko,*Doctor of Economic Sciences, Associate Professor,
Professor of the Department of Financial Investigations and Economic Security
at the Research and Training Institute of Economic Security and Customs Affairs,
State Tax University***Г. О. Панасенко,***доктор економічних наук, доцент,
професор кафедри фінансових розслідувань та економічної безпеки
Навчально-наукового інституту економічної безпеки та митної справи,
Державний податковий університет
email: panasenkohanna@uacu.edu.ua***ORCID 0000-0002-6743-6728**

FINANCIAL INVESTIGATION OF SEXTORTION THROUGH THE LENS OF PAYMENT INFRASTRUCTURE AND MONEY MULE DETECTION

ФІНАНСОВЕ РОЗСЛІДУВАННЯ СЕКСУАЛЬНОГО ВИМАГАННЯ КРІЗЬ ПРИЗМУ ПЛАТІЖНОЇ ІНФРАСТРУКТУРИ ТА ВИЯВЛЕННЯ ФІНАНСОВИХ МУЛІВ

The rapid growth of financially motivated cybercrime recorded at the global level necessitates the development of specialized methodological tools for its detection and investigation within the financial monitoring system. The purpose of the article is to examine the payment infrastructure of financially motivated sexual extortion and to develop methodological foundations for its identification within the financial monitoring system. The study is based on a comparative analysis of official statistics from law enforcement agencies and international organizations across multiple jurisdictions, employing methods of typological analysis of financial crimes, transactional profiling, and forensic reconstruction of fund movement chains. It is established that financially motivated sexual extortion is characterized by a stable transactional typology: serial small-value transfers, atypical temporal activity, discrepancy



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

© Panasenko G. O., 2026

between payment references and context, and indicators of transit account usage with subsequent value extraction through convertible virtual assets and cross-border channels. The study systematizes five primary payment channels of the scheme with corresponding risk indicators. A mechanism for detecting "mirror transactional anomalies" is substantiated, enabling the correlation of fiat and cryptocurrency flows without obtaining KYC data at the initial investigative stage. A three-stage forensic algorithm for financial investigation is developed, encompassing primary express detection, retrospective transactional analysis, and procedural digital evidence preservation. The necessity of modifying standard risk indicators for destabilized payment environments is substantiated, where classical behavioral and geographic compliance filters demonstrate a critical level of false positives. Effective counteraction to financially motivated sexual extortion requires a transition from reactive responses to a systemic financial investigation methodology grounded in risk-based analysis of transactional anomalies across a composite set of parameters. The proposed toolkit ensures the procedural linking of local intermediaries to transnational scheme organizers even when the ultimate value extraction point lies beyond the reach of national investigation.

Keywords: financially motivated sexual extortion, financial investigation, money mules, transactional analysis, payment infrastructure, cryptocurrency circuit, risk indicators, financial monitoring.

Стрімке зростання кіберзлочинів із фінансовою мотивацією, що фіксується на глобальному рівні, зумовлює потребу в розробці спеціалізованого методологічного інструментарію для їх виявлення та розслідування в системі фінансового моніторингу. Метою статті є дослідження платіжної інфраструктури фінансово мотивованого сексуального вимагання та розробка методологічних засад його виявлення в системі фінансового моніторингу. Дослідження ґрунтується на порівняльному аналізі офіційної статистики правоохоронних органів і міжнародних організацій у розрізі декількох юрисдикцій, методах типологічного аналізу фінансових злочинів, транзакційного профілювання та криміналістичної реконструкції ланцюгів руху коштів. Встановлено, що фінансово мотивоване сексуальне вимагання характеризується стійкою транзакційною типологією: серійність дрібних переказів, нетипова часова активність, невідповідність призначень платежів контексту та ознаки транзитного використання рахунку з подальшим виведенням вартості через конвертовані віртуальні активи й транскордонні канали. У процесі дослідження систематизовано п'ять основних платіжних каналів схеми з відповідними індикаторами ризику. Обґрунтовано механізм виявлення «дзеркальних транзакційних аномалій», що дає змогу встановити кореляцію між фіатним і криптовалютним контурами без отримання даних KYC на першому етапі. Розроблено триетапний криміналістичний алгоритм фінансового розслідування, що охоплює первинну експрес-детекцію, ретроспективний транзакційний аналіз і процесуальну фіксацію цифрових слідів. Обґрунтовано потребу в модифікації стандартних індикаторів ризику для умов дефініційованого платіжного середовища, в якому класичні поведінкові та географічні фільтри комплаєнсу демонструють критичний рівень хибних спрацювань.

Ефективна протидія фінансово мотивованому сексуальному вимаганню потребує переходу від реактивного реагування до системної методології фінансового розслідування, заснованої на ризик-орієнтованому аналізі трансаційних аномалій у сукупності параметрів. Запропонований інструментарій забезпечує процесуальне пов'язування локальних посередників із транснаціональними організаторами схеми навіть за умови недосяжності кінцевої точки виведення коштів для національного слідства.

Ключові слова: фінансово мотивоване сексуальне вимагання, фінансове розслідування, підставні одержувачі коштів, трансаційний аналіз, платіжна інфраструктура, криптовалютний контур, індикатори ризику, фінансовий моніторинг.

Problem Statement. Financially motivated sexual extortion (FMSE) constitutes a category of cybercrime in which coercion to make monetary transfers is effected through the threat of disseminating compromising materials. The payment dimension of the scheme represents the primary object of financial investigations – the movement of funds generates an observable trail enabling the identification of perpetrators, intermediaries, and mechanisms for concealing criminal proceeds.

The scale of FMSE as a financial crime typology is corroborated by data across multiple jurisdictions. In 2024, the FBI recorded approximately 55,000 reports related to FMSE, with aggregate financial losses of USD 33.5 million – a 59 % increase relative to 2023. Over the period October 2021 through July 2025, the Homeland Security Investigations (HSI) division of the U.S. Department of Homeland Security received 8,483 reports, resulting in the identification of 854 victims, 232 arrests, and the preparation of 96 indictments. In Australia, the Australian Centre to Counter Child Exploitation (ACCCE) recorded an average of 300 reports per month throughout 2023; in the first half of 2024, this figure declined to 93 reports per month amid targeted disruption of the scheme's financial channels. In the United Kingdom, the Internet Watch Foundation (IWF) confirmed 176 cases of sextortion involving child sexual abuse material in 2023, compared to 21 in 2022; by 2025, the number of reports submitted through the Report Remove service reached 394. At the global level, aggregated NCMEC data indicate a 149 % increase in reports over the 2022–2023 period. The social consequences of this typology are critical in nature: since 2021, no fewer than 36 minors in the United States have died by suicide as a result of threats to publish intimate materials.

A concise statistical overview of the subject matter across jurisdictions is presented in Table 1.

Table 1 – Key Statistical Indicators of Financially Motivated Sexual Extortion by Jurisdiction [1–6]

Jurisdiction	Source	Period	Indicator
USA	FBI / FinCEN	2024	55,000 reports; \$33.5 million in losses; +59 % compared to 2023
USA	HSI (DHS)	Oct. 2021 – Jul. 2025	8,483 reports; 854 victims; 232 arrests; 96 indictments
USA	FBI	since 2021	More than 36 suicides of minors related to FMSE
Australia	ACCCE / AFP	2023	300 reports per month; operation Huntsman: > 1,800 closed accounts
Australia	ACCCE / AFP	1st half of 2024	560 reports (93 per month); 69 % decrease compared to the 2023 average
UK	IWF	2021–2025	6 (2021) → 21 (2022) → 176 (2023) → 175 (2024) → 394 (2025) cases
UK	IWF	2025	98 % of victims are boys aged 14–17
Globally	NCMEC / Thorn	2022–2023	10,731 → 26,718 reports (+149 %); ~812 reports per week

The persistent recurrence of the typology and the scale of losses necessitate treating financially motivated sexual extortion as a systemic threat in which the financial infrastructure functions simultaneously as an instrument of coercion and a channel for extracting criminal proceeds.

The transnational character of financially motivated cybercrime is corroborated by FATF data: according to the organization's assessments, proceeds from cybercrime migrate rapidly across multiple jurisdictions, rendering their tracing critically dependent on inter-agency cooperation and timely financial intelligence exchange [7]. The report further establishes that the deployment of money mule networks in financially motivated cybercrime schemes constitutes a stable typology, wherein accounts are utilized for a limited period through legitimate account-opening procedures, substantially impeding the timely detection of anomalous activity by financial institutions.

The relevance of financially motivated sexual extortion to Ukraine is determined by a set of structural factors that elevate the financial system's vulnerability to this typology. According to the ENISA Threat Landscape report for the Finance Sector covering January 2023 through June 2024, European jurisdictions affected by armed conflict exhibit a significant increase in financially motivated cybercrime, with social engineering and online extortion schemes ranking among the most prevalent instruments employed [8]. Under conditions of ongoing conflict, standard client behavioral patterns undergo substantial transformation – forced population mobility, the mass opening of new accounts, and atypical transaction geographies complicate the differentiation of anomalous activity associated with financially motivated sexual extortion from the broader backdrop of a destabilized payment environment.

Children and adolescents constitute the most vulnerable demographic group in the context of financially motivated sexual extortion in Ukraine. In particular, according to the verified findings of an all-Ukrainian empirical study conducted by the State Service for Education Quality

Panasenko G. O. Financial investigation of sextortion through the lens of payment infrastructure and money mule detection

of Ukraine in partnership with the Dignity Online expert community and the Proinsight Lab analytical agency under the auspices of the Cabinet of Ministers of Ukraine, approximately 12.6 % of student respondents aged 10–17 had encountered direct demands to generate and transmit personal intimate content. In 53 % of recorded incidents, the primary initiators of such harmful communications were entirely unknown individuals, substantially increasing the latency of the threat. Against this backdrop, the willingness of minors to transition from virtual interaction to real-world offline meetings demonstrated a critical surge – from 7 % in 2020 to 31.8 % in 2024 – exponentially expanding the potential victim pool subject to criminal coercion [9; 10].

Accordingly, preventive financial monitoring of anomalous transactional flows and the proactive identification of distributed money mule networks assume the status of critically significant instruments for collective security assurance within the prevailing geopolitical and macroeconomic context. The modernization of compliance procedures and the disruption of criminal proceeds laundering channels represent, in this context, an indispensable condition for minimizing latent cyber threats and protecting the most vulnerable segments of the population amid the comprehensive destabilization of the traditional financial sector.

Literature Review. The subject of sexual extortion within the context of financial and payment infrastructures remains a comparatively nascent and fragmented area of scholarly inquiry. Despite a growing body of work on cybercrime and financial flows in the digital environment, specialized studies integrating sextortion with the analysis of payment mechanisms remain limited.

Edwards and Hollely [11] examine the characteristics of financially motivated cyber extortion (sextortion) through the analysis of more than 23,000 anonymous victim reports submitted to the Scam Survivors support forum. Primary attention is devoted to typical offending patterns: perpetrator profiles (most commonly impersonating young women), platforms utilized for initial contact and communication, preferred payment methods, and the geographic origin of extortionists (predominantly the Philippines and West African states). The authors draw particular attention to the rapid diversification of criminal tactics: whereas offenders previously concentrated their activity on a limited number of platforms (Skype, Facebook) and transfer services (Western Union), they now exploit a broad spectrum of emerging applications (such as Instagram) and cryptocurrency wallets, posing significant obstacles for law enforcement and complicating the development of universal protective measures.

The phenomenon of large-scale sextortion spam campaigns demanding Bitcoin ransoms is examined by Paquet-Clouston, Romiti, Haslhofer, and Charvat [12]. Drawing on a dataset of more than 4.3 million spam messages, the authors analyze the pricing strategies employed by offenders (ransom amounts frequently vary by message language and specific campaign), document instances of Bitcoin address reuse, and trace money laundering pathways within the blockchain. The principal finding highlighted by the researchers is that sextortion enables spam operators to substantially reduce operational costs by eliminating complex stages characteristic of conventional spam (such as website hosting or goods delivery), while generating substantial profits – at minimum USD 1.3 million over an eleven-month period.

Particular attention is warranted by the findings presented in the report of the Rights Lab research centre at the University of Nottingham [13]. The researchers examine financial flow

mechanisms and payment methods employed in the online sexual exploitation of children, with specific focus on live-streamed abuse cases originating in the Philippines. The analysis investigates the use of money transfer services, banking transactions, and cryptocurrencies through which offenders in developed countries direct small-value payments to local facilitators. The central problem identified by the authors is the extreme difficulty faced by the financial sector and law enforcement in detecting such payments: low-value transfers are readily disguised as legitimate remittances or charitable contributions, while stringent banking confidentiality and data protection legislation impedes effective information sharing with investigative authorities.

The study by Choi, Chawki, and Basu [14] investigates the financial infrastructure of cryptocurrency-enabled cyber extortion on the basis of 87 confirmed cases. Employing blockchain forensic methods and extortion text analysis, the authors examine how offenders structure their operations and the money laundering techniques they deploy, including the use of cryptocurrency mixers, peel chain algorithms, and regulated cryptocurrency exchanges.

Identification of Previously Unresolved Aspects of the Problem. Notwithstanding the rapid escalation of cybercrime, the scientific and methodological toolkit for financial monitoring of sextortion payment infrastructure remains fragmented, with specialized research in this domain being extremely limited in scope. At the applied level, existing banking compliance algorithms are incapable of effectively differentiating the latent low-value transactions of extortionists from standard retail transfers – a challenge that is critically compounded by the forced distortion of client behavioral patterns under wartime conditions. Furthermore, institutional and legal barriers in the sphere of data confidentiality protection continue to obstruct the development of mechanisms for prompt end-to-end exchange of actionable intelligence between financial sector representatives and specialized cybercrime investigative units.

The purpose of the article is to examine the payment infrastructure of financially motivated sexual extortion and to develop methodological foundations for its identification within the financial monitoring system.

Presentation of the Main Research Findings. The standard algorithm of financially motivated sexual extortion comprises four stages: initial contact through social networks or gaming platforms; migration of communication to closed channels; acquisition of compromising material (obtained directly from the victim or synthesized from available content); and submission of a monetary transfer demand. The temporal dynamics of the scheme are of critical significance: extortion may unfold within a matter of minutes, and following the first payment, pressure typically intensifies, evolving into a series of repeated demands. The serial nature of transfers increases the probability of detection through monitoring systems, while simultaneously elevating the risk of secondary victimization.

The selection of a payment channel is determined by the victim's characteristics and the offender's strategy for minimizing the evidentiary trail. Transfers involving minors typically fall within the range of USD 10–50; those involving adults, within USD 500–2,500. These intervals serve as probabilistic parameters for comparison against the client's behavioral profile rather than as formal threshold values.

Table 2 – Payment Channels of Financially Motivated Sexual Extortion and Corresponding Risk Indicators

Channel	Characteristic	Risk Indicator
P2P transfers (phone/e-mail)	High speed, low transaction costs	Serial transfers, night-time activity
Prepaid cards / gift cards	Anonymity, transmission of card credentials	Single top-up with immediate transfer
Cash money transfers	Cross-border disbursement in local currency	Atypical destinations, no business nexus
Convertible virtual currency	Trail disruption, withdrawal to external wallet	CVV purchase with immediate extraction
Postal items (cheques, cash)	Minimal digital footprint	Atypical account activity

The diversity of channels indicates a deliberate distribution of blocking risk across multiple segments of the payment infrastructure, which complicates monitoring by any individual provider [11].

The cryptocurrency circuit of the scheme presents particular analytical complexity, wherein traditional financial monitoring instruments encounter fundamental limitations of both jurisdictional and technological character.

A promising direction for advancing the investigative methodology of the cryptocurrency circuit involves the transition from linear wallet tracing to a method of end-to-end chronological cross-referencing of fiat and digital flows. The principal practical impediment lies in the fact that direct requests to foreign cryptocurrency platforms are either time-consuming or altogether impossible when perpetrators utilize unregulated exchange services.

To overcome this barrier, the author proposes the application of a "mirror transactional anomaly" detection mechanism. This approach does not require the immediate disclosure of exchange data and is premised on the analysis of two parallel investigative lines:

1. In the fiat sector, the precise timestamp and volume of funds debited from the money mule's account via a banking application to a specific P2P exchange are recorded.
2. In the digital sector, the wallet of that same exchange is identified within the public blockchain, from which an equivalent sum in virtual assets is transmitted – within an analogous time interval, adjusted for the network's technological latency of several minutes – to the address of the scheme's organizer.

The strict temporal and value-based correlation between the fiat outflow and the cryptocurrency receipt enables the investigator to proceed without KYC data at the initial stage. The coincidence of these parameters constitutes a sufficient body of circumstantial evidence to establish the legal fact of ownership or control over a specific anonymous wallet. In the context of judicial proceedings, this affords the procedural means to prove criminal intent and to link the conduct of local intermediaries (money mules) to the transnational organizers of the extortion scheme, even where the ultimate value extraction point lies beyond the reach of the national investigation.

The inaccessibility of the ultimate extraction point to the national investigation is a direct consequence of the transnational organizational structure of financially motivated sexual extortion.

The organizers of such schemes are typically located outside the victim's country of residence – predominantly in West African and Southeast Asian states – and conceal their actual whereabouts through the manipulation of network access parameters. Value is extracted through money transfer operators with disbursement in local currency, conversion into convertible virtual currency with transfer to an external wallet, or a commodity circuit involving the procurement of goods by intermediaries with subsequent dispatch to the organizer abroad. For investigative purposes, it is not only the place of registration of the payment service that is relevant, but also the routing of value following the initial crediting of funds [15].

The differentiation between the role of a victim and that of a money mule is conducted through the analysis of the structure of incoming and outgoing flows, time intervals, counterparty recurrence, and the content of payment references. A complicating factor is the practice of coercing the victim into the role of an intermediate recipient, in which case the account simultaneously exhibits indicators characteristic of both profiles [16]. The characteristics of the participants in the financially motivated sexual extortion scheme are presented in Table 3.

Table 3 – Differential Indicators of Participant Roles within the Financially Motivated Sexual Extortion Scheme

Criterion	Victim Profile	Money Mule Profile
Flow direction	Predominantly outgoing	Multiple incoming → rapid transit
Counterparties	Previously unconnected	Unrelated senders, new recipients
Temporal structure	Night-time / early morning, urgency	Operational dispersal along the chain
Payment references	Requests to cease threats / neutral wording	Absent or economically inexplicable
Funds retention	Minimal (account is depleted)	Minimal (transit)
CVV utilization	Single purchase under duress	Systematic conversion for extraction
Behavioral anomalies	Crisis profile, atypical activity	Stable transit-type pattern

None of the indicators identified above is sufficient in isolation; the investigative hypothesis is formulated on the basis of their concordant aggregate. The financial investigation must reconstruct the value route as a unified process, wherein the role of each subject is determined by their position within the transaction sequence.

For the practical implementation of this approach, the authors have developed a universal end-to-end forensic algorithm and delineated operational procedures for conducting financial

investigations, adapted to the specific working requirements of financial intelligence unit (FIU) analysts and investigators. This operational framework comprises three sequential stages, ensuring a progressive transition from the detection of primary criminal transactions to the formation of a comprehensive evidentiary record.

1. Stage of Primary Express Detection (Transactional Anomaly Screening). At this stage, compliance analysts within financial institutions monitor current payment flows with the objective of identifying the signal triggers recorded in Table 2. In global practice, primary attention is directed toward an abrupt change in the behavioral profile of the potential victim's account, characterized by the sudden emergence of serial P2P transfers occurring during night-time hours that are atypical of the client's historical conduct.

Ukraine-specific qualification: When extrapolating this stage to the Ukrainian financial sector, the standard detection logic requires substantial normative modification. Under conditions of ongoing armed conflict, classical behavioral and geographic compliance filters inevitably generate a critical level of false positives as a result of forced mass population displacement, the disorderly opening of accounts, and the anomalous geographic distribution of payments. Consequently, for Ukraine, the key verifying marker is not geography or device change, but rather the rigid microstructural and temporal dynamics of the transaction – the high-speed zeroing of a card balance immediately following the crediting of funds, or the instant conversion of incoming traffic into prepaid virtual cards and crypto assets.

2. Stage of Retrospective Transactional Analysis (Verification and Link Development). Following the recording of the primary signal, the investigation transitions to in-depth analysis of retrospective data. The investigator's objective at this stage is to verify the roles of scheme participants in accordance with the differential indicators set out in Table 3. The procedure entails mapping the entire counterparty chain: from the payer's account (the victim) through transit nodes of the first, second, and accumulating levels (money mules). The financial investigator reconstructs in detail the time intervals between credits and debits, determining the rate of capital distribution along the chain, and assesses the economic groundlessness of payment references – or their complete absence – thereby enabling the isolation of legitimate civilian transfers from professional cash-out transit networks.

3. Stage of Procedural Digital Evidence Preservation. The defining characteristic of financially motivated sexual extortion lies in the fact that the primary compromising content (video or photo transmissions) is generated in real time and is virtually never retained on the physical devices of scheme participants, rendering classical computer forensic examinations impossible. Under these conditions, the transactional trail acquires the status of a fundamental item of circumstantial evidence capable of procedurally confirming criminal intent, systematic conduct, and the mercenary motive of the offence. The standard operating procedure for evidence preservation requires the investigator to ensure the evidentiary admissibility of materials: thorough documentation of precise server timestamps, IP address access log files for online banking sessions, recording of unique electronic wallet identifiers, and the official consolidation of the payment sequence through verified bank statements. This enables the construction of an irrefutable, coherent model of the criminal mechanism for subsequent presentation before judicial authorities.

Conclusions. Financially motivated sexual extortion is characterized by a stable transactional typology: serial small-value transfers, atypical temporal activity, discrepancy between payment references and context, indicators of transit account usage, and the subsequent extraction of value through convertible virtual currency and cross-border channels. The scale of this phenomenon precludes episodic responses and necessitates reproducible investigative hypotheses grounded in risk-based anomaly analysis.

The end-to-end forensic algorithm developed within the framework of this study systematizes the operational procedures of financial investigation into three sequential stages – primary express detection, retrospective transactional analysis, and procedural digital evidence preservation – providing a reproducible methodological foundation for financial intelligence unit analysts.

Effective counteraction requires: the integration of internal control procedures with the reconstruction of the fund movement chain; the assessment of operations across a composite set of parameters – amount, recurrence, redistribution rate, and counterparty connectivity; and the thorough documentation of timestamps, payment references, and transaction sequences to ensure the evidentiary admissibility of materials. A suspicious activity report must reflect a coherent model of the presumed criminal mechanism rather than a set of disparate indicators. Simultaneously, the specific nature of the typology necessitates appropriate escalation procedures that account for the pronounced psychological vulnerability of the victim-client.

The proposed mirror transactional anomaly detection mechanism enables the establishment of correlation between fiat and digital flows without obtaining KYC data at the initial stage of the investigation, generating a sufficient body of circumstantial evidence for the procedural linking of local intermediaries to the transnational organizers of the scheme.

REFERENCES

1. Federal Bureau of Investigation. 2024 Internet Crime Report. FBI Internet Crime Complaint Center (IC3). 2025. URL : <https://www.ic3.gov>
2. Department of Homeland Security, Homeland Security Investigations (HSI). Sextortion Statistics: October 2021 – July 2025 / U. S. 2025. URL : <https://www.dhs.gov>
3. Australian Federal Police / Australian Centre to Counter Child Exploitation (ACCCE). Promising results as sextortion reports drop but concern for children remains. 2024. URL : <https://www.accce.gov.au/news-and-media/media-release/promising-results-sextortion-reports-drop-concern-children-remains>
4. *Sexually Coerced Extortion: IWF Annual Data and Insights Report 2024* / Internet Watch Foundation (IWF). 2024. URL : <https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/sexually-coerced-extortion/>
5. Nine reports a week from UK children facing online sextortion / Internet Watch Foundation (IWF). 2026. URL : <https://www.iwf.org.uk/news-media/news/nine-reports-a-week-from-uk-children-facing-online-sextortion-as-charity-warns-record-year-just-tip-of-the-iceberg/>
6. Thorn & National Center for Missing & Exploited Children (NCMEC). *Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data*. 2024. URL : https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf.

Panasenko G. O. Financial investigation of sextortion through the lens of payment infrastructure and money mule detection

7. Financial Action Task Force (FATF). *Illicit Financial Flows from Cyber-enabled Fraud*. FATF/OECD, Egmont Group / INTERPOL. 2023. URL : <https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html>
8. *ENISA Threat Landscape: Finance Sector, January 2023 to June 2024* / European Union Agency for Cybersecurity (ENISA). 2025. URL : https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf
9. Dignity Online, State Service of Quality of Education of Ukraine, Proinsight Lab / *Vseukrainske doslidzhennia pro dosvid ukrainskykh ditei v interneti u voienni chasy*. 2025. URL : <https://dignityonline.in.ua/adult/posibnyky/vseukrainske-doslidzhennia-pro-dosvid-ukrainskykh-ditei-v-interneti-u-voienni-chasy-2025/>
10. Кібернасильство: знаємо та протидіємо – в Україні стартує інформаційна кампанія до «16 днів проти насильства» / Кабінет Міністрів України : офіційний урядовий портал. 2024. URL : <https://www.kmu.gov.ua/news/kibernasylstvo-znaiemo-ta-protydiemo-v-ukraini-startuie-informatsiina-kampaniia-do-16-dniv-proty-nasylstva>
11. Edwards M., Hollely N. M. Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*. 2023. Vol. 2. 100038. DOI : <https://doi.org/10.1016/j.jeconc.2023.100038>
12. Paquet-Clouston M., Romiti M., Haslhofer B., Charvat T. Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem / *Advances in Financial Technologies (AFT19)*. 2019. DOI : <https://doi.org/10.48550/arXiv.1908.01051>
13. Celiksoy E., Schwarz K., Sawyer L., Ciucci S. Payment methods and investigation of financial transactions in online sexual exploitation of children cases / University of Nottingham Rights Lab. 2023. URL : <https://www.nottingham.ac.uk/rights-lab>
14. Choi K.-S., Chawki M., Basu S. Uncovering Cryptocurrency-Enabled Sextortion: A Blockchain Forensic Analysis of Transactions and Offender Laundering Tactics. *Information*. 2026. Vol. 17, № 3. P. 236. DOI : <https://doi.org/10.3390/info17030236>
15. Financial Action Task Force (FATF). *Recovering International Proceeds of Crime through Inter-Agency Networks* / FATF-OECD. 2023. URL : <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Recovering-international-proceeds-crime-inter-agency-networks.html>
16. Proceeds of fraud: Detecting and preventing money mules / Financial Conduct Authority (FCA). 2024. URL : <https://www.fca.org.uk/publications/multi-firm-reviews/proceeds-fraud-detecting-preventing-money-mules>

Дата надходження 14.07.2026

Дата прийняття після рецензування 25.07.2026

Дата рекомендації 27.08.2026

Дата публікації 30.09.2026