УДК: 004.4

https://doi.org/10.32689/2617-9660-2021-3(15)-80-86

Кривоножко Галина Євгенівна,
кандидат технічних наук, старший науковий співробітник, завідувач сектором інформаційних технологій лабораторії авторського права та інформаційних технологій, Науково-дослідний центр судових експертиз з питань інтелектуальної власності бульвар Л. Українки, 26, офіс 501, м. Київ, 01133, тел.: +38 044 5921401, e-mail: kr_galina@ukr.net, htpp//orcid.org/0000-0002-7635-541X

ПРОБЛЕМНІ ПИТАННЯ ВИЗНАЧЕННЯ РЕФАЙЛІНГУ ЯК ОДНОЇ ІЗ СКЛАДОВИХ КІБЕРЗЛОЧИНУ В УКРАЇНІ ПІД ЧАС ВИКОНАННЯ СУДОВИХ ЕКСПЕРТИЗ (ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ)

Анотація. Експертні дослідження передбачають, що дослідження, проведені експертом, здійснюються на підставі чинного законодавства та на основі спеціальних знань, матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи. В світі та в Україні не існує на сьогодні єдиної методології визначення шкоди від небезпечних діянь у кіберпросторі та/або з його використанням, в тому числі для цілей судочинства. Однак це не заперечує можливості досліджень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, де предметом злочинних посягань є саме комп'ютерна інформація. Також в спеціалізованих експертних установах України здійснюється методичне забезпечення дослідження програмних продуктів як засобів здійснення комп'ютерних злочинів.

В статті наведено основні типи та види кіберзлочинів. Більш детально в статті приділено увагу рефайлінгу (незаконна підміна телефонного трафіку). Розглянуті основні види систем виявлення рефайлінгу, особливості та проблемні питання проведення експертних досліджень щодо визначення рефайлінгу.

Викладені перспективи подальших досліджень з питань, що стосуються визначення рефайлінгу. Тематика проведених досліджень відноситься та спрямована на підвищення ефективності наукових досліджень у сфері телекомунікацій та інформаційних технологій. Рекомендується для використання при проведенні комплексного інженерно-технічного дослідження (експертна спеціальність 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів») та дослідження у сфері інтелектуальної власності (експертна спеціальність 13.1.2 «Дослідження, пов'язані з комп'ютерними програмами і компіляціями даних (базами даних)).

Ключові слова: нелегальна термінація трафіку, рефайлінг, судова експертиза.

Kryvonozhko Halyna Evgenievna,
Candidate of Technical Sciences, Senior Researcher, Head of Information Technology Sector, Laboratory of Copyright and Information Technology, Research Center for Forensic Expertise on Intellectual Property of the Ministry of Justice of Ukraine, 01133, Kyiv, Lesi Ukrainky Blvd, 26: (044) 592-14-01, Email: kr_galina@ukr.net, htpp//orcid.org/0000-0002-7635-541X

PROBLEM QUESTIONS DEFINITION OF REFILEING AS ONE OF THE COMPONENTS OF CYBER CRIME IN UKRAINE DURING THE PERFORMANCE OF FORENSIC EXPERTISE (EXPERT RESEARCH)

Abstract. Expert research assumes that research conducted by an expert is carried out on the basis of current legislation and on the basis of special knowledge, material objects, phenomena and processes that contain information about the circumstances of the case. There is currently no single methodology in the world and in Ukraine for determining the harm from dangerous acts in cyberspace and / or with its use, including for judicial purposes. However, this does not preclude research into the use of computers, systems and computer networks and telecommunications networks, where computer information is the subject of criminal encroachments. Also, specialized expert institutions of Ukraine provide methodological support for the study of software products as a means of committing computer crimes.

The article presents the main types and kinds of cybercrimes. The article pays more attention to refilling (illegal substitution of telephone traffic). The main types of refilling detection systems, features and problematic issues of conducting expert research on the definition of refilling are considered.

Prospects for further research on issues related to the definition of refilling are outlined. The subject of the research is related to the effectiveness of research in the field of telecommunications and information technology. Recommended for use in conducting comprehensive engineering research (expert specialty 10.9 «Research of computer hardware and software», 10.17 «Research of telecommunication systems (equipment) and tools») and research in the field of intellectual property (expert specialty 13.1.2) Research related to computer programs and data compilations (databases)).

Keywords: illegal traffic termination, refilling, forensic expertise.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В Україні не існує на сьогодні єдиної методології визначення шкоди від небезпечних діянь у кіберпросторі та/або з його використанням (один з видів кіберзлочинів *рефайлінг, коли* злочинці для отримання неправомірної вигоди втручаються у роботу мереж операторів), в тому числі для цілей судочинства. Однак це не заперечує можливості досліджень [1, 2] у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, де предметом злочинних посягань є саме комп'ютерна інформація.

Аналіз останніх публікацій за проблематикою. Нелегальна термінація трафіку стала однією з основних проблем будь-якого телекомунікаційного оператора. Проблема такої кіберзлочинності є загальносвітовою [3].

Аналіз досліджень і публікацій свідчить про те, що даному питанню приділяється певна увага. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н. М. Ахтирська, Ю. М. Батурин, П. Д. Біленчук, О. В. Ботвінкін, В. О. Голубєв, В. Д. Гавловський, М. В. Гуцалюк, М. В. Карчевський, М. О. Кравцова, О. М. Литвинов, Ю. Ю. Нізовцев, О. А. Парфило, Б. В. Романюк, О. Р. Росинська, Т. Л. Тропіна, В. С. Цимбалюк, О. М. Черкун, О. К. Юдін та інші.

Незважаючи на значну кількість наукових публікацій, присвячених даним проблемам, розвиток інформаційних технологій, поява нових способів і методів кіберзлочинів зумовлює потребу подальших досліджень цієї тематики [4-6].

Мета статті. Метою статті є загальний опис значення рефайлінгу, проблемних питань, що виникають під час проведення судових експертиз (експертних досліджень) з метою виконання певного експертного завдання експертами.

Тематика проведених досліджень відноситься та спрямована на підвищення ефективності наукових досліджень у сфері телекомунікацій та інформаційних технологій. Узагальнення та висновки, надані за результатами дослідження сприятимуть проведенню об'єктивних та науково обґрунтованих досліджень та рекомендується для використання при проведенні комплексного інженерно-технічного дослідження (експертна спеціальність 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів») та дослідження у сфері інтелектуальної власності (експертна спеціальність 13.1.2 «Дослідження, пов'язані з комп'ютерними програмами і компіляціями даних (базами даних)).

Виклад основного матеріалу. Експертні дослідження передбачають, що дослідження, проведені експертом, здійснюються на підставі чинного законодавства та на основі спеціальних знань, матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи [1]. Сьогодні в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень носіїв комп'ютерної інформації, які використовуються, у тому числі й для методичного забезпечення дослідження програм-

них продуктів як засобів здійснення комп'ютерних злочинів [6].

У Законі України «Про основні засади забезпечення кібербезпеки України»: «*кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України*».

До основних типів кіберзлочинів можна віднести:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;
- правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;
- правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією;
- правопорушення, пов'язані з порушенням авторських і суміжних прав.

До основних видів кіберзлочинів відносяться*:*

кардинг; фішинг (СМС-фішинг; Інтернет-фішинг), вішинг; скімінг; шимінг; онлайн-шахрайство; піратство; мальваре; протиправний контент; рефайлінг. Насьогодні рефайлінг і в Україні інтенсивно розвивається. *Рефайлінг – незаконна підміна телефонного трафіку*.

Відповідно до ч.1 с.42 Закону України «Про телекомунікації»: «*Діяльність у сфері телекомунікацій здійснюється за умови включення до реєстру операторів, провайдерів телекомунікацій, а у визначених законом випадках також за наявності відповідних ліцензій та/або дозволів*» [2]. Передбачена відповідальність відповідно до ст. 361 Кримінального кодексу України за «*несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації*» [7]. Однак, незалежно до вимог, злочинці для отримання неправомірної вигоди втручаються у роботу мереж операторів, чим завдають значної шкоди [3, 8].

Результати впровадження сучасних технічних засобів і технологій інформаційного забезпечення дозволяють говорити про новий етап розвитку процесів інформатизації. При цьому мова йде не тільки про розширення і модернізацію комплексу обчислювальних засобів, а й процеси формування єдиної інформаційної мережі, баз і банків даних, засобів телекомунікації.

Тому *предметом злочинних посягань*, відповідальність за які передбачена розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України, є саме *комп'ютерна інформація* [7].

До основних видів систем виявлення рефайлінгу відносяться [9-11]:

- *активні системи* – що виявляють фродові номери, здійснюючи сесії тестових викликів (продзвонів) з різних частин світу на номери оператора,

• *пасивні системи* – що відрізняють фродові карти від живих абонентів.

До особливостей та проблемних питань проведення експертних досліджень щодо визначення рефайлінгу відносяться [11]:

• злочинець залишається анонімним безпосередньо до розкриття даного злочину. Кіберзлочин – це реальна можливість залишатися на відстані багатьох тисяч кілометрів від своєї жертви чи навіть жертв;

• кіберзлочини важко виявляти та розслідувати саме тому що вони вчиняються за допомогою електронно-обчислювальних машин, які мають свою IP-адресу і правоохоронцям необхідно визначити її серед сотні тисяч інших;

• даний вид злочину приносить значні збитки;

• для розкриття кіберзлочинів необхідне залучення висококваліфікованих ІТ – спеціалістів, оскільки для виявлення і розслідування кіберзлочинів необхідні спеціальні знання та навички;

• особливістю даного виду злочину також являється те, що він має міжнародний характер, тому необхідно розвивати міжнародне співробітництво (а також методи загальної та спеціальної превенції, реалізація яких має здійснюватися на міжнародному рівні) в даній сфері, що сприятиме значному посиленню безпеки, зменшенню кількості кіберзлочинів (особливо на початковому етапі їх скоєння).

Висновки і перспективи подальших досліджень. Таким чином, в даній статті проаналізовано особливості проведення судових експертиз (експертних досліджень) щодо визначення питань вчинення рефайлінгу в Україні.

Перспективою подальших досліджень є завдання із опрацювання методичних рекомендацій щодо проведення експертних досліджень з питань, що стосуються визначення рефайлінгу. Висвітлення проблемних питань, запропонованих рекомендацій щодо процедури аналізу ознак реалізації функцій програмного забезпечення та дій комп'ютера/телекомунікаційного пристрою, на який встановлено програмне забезпечення, можуть бути основою для розробки методик проведення судових експертиз спеціальних програмних засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Наказ Міністерства юстиції України Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : прийнятий 8 жовт. 1998 року № 53/5 // Офіційний вісник України. – 1998. – № 46.

2. Закон України «Про телекомунікації». – Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1280-15.

3. Проблемні питання протидії рефайлінгу в Україні [Електронний ресурс]. – Режим доступу: https://journals.indexcopernicus.com/api/file/viewByFileId/767939.pdf.

4. Проблеми правового та експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності [Електронний ресурс]. – Режим доступу: http://www.academy.ssu.gov.ua/ua/page/page_1581430420.htm.

5. Пассивные методы выявления нелегальной терминации трафика [Елек-

тронний ресурс]. – Режим доступу: https://habr.com/ru/post/320716/.

6. Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації : методичні рекомендації. – Київ : ІСТЕ СБУ, 2016. – 31 с.

7. Кримінальний кодекс України. – Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14.

8. Гладьо Ю.О. Правові аспекти відшкодування операторам мобільного зв'язку шкоди, завданої рефайлінгом. Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід: матеріали ІІ Міжнар. наук.-практ. конф. (Тернопіль, 21-22 квіт. 2017 р.). Тернопіль: Економічна думка, 2017. С. 341-344.

9. Закон України «Про основні засади забезпечення кібербезпеки України». – Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

10. Карчевський М.В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (тези лекцій) / М.В. Карчевський // Злочини в сфері використання ІТ. [Електронний ресурс]. – Режим доступу: http://it-crime.at.ua/index/tezi_lekcij/0-31.

11. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. [Електронний ресурс] – Режим доступу: https://www.gurt.org.ua/articles/34602/.

REFERENCES:

1. Nakaz Ministerstva yustytsiyi Ukrayiny Pro zatverdzhennya Instruktsiyi pro pryznachennya ta provedennya sudovykh ekspertyz ta ekspertnykh doslidzhen′ ta Naukovo-metodychnykh rekomendatsiy z pytan′ pidhotovky ta pryznachennya sudovykh ekspertyz ta ekspertnykh doslidzhen′ : pryynyatyy 8 zhovt. 1998 roku № 53/5 [Order of the Ministry of Justice of Ukraine On Approval of the Instruction on the Assignment and Conduct of Forensics and Expert Research and Scientific and Methodological Recommendations on the Issues of Preparation and Assignment of Judicial Expertise and Expert Research from October 8 1998, № 53/5]. Official Bulletin of Ukraine – Voice of Ukraine, 46 [in Ukrainian].

2. Zakon Ukrayiny «Pro telekomunikatsiyi» [The Law of Ukraine «On Telecommunications»]. (n.d.). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/1280-15 [in Ukrainian].

3. Problemni pytannya protydiyi refaylinhu v Ukrayini [Problematic issues of counteracting refilling in Ukraine]. (n.d.). Retrieved from https://journals.indexcopernicus.com/api/file/viewByFileId/767939.pdf. [in Ukrainian].

4. Problemy pravovoho ta ekspertnoho zabezpechennya pravookhoronnoyi diyal′nosti u sferi protydiyi kiberzlochynnosti [Problems of legal and expert support of law enforcement in the field of combating cybercrime]. (n.d.). Retrieved from http://www.academy.ssu.gov.ua/ua/page/page_1581430420.htm. [in Ukrainian].

5. Passivnyye metody vyyavleniya nelegal'noy terminatsii trafika [Passive methods for detecting illegal traffic termination]. (n.d.). Retrieved from https://habr.com/ru/post/320716/. [in Russian].

6. Doslidzhennya prohramnykh zasobiv shchodo yikh vidnesennya do spetsial′nykh tekhnichnykh zasobiv nehlasnoho otrymannya informatsiyi : metodychni rekomendatsiyi. – Kyyiv : ISTE SBU, 2016. – 31 s.

7. Kryminal′nyy kodeks Ukrayiny [Criminal codex of Ukraine]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].

8. Gladyo, Yu. O. (2017). Pravovi aspekty vidshkoduvannya operatoram mobil′noho zv″yazku shkody, zavdanoyi refaylinhom. [Legal aspects of compensation for damage caused by refilling by mobile operators].

Ukrayina v umovakh reformuvannya pravovoyi systemy: suchasni realiyi ta mizhnarodnyy dosvid: materialy II Mizhnar. nauk.-prakt. konf. (Ternopil′, 21-22 kvit. 2017 r.). Ternopil′: Ekonomichna dumka, 2017. S. 341-344. [in Ukrainian].

9. Zakon Ukrayiny «Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny» [The Law of Ukraine «On the basic principles of cybersecurity in Ukraine»]. (n.d.). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

10. Karchevsky, M. V. (Ed.). (2021). Zlochyny v sferi vykorystannya elektronno-obchyslyuval′nykh mashyn (komp″yuteriv), system ta komp″yuternykh merezh i merezh elektrozv'yazku (tezy lektsiy) [Crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks (abstracts of lectures) // Crimes in the field of IT]. Retrieved from http://it-crime.at.ua/index/tezi_lekcij/0-31 [in Ukrainian].

11. Kiberzlochynnist′ u vsikh yiyi proyavakh: vydy, naslidky ta sposoby borot′b [Cybercrime in all its manifestations: types, consequences and methods of combating] (2016) Retrieved from https://www.gurt.org.ua/articles/34602/ [in Ukrainian].