DOI: https://doi.org/10.32839/2304-5809/2019-11-75-67
УДК 341.456:061.1ЄС

Данильченко А.М.
Національний юридичний університет імені Ярослава Мудрого

БОРОТЬБА ЄВРОПОЛУ З НОВИМИ ТЕНДЕНЦІЯМИ ОНЛАЙН-ЗЛОЧИННОСТІ

Анотація. Стаття присвячена проблемі поширення нових видів онлайн-злочинів та способів Європолу боротьби з ними. Внаслідок стрімкого розвитку шахрайства з банківськими картками, соціальної інженерії, «крадіжки» криптовалют, сексуальної експлуатації дітей в інтернеті та діяльності даркнету і злочинних онлайн-ринків – ці злочини є недостатньо вивченими, а отже і недостатньо врегульованими з правової та організаційної сторони. А анонімність глобальних інформаційних мереж та швидкість передачі інформації дає змогу злочинцям залишатися невідомими та уникати від відповідальності. Саме тому, одним із завдань Європолу є боротьба з цими викликами сьогоденності. Вона полягає у розробці ефективних дій організаційного, правового, технічного характеру та у співробітництві між країнами для виявлення, усунення, покарання та здійснення превентивних заходів.

Ключові слова: Європол, онлайн-злочинність, кіберзлочинність, шахрайство, соціальна інженерія, даркнет.

Danilchenko Angelina
Yaroslav Mudryi National Law University

THE EUROPOL FIGHT AGAINST NEW TRENDS OF THE ONLINE CRIME

Summary. Article is devoted to a problem of fight of Europol as institutions of law and order with distribution of new types online of crimes. It is found out what measures need to be carried out for effective counteraction. In particular it is investigated crimes in the Internet which gets global scale. It is possible to refer frauds with cash cards to them, social engineering, "theft" of cryptocurrencies, sexual exploitation of children on the Internet and activity of the Darknet and criminal online of the markets. On the present, rapid development electronic money - cryptocurrency entered. The question of their address and use is almost not settled in the legislation of the countries, using it criminals steal this money and are enriched. One more problem is illegal obtaining personal data of people on the Internet also the social engineering. As a result, malicious applications extend and fraud with cash cards is committed. Separately, there is a question of trade in children on the Internet and their retractions in commercial sexual exploitation that involves awful consequences. Not less dangerous threat is creation "black" the online market in which extend illegal goods and substances in limited access. Considering these crimes it becomes clear that they are insufficiently studied and consequently and insufficiently settled on legal and the organizational side that generates negative consequences and need to develop approaches for their termination and counteraction. Besides, the anonymity of global information networks and speed of information transfer allows criminals to remain unknown and to avoid from responsibility. For this reason, one of tasks of Europol is fight against these calls, namely need of development of effective actions of organizational, legal, technical character and cooperation between the countries for identification, elimination, punishment and implementation of preventive measures.

Keywords: Europol, online crime, cyber crime, fraud, social engineering, Darknet.

Постановка проблеми. Внаслідок стрімкого розвитку злочинності в Інтернеті, правопорушення, які вчиняються є недостатньо вивченими, а отже і недостатньо врегульованими з правової та організаційної сторони. Багато злочинців залишаються невідомими та уникають від відповідальності. А отже, одним із завдань Європолу є боротьба з цими викликами сьогоденності. Саме тому доцільно розглянути цю проблему та з`ясувати, якими способами можна зменшити кількість вчинюваних злочинів та які превентивні заходи необхідно вжити.

Аналіз останніх досліджень і публікацій. Дане питання досліджували у свої статтях Гуцалюк М.В, Довгань О., Стрельцова О.В., Устименко О.С., Федорова Ю.В, Чорноус Ю.М., Швед О.В. тощо. Науковці досить глибоко аналізували різні види злочинів, які пов'язані з онлайн-злочинністю.

Виділення не вирішених раніше частин загальної проблеми. Діяльність Європолу є невід'ємною частиною боротьби з онлайн-злочинністю. Оскільки щодня вчиняються такі злочини, то ефективна протидія є одним із способів її подолання. Однак для того, щоб здійснювати протидію необхідно досконало вивчити конкретні види онлайн-злочинів. А на сьогоднішній день дане питання недостатньо досліджене, внаслідок чого виникають значні труднощі.

Мета статті. Головною метою цієї роботи є дослідження нових тенденцій онлайн-злочинності, які на сьогодні є поширеними у всьому світі. З'ясування причин та цілей такого явища. Розглянути, чому деякі види онлайн-злочинності залишаються нерозкритими. Виділити та проаналізувати заходи, які здійснює Європол для боротьби та протидії злочинній діяльності в мережі Інтернет.

Виклад основного матеріалу. Кожного дня у світі вчиняється безліч злочинів у різних сферах життя. Для розкриття, попередження злочинів та здійснення ефективної протидії злочинним угрупуванням у кожній країні діють правоохоронні органи та інші спеціальні установи. У системі інституцій Європейського Союзу такою є Європейський поліцейський офіс (Європол) як установа правопорядку. Її метою є підвищення якості взаємодії компетентних органів країн у сфері протидії транснаціональній зло-

чинності. Європол поширює свою діяльність на територію 28 держав-членів Європейського Союзу. Крім того, він компетентний встановлювати співробітництво з третіми державами, які не входять до складу ЄС [1, с. 150]. Україна також здійснює співробітництво з цією організацією в рамках угоди про співпрацю.

Одним із напрямів діяльності Європолу є боротьба з організованою злочинністю в інтернеті. Щодня люди використовують інтернет для задоволення різноманітних цілей: від простого перегляду новин до проведення складних фінансових операцій. Віртуальна реальність стала частиною нашого повсякденного життя, а в ній, як і в реальному світі проходить безліч процесів. Не виключенням серед них – вчинення онлайн-злочинів. Анонімність глобальних інформаційних мереж та швидкість передачі інформації дає змогу використовувати ці переваги не тільки для розвитку інформаційного суспільства, але й для вчинення протиправних діянь. Серед нових та найбільш поширених – «крадіжка» криптовалюти, шахрайство з банківськими картками, соціальна інженерія, сексуальна експлуатація дітей в інтернеті та злочинні онлайн-ринки. Останніми роками Європол стурбований такими небезпечними проявами для суспільства, саме тому у своїх звітах акцентує увагу на такі злочини та способи їх вирішення.

Кіберзлочинність – це злочинність у так званому «віртуальному просторі». Останніми роками здійснюється поширення електронних грошей – криптовалют. Найпоширенішим їх видом сьогодні є біткоїни. Власники та користувачі криптовалют стають жертвами численних хакерських атак та викрадення особистих даних, надаючи доступ до особистих даних. Через відсутність регулюючих механізмів немає гарантії збереження електронних криптогаманців та тягне за собою, неможливість поновити гроші. А анонімність і конфіденційність транзакцій роблять можливим спекулювання валютою та використання її для злочинних операцій, таких як торгівля людьми, контрабанда наркотиків, фінансування тероризму тощо [2, с. 773].

Як наслідок, заволодівши електронними грошима шахраї дедалі більше використовують криптовалюти для фінансування своєї кримінальної активності. Згідно з останніми тенденціями, хакери дедалі більше використовують так званий криптоджекінг. Це означає, що на комп'ютер жертви встановлюється програма, яка здійснює у фоновому режимі майнінг криптовалют. Тобто зловмисники крадуть вже не інформацію, а обчислювальні ресурси. І це набагато ускладнює роботу по виявленню таких загроз, адже важко зрозуміти, що шукати [3, с. 29–30]

Ще однією проблемою пов`язаною з нелегальним отриманням особистих даних людей в Інтернеті є розповсюдження шкідливих програм та шахрайство з банківськими картками. Щодо шахрайства з банківськими картками, то це є досить розповсюдженою проблемою в багатьох країнах ЄС. Шахраї проводять операцію з платіжної картки або з її реквізитами, яка не була ініційована власником картки. Тобто, використовуючи персональні дані особи злочинці можуть здійснити незаконну фінансову операцію перебуваючи у будь-якому місці, чи навіть, країні, що ускладнює розслідування даного злочину. Сьогодні, персональні дані – це новий товар, що пропонується кіберзлочинністю. В еру цифрових технологій людей легко ідентифікувати через банківські рахунки, паролі, які стали основним предметом торгівлі для шахраїв в усьому світі. Адже отримавши дані, злочинці використовують інформацію для здійснення подальшої злочинної діяльності: або проведення фінансових операції, або продаж даних іншим особам у інтернеті. Таким чином, отримуючи фінансову користь та задоволення ідеологічних та політичних цілей.

Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані. Наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [4].

Соціальна інженерія – це спеціальна методика маніпуляції, яка допомагає хакерам витягнути з людини необхідну інформацію завдяки використанню її психології. Метою є отримання особистих даних або здійснити незаконні платежі. Люди не так часто переходять за першим посиланням-приманкою, яке бачать, тож «на гачок» потрапляють не часто. Але якщо влучити в «правильну» ціль, то інколи може бути достатньо і однієї особи, яка зробить це, щоб дістатися до мережі цілої організації [5]. Оскільки проблема кіберзлочинності набула глобального масштабу, а збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн. на рік, а за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн. [7, с. 118], Європол здійснює заходи спрямовані на протидію «крадіжки» особистих даних та майна осіб.

Ще одним напрямком діяльності Європолу в боротьбі з онлайн-злочинами є питання сексуальної експлуатації дітей. У мережі Інтернет здійснюється торгівля дітьми та їх втягування в комерційну сексуальну експлуатацію. Це явище включає в себе дитячу проституцію, порнографію та торгівлю дітьми, кібер-секс туризм. За даними звіту Європолу із питань сексуального примусу та шантажу дітей з використанням мережі Інтернет 2017 року, існує дві основні мотивації для вчинення цих злочинів: сексуальна та фінансова. Неповнолітні є жертвами обох цих мотивацій, проте сексуальне задоволення злочинця, очевидно, є основним мотиваційним чинником. Злочини з фінансовою мотивацією скоюють переважно організовані злочинні групи, які локалізовані за межами Європейського союзу [6, с. 6]. На жаль, в Інтернеті продовжує зростати кількість матеріалів, що містять сексуальну експлуатацію дітей. Однією з таких причин є доступ дедалі молодших дітей до інтернету і соцмереж. А через те, що зловмисники використовують засоби анонімності та шифрування, питання їх виявлення та розкриття ускладнюється. Даний вид Інтернет-злочину є новим, а отже, і недостатньо дослідженим, що тягне за собою обмеженість у виборі засобів та програм втручання для протидії сексуальному примусу та шантажу. Боротьба з сексуальною експлуатацією дітей є проблемою, яка потребує першочергового вирішення, оскіль-

ки вона несе ряд негативних наслідків для фізичного і психічного здоров'я дитини та навіть, її життя. За даними звіту Європолу, серед відомих випадків негативних наслідків одна дитина з трьох (31%) унаслідок віктимізації заподіяла собі шкоду, погрожувала або намагалася покінчити життя самогубством. Стосовно негативних наслідків не було відмінностей, пов'язаних зі статтю або віком дитини [6, с. 25–26].

Даркнет і злочинні онлайн-ринки – не менш небезпечна загроза, яка криється в мережі Інтернет Організовані злочинні угруповання у своїй діяльності часто використовують мережу даркнет. Принцип її роботи полягає в тому, що на веб-сайти такої мережі неможливо потрапити через пошукові системи, а завдяки анонімності та онлайн розрахункам злочинці створили «чорний ринок», на якому розповсюджують нелегальні товари і речовини (наркотики, вкрадені товари, дитяча порнографія, зброя тощо). Діяльність цієї мережі неконтрольована правоохоронними органами, бо не врегульована законодавчо. Як наслідок, злочинні угруповання мають неправомірний доступ до комп'ютерних систем, продають шкідливе програмного забезпечення, організовують хакерські кібератаки, викрадають та продають персональні дані. Незважаючи на те, що правоохоронці закривають такі незаконні онлайн-ринки, постійно з'являються нові.

Розглядаючи такі прояви онлайн-злочинність зрозуміло, що необхідно розробляти правові та інші підходи для їх припинення та протидії. Серед ефективних заходів Європолу щодо протидії кіберзлочинності можна вказати на створення Європейського центру кіберзлочинності. За час його дії було проведено десятки великих операцій з викриття онлайн-злочинності та арешту багатьох злочинців. Окрім того, щороку Європол робить звіти та рекомендації задля поінформованості громадян у реальних небезпеках, які їм загрожують. Оскільки, найбільший успіх у боротьбі із, наприклад, соціальною інженерією матиме освіта потенційних жертв. Щодо вирішення проблеми даркнету, то явно зрозумілим є вироблення міжнародної стратегії, бо одна країна самостійно не зможе припинити цю злочинну діяльність. Європол у співпраці з Європейським центром кіберзлочинності маючи ресурси та можливість виявляють та ефективно борються з онлайн-злочинністю. Вирішення питання дитячої сексуальної експлуатації онлайн потребує окремої стратегії, оскільки йдеться про захист дітей. За рекомендаціями Європолу, пропонується посилити співпрацю між приватним сектором, громадянським суспільством та науковцями для своєчасного виявлення, втручання, розроблення відповідних законодавчих актів, стратегій, механізмів протидії, для запобігання злочинам та реалізації втручань, які враховують потреби жертви, правопорушника та інших груп зацікавлених осіб.

Висновки і пропозиції. Аналізуючи вище сказане, хочеться зробити висновок, що діяльність Європолу є невід'ємною частиною боротьби з онлайн-злочинністю, виходячи з сучасних життєвих реалій. Адже організована злочинність постійно зростає та проявляється у нових злочинах: «крадіжка» криптовалют, шахрайство з банківськими картками, розповсюдження шкідливих програм, соціальна інженерія, сексуальна експлуатація дітей в інтернеті, діяльності даркнету та злочинних онлайн-ринків. Усі ці негативні явища несуть загрозу для людей: деякі з них шкодять майновому стану, а інші – фізичному та психічному стану. У зв'язку з цим, Європол вживає різноманітних заходів організаційного, правового та технічного характеру з метою захисту громадян.

Однак, зважаючи на те, що сьогодні онлайн-злочини є частим та поширеним явищем, окрім вказаних заходів, необхідно проводити співробітництво з країнами, з якими не підписано угоду про співпрацю для ефективного виявлення та протидії злочинності. Адже специфіка Інтернет-злочинів полягає у тому, що перебуваючи на відстані тисячі кілометрів можна нашкодити особам, державі, й не нести за це відповідальності. Не менш ефективним способом може бути проведення спільних нарад для розробки стратегій і програм. І звичайно, інформувати населення про потенційні загрози, проводити навчання серед дорослих та дітей як не потрапити «на гачок» злочинців. Тільки об'єднавши зусилля можна зменшити злочинну діяльність пов'язану з онлайн-злочинами.

Список літератури:

1. Чорноус Ю.М. Завдання міжнародних організацій у боротьбі зі злочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. № 25. С. 144–152.
2. Федорова Ю.В Криптовалюти та їх місце у фінансовій системі. *Економіка і суспільство.* 2018. № 15. С. 771–774. URL: http://economyandsociety.in.ua/journal/15_ukr/116.pdf (дата звернення: 01.11.2019).
3. Довгань О. Світові тенденції в галузі кібербезпеки. *Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест*. 2019. № 6 (червень). С. 71. URL: http://ippi.org.ua/sites/default/files/2019-6.pdf (дата звернення: 24.10.2019).
4. Довбиш Н. Кіберзлочинність в Україні. *Scientific Social Community (Соціально-наукова мережа).* 2013. URL: https://www.science-community.org/ru/ node/16132 (дата звернення: 01.11.2019).
5. Савчук Т. Європол: нові тенденції онлайн-злочинності. *Радіо Свобода.* 2018. URL: https://www.radiosvoboda.org/a/europol-cyber-crime/29496631.html (дата звернення: 01.11.2019).
6. Агенція Європейського Союзу з питань співробітництва правоохоронних органів. Сексуальний примус та шантаж через мережу Інтернет як вид злочину проти дітей. Точка зору правоохоронців. *Інформаційно-ресурсний центр «Дитинство без насильства».* 2017. URL: https://rescentre.org.ua/bezpeka-ditei-v-interneti/zvit-yevropolu-shchodo-seksualnoh o-prymusu-ta-shantazhu-ditei-onlain (дата звернення: 31.10.2019).
7. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1(28). С. 118–128.

References:

1. Chornous, Yu.M. (2011). Zavdannia mizhnarodnykh orhanizatsii u borotbi zi zlochynnistiu [Tasks of international organizations in the fight against crime]. *Combating Organized Crime and Corruption (Theory and Practice),* no. 25, pp. 144–152.
2. Fedorova, Yu.V. (2018). Kryptovaliuty ta yikh mistse u finansovii systemi [Cryptocurrencies and their place in the financial system]. *Economy and society*, no 15, pp. 771–774. Available at: http://economyandsociety.in.ua/journal/15_ukr/116.pdf (accessed 01 November 2019).
3. Dovhan, O. (2019). Svitovi tendentsii v haluzi kiberbezpeky [Global trends in cybersecurity]. *Cybersecurity in the Information Society: An Information and Analysis Digest*, no 6, p. 71. Available at: http://ippi.org.ua/sites/default/files/2019-6.pdf (accessed: 24 October 2019).
4. Dovbysh, N. (2013). Kiberzlochynnist v Ukraini [Cybercrime in Ukraine]. *Scientific Social Community (Social Science Network).* Available at: https://www.science-community.org/ru/ node/16132 (accessed 01 November 2019).
5. Savchuk, T. (2018). Yevropol: novi tendentsii onlain-zlochynnosti [Europol: New Trends in Online Crime]. *Radio Liberty.* Available at: https://www.radiosvoboda.org/a/europol-cyber-crime/29496631.html (accessed 01 November 2019).
6. European Union Agency for the Cooperation of Law Enforcement Bodies. (2017). Sexual coercion and blackmail through the Internet as a crime against children. The point of view of law enforcement officers [Seksualnyi prymus ta shantazh cherez merezhu Internet yak vyd zlochynu proty ditei. Tochka zoru pravookhorontsiv]. *Information resource center "Childhood without violence"*. Available at: https://rescentre.org.ua/bezpeka-ditei-v-interneti/zvit-yevropolu-shchodo-seksualnoh o-prymusu-ta-shantazhu-ditei-onlain (accessed 31 October 2019).
7. Hutsaliuk, M.V. (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti [Current trends in organized cybercrime]. *Information and law,* no. 1(28), pp. 118–128.