УДК 343.451

A. Savchenko,
P. Vorobei,
Yu. Belskyi

REFILING (REFILE) AS A METHOD OF COMMITTING OF UNAUTHORIZED INTERFERENCE IN THE WORK OF TELECOMMUNICATION NETWORKS

А.В. Савченко
доктор юридичних наук, професор,
завідувач кафедри кримінального права
Національної академії внутрішніх справ
м. Київ

П.А. Воробей
доктор юридичних наук, доцент,
професор кафедри кримінального права
Національної академії внутрішніх справ
м. Київ

Ю.А. Бельський
кандидат юридичних наук,
провідний спеціаліст відділу правового забезпечення
дозвільної діяльності та застосування санкцій
Управління правового забезпечення
Державної інспекції ядерного регулювання України

РЕФАЙЛІНГ (РЕФАЙЛ) ЯК СПОСІБ ВЧИНЕННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Постановка проблеми. Сьогоднішнє життя вже неможливо уявити без використання мобільних телефонів та мережі Інтернет. Через свою відносну зручність та доступність останнім часом зросла та продовжує зростати кількість дзвінків саме з використанням мережі Інтернет. При цьому провідну роль в цих дзвінках відіграють смартфони, що обладнані відповідними програмами для Інтернет-дзвінків. Такі можливості Інтернету дуже часто стають сферою корисливих інтересів «комп'ютерних» злочинців, які прагнуть отримувати надприбутки, використовуючи відповідні технічні засоби та прогалини у національному законодавстві. Зокрема, останнім часом представники кримінального світу почали масово здійснювати несанкціоноване втручання в роботу мереж електрозв'язку через рефайлінг (рефайл) — незаконну підміну телефонного трафіку. Однак, працівники правоохоронних органів і суди виявилися

не зовсім підготовленими до всебічного розуміння механізму рефайлінгу, а отже і до правильної кваліфікації окреслених вище протиправних дій, відмежування їх від інших і суміжних посягань. Більше того, протидія рефайлінгу вважається одним із завдань кіберполіції, яка відносить його до кіберзлочинів у сфері інформаційної безпеки [1]. Відтак питання з'ясування змісту та сутності рефайлінгу (рефайлу) як способу вчинення несанкціонованого втручання в роботу мереж електрозв'язку є абсолютно актуальними, оскільки мають принципове значення для теорії та практики застосування закону України про кримінальну відповідальність.

Аналіз останніх досліджень і публікацій. Дослідженнями питань про кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також інші «комп'ютерні» злочини, займалися такі науковці як: П.П. Андрушко, Д.С. Азаров, В.М. Бутузов, М.В. Карчевський, В.В. Кузнецов, С.О. Орлов, М.В. Плугатир, Н.А. Савінова та ін. Проте й дотепер такі питання не знайшли свого остаточного вирішення, особливо в контексті специфіки різноманітних форм і способів прояву окремих злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Метою статті є дослідження рефайлінгу (рефайлу) як способу вчинення несанкціонованого втручання в роботу мереж електрозв'язку та формулювання на цій основі теоретичних висновків і практично значущих пропозицій, здатних вплинути на запобігання та протидію цьому негативному кримінально-правовому феномену.

Основні результати дослідження. Мережа Інтернет на сьогодні настільки інтегрувалась в повсякденне життя, що 16.05.2011 р. Спеціальний доповідач ООН з питань про заохочення і захист права на свободу думки та її вільне виявлення Франк Ла Рю представив Раді ООН з прав людини доповідь, в якій підкреслив унікальний та трансформаційний характер Інтернету не тільки для того, щоб люди могли використовувати своє право на свободу думки та вираження поглядів, а й цілу низку інших прав людини та сприяти прогресу суспільства в цілому [2, p. 1]. У наш час смартфони зайняли провідне місце серед пристроїв для зв'язку через мережу Інтернет. При цьому у 2017 р. Україна займала лише 38 місце у світовому рейтингу держав за кількістю використання смартфонів серед населення, оскільки лише 23,5 % мобільних телефонів українців являються смартфонами (для порівняння: в сусідній Польщі цей показник становить 63,4 % всіх мобільних телефонів населення країни) [3]. Таким чином на сьогодні «класичні» дзвінки (за схемою «телефон — телефон») все ще залишаються одним із основних засобів зв'язку в Україні та світі.

Варто зазначити, що телефоні дзвінки, як і будь які інші телекомунікаційні послуги, надаються операторами зв'язку за відповідну абонентну плату у відповідності до постанови Кабінету Міністрів України (далі — КМУ) від 11.04.2012 р. № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг» [4]. При цьому кожному, хто прийняв рішення стати оператором та самостійно надавати послуги у сфері телекомунікацій, слід

зареєструватись та отримати відповідну ліцензію відповідно до законів України від 02.03.2018 р. № 222-VIII «Про ліцензування видів господарської діяльності» (зокрема, п. 8 ч. 1 ст. 7) [5] та від 18.11.2003 р. № 1280-IV «Про телекомунікації» (зокрема, п. 1 ч. 1 ст. 39) [6].

При отриманні дзвінка з-за кордону вітчизняним операторам мобільного зв'язку має надходити оплата від зарубіжних колег за кожний прийнятий дзвінок. При цьому при здійсненні міжнародного дзвінка голосовий трафік, перед тим як потрапляє у мережу вітчизняного оператора, проходить складними каналами телекомунікаційних мереж. Таким чином, встановивши відповідне обладнання та зайнявши місце оператора, можна отримати прибуток, заробляючи на різниці у вартості дзвінків всередині країни та дзвінків за кордон. Саме такі дії називаються «рефайлінгом» (рефайлом), суть яких полягає в підміні голосового трафіку з метою обходу офіційних міжнародних центрів комутації зв'язку та створення з'єднання між абонентами за схемами: «Інтернет — телефон» або «телефон — Інтернет — телефон».

Отже, поняття «рефайлінг» використовується для позначення процесу підміни міжнародного голосового трафіку на локальний шляхом використання IP-телефонії (технології VoIP, англ. «voice over IP» — голос через IP, Інтернет протокол), що являє собою технологію передачі даних за допомогою набору протоколів мережі Інтернет. Цей процес відбувається шляхом перетворення звукових сигналів у цифрові, їх стискання та передачу мережею Інтернет, а також зворотного перетворення в звукові. Суб'єкти, які здійснюють рефайлінг, зазвичай мають фахові знання у галузі телефонії та телекомунікацій, використовують спеціальне комунікаційне обладнання, зокрема GSM-шлюзи, котрі містять набори відповідних SIM-карт, що переводять дзвінки з мережі Інтернет на вітчизняні сім-картки, з яких потім дзвінок переводиться у мережу вітчизняного оператора, де тарифікується лише як дзвінок всередині мережі з подальшою оплатою за «домашніми» тарифами.

Типовою зовнішньою ознакою рефайлінгу може бути ситуація, за якої, наприклад, у абонента Б. номер абонента, що викликає, взагалі не висвічується або висвічується інший (зокрема, місцевий), при цьому абонент Б. не може передзвонити або відправити SMS абоненту А. по номеру, який висвічується [7]. Слід наголосити, що рефайлінгом можуть займатися як окремі зловмисники, так і представники різних комерційних компаній, що спеціалізуються на наданні телекомунікаційних послуг. Існує небезпека того, що рефайлінг можуть неофіційно вчиняти навіть конкуруючі мобільні оператори. За деякими даними можна говорити про існування значної кількості рефайлінгових фірм, на які може припадати близько 20 % всіх доходів, що могли б отримати мобільні оператори за обслуговування міжнародних дзвінків (зокрема, у 2016 р. було зафіксовано понад 12 тис. випадків «рефайлінгу» тільки щодо «Укртелекому») [8].

Різниця між рефайлінгом та використанням легальних Інтернет програм для дзвінків (наприклад, Skype, Viber, What's Up тощо) полягає у тому, що при здійсненні дзвінка через такі програми вони мають бути інстальовані в обох абонентів, тобто на двох кінцях лінії, або ж при дзвінках з програми

(наприклад, такої як «Skype») на фіксований номер мобільного чи стаціонарного зв'язку, тобто виходячи на «+ 380», абонент, який користується зазначеною програмою, повинен оплатити компанії власнику програми «Skype» такий дзвінок, при цьому «Skype» виплачує частину сплачених абонентом коштів оператору зв'язку, до абонента якого надійшов дзвінок. Вважається, що така схема («світ — Україна») є найбільш прибутковою, проте також трапляються схеми, коли дзвінки здійснюються з території України за кордон, чи схеми, в яких територія України виступає транзитом міжнародного трафіку в рефайлінговій схемі.

Поряд із цим можна спрогнозувати, що у майбутньому рефайлінг поступово втрачатиме свою актуальність через зростання популярності голосових сервісів та месенджерів (таких, як Viber, Skype, Telegram, What's UP тощо). Чим більше людей у світі буде мати можливість купувати сучасні смартфони (комунікатори) та використовувати програми, які дозволяють здійснювати безкоштовні дзвінки через мережу Wi-Fi або мобільні мережі, де буде оплачуватися лише Інтернет-трафік, тим меншими будуть доходи мобільних операторів та осіб, які здійснюють рефайлінг. Проте поки що є чимало і тих, хто постійно звертається до рефайлерів. Цьому є багато причин, у т.ч. висока вартість пристроїв із сенсорним екраном, небажання вивчати нові технології (у т.ч. через вікові особливості), нестабільність сигналу безпровідних мереж, політика ідентифікації клієнтів різноманітних сервісів тощо.

В умовах сьогодення досить поширеною є схема рефайлінгу у поєднанні з одним з таких сервісів, як Viber. Цей вид проводиться за схемою «GSM to Viber» (телефон — Інтернет). Для прикладу: абонент з країни А. телефонує абоненту в країні Б., у якого окрім звичайної SIM-карти інстальована ще й програма Viber, при цьому в абонента А. такий сервіс не встановлений. При проходженні дзвінка центрами комутації, якими в цій схемі виступають рефайлери, дзвінок перенаправляється по IP на Viber, таким чином абонент країни Б. приймає вхідний дзвінок не на номер SIM-карти, а на програму Viber. У такій схемі абонент країни А. оплачує своєму оператору вартість міжнародного дзвінка, проте оператор країни Б. свій відсоток оплати за цей дзвінок не отримує, оскільки його отримують рефайлери, які перенаправили цей дзвінок. Така схема є простішою, оскільки для її реалізації потрібна менша кількість обладнання, тобто після перекодування аналогового сигналу з GSM мережі в цифровий і переведення його в Інтернет цей сигнал не потрібно перекодовувати та виводити його в GSM мережу в зворотному порядку.

Законодавством України (законами України «Про телекомунікації» від 18.11.2003 р. № 1280-IV [6], «Про радіочастотний ресурс України» від 01.06.2000 р. № 1770-II [9], постановою КМУ від 11.04.2012 р. № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг» [4]; рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 05.07.2012 р. № 324 «Про затвердження Порядку маршрутизації трафіка в телекомунікаційній мережі загального користування України» [10] та іншими нормативно-правовими актами) врегульовано порядок надання та отримання телекомунікаційних послуг, а саме відносини між

операторами, провайдерами телекомунікацій та споживачами послуг. Зокрема, оператори та провайдери повинні бути внесені до реєстру операторів та провайдерів телекомунікацій, який веде Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі — НКРЗ), а у випадках, встановлених законодавством України, вони повинні мати ліцензії на провадження відповідного виду діяльності у сфері телекомунікацій та/або користування радіочастотним ресурсом України (для операторів) чи копії ліцензій (для провайдерів).

Крім того, рішенням НКРЗ від 29.11.2012 р. № 624 «Про затвердження Основних вимог до договору про надання телекомунікаційних послуг та визнання таким, що втратило чинність, рішення НКРЗ від 26.03.2009 р. № 1420» [11] визначено відповідні вимоги, які є обов'язковими для застосування операторами, провайдерами телекомунікацій і споживачами телекомунікаційних послуг при укладенні договорів про надання телекомунікаційних послуг, внесенні змін та доповнень до них. Таким чином, безліцензійна діяльність або діяльність з порушенням наявних відповідних ліцензій та договорів вважається протиправною і за її вчинення передбачено кримінальну, цивільну та адміністративну відповідальність.

У ст. 33 Закону України «Про телекомунікації» визначено обов'язки споживачів телекомунікаційних послуг (зокрема, споживачі телекомунікаційних послуг зобов'язані дотримуватися Правил надання та отримання телекомунікаційних послуг, що затверджує КМУ) [6]. На сьогодні саме в Правилах надання та отримання телекомунікаційних послуг (набрання чинності відбудеться 23.03.2018 р.) прямо закріплено нормативне поняття рефайлу, яке було внесено постановою КМУ від 20.09.2017 р. № 703 «Про внесення змін до Правил надання та отримання телекомунікаційних послуг», відповідно до якої «рефайл — зміна виду трафіку з метою отримання максимального прибутку за рахунок його маршрутизації за іншою розрахунковою таксою» [12]. Також аналіз цієї постанови КМУ дає підстави стверджувати, що рефайл є одним із способів несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж. Саме ж несанкціоноване втручання в роботу та/або використання телекомунікаційних мереж розуміється як дії, що зафіксовані актом про порушення правил надання і отримання телекомунікаційних послуг і призвели до: витоку, втрати, підробки, блокування, перекручення чи знищення інформації; порушення порядку маршрутизації трафіку голосової телефонії; отримання послуг безоплатно або за тарифами, нижчими від тих, що встановлені; розповсюдження комп'ютерних вірусів (шкідливих програмних засобів); рефайлу; аномальної інтенсивності викликів; непродуктивного трафіку; хибного або помилкового автовідповідача; зациклення трафіку; відмови в обслуговуванні. Більше того, відповідно до ст. 1 Закону України «Про телекомунікації» від 18.11.2003 р. № 1280-IV, поняття «телекомунікації» та «електрозв'язок» є тотожними [6].

Одночасно через рефайл відбувається виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації. Ці наслідки прямо передбачені

ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». І саме цей злочин, як свідчить сучасна судова та слідча практика в Україні, охоплює випадки рефайлінгу. Типовим є такий приклад з практики: відповідно до вироку Франківський районний суд м. Львова від 27.06.2017 р. ОСОБУ_3 визнано винною у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 361 КК України за те, що він у лютому 2016 р. з метою незаконного збагачення шляхом втручання в мережу електрозв'язку національного оператора мобільного зв'язку з використанням спеціального програмно-апаратного комплексу, ознайомившись на Інтернет-ресурсі «GSMmoney» із детальною інструкцією про налаштування за допомогою комп'ютерного обладнання підключень до мережі Інтернет та перетворення їх в «GSM канали», придбавши декілька стартових пакетів мобільного зв'язку, із використанням належного йому портативного комп'ютера (ноутбуку) та чотирьох модемів, почав здійснювати свою незаконну діяльність, спрямовану на несанкціоноване втручання в роботу мереж електрозв'язку оператора мобільного зв'язку «Київстар» [13].

Зазначимо, що вчинення несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку способом рефайлінгу є сьогодні досить поширеною практикою та свідчить про існування цілої злочинної кіберіндустрії. Наприклад: вироком Зарічного районного суду м. Суми від 28.09.2017 р. було встановлено, що, реалізуючи свій злочинний умисел, спрямований на вчинення необмеженої кількості тотожних діянь, які полягають у зміні напрямку міжнародних телефонних дзвінків у телефонній мережі України під виглядом внутрішньодержавних дзвінків, минаючи міжнародні центри комутації з порушенням встановленого порядку їх маршрутизації, діючи з корисливих мотивів, на порушення вимог п. 4 ч. 1 ст. 33 Закону України «Про телекомунікації», п. 5 ч. 36 «Правил надання та отримання телекомунікаційних послуг», ОСОБА_2, ОСОБА_3 та ОСОБА_4, не являючись оператором телекомунікацій, з початку січня 2017 року, використовуючи комплекс телекомукаційного обладнання, запустили і активували вказане обладнання, в результаті чого стали учасниками технологічного процесу з надання послуг міжнародного телефонного зв'язку і отримали можливість організовувати і завершувати вхідні міжнародні телефонні виклики, тим самим, умисно вчинили несанкціоноване втручання в роботу мережі електрозв'язку, яке виразилось в направленні отриманого в мережі Інтернет вхідного міжнародного телефонного трафіка в мережу операторів мобільного зв'язку ПрАТ «МТС Україна» під виглядом внутрішньодержавного дзвінку. При цьому, завершення зазначених викликів здійснювалося з порушенням порядку маршрутизації, встановленого п. 4 «Порядку маршрутизації трафіка в телекомунікаційній мережі загального користування України», затвердженого рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 05.07.2012 р. за № 324, п. 4.8 наказу Державного комітету зв'язку та інформатизації України «Про затвердження положення

про діяльність операторів міжміського, міжнародного зв'язку телефонної мережі загального користування та їх взаємодії між собою» № 19 від 14.02.2001 р., а саме минаючи міжнародних центрів комутації, опорно-транзитних станцій, автоматичних міжміських телефонних станцій. Дії обвинувачених ОСОБА_4, ОСОБА_2 та ОСОБА_3 були кваліфіковані судом за ч. 3 ст. 28, ч. 2 ст. 361 КК України, тобто як несанкціоноване втручання в роботу мереж електрозв'язку, що призвело до порушення встановленого порядку маршрутизації інформації,спотворення процесу обробки інформації, за попередньою змовою у складі організованої групи [14].

У наш час в мережі Інтернет існує безліч компаній, які надають послуги щодо продажу налаштування та обслуговування обладнання й програмного забезпечення, призначеного для рефайлінгу. Однак, такі діяння фактично містять ознаки складу злочину, передбаченого ст. 361 КК України [15, с. 830—834], та є прямим порушенням ст. 31 Конституції України в частині порушення таємниці телефонних розмов [16]. Наприклад, зважаючи на інформацію в Інтернеті, компанія GoAntiFraud надає послуги із встановлення обладнання та надання консультативно-обслуговуючих послуг з налаштування та обслуговування обладнання для рефайлінгу за абонентну плату від 400 $ на місяць, при цьому в пакеті послуг також передбачено можливість запису дзвінків [17].

Як вже наголошувалося, рефайлінг є способом вчинення злочину, передбаченого ст. 361 КК України, а не специфічним проявом крадіжки, шахрайства чи якогось іншого злочину. Загалом під поняттям «спосіб вчинення злочину» слід розуміти прийом або систему прийомів, спрямованих на досягнення результату, що вчинюються в певному порядку, однак в науці кримінального права поки що немає єдності поглядів щодо визначення цього поняття, а тому в даний час воно є дискусійним [18, с. 104]. При несанкціонованому втручанні в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку рефайлінг як спосіб цього злочину — це ціла система складних прийомів, методів, рухів, схем, зв'язків тощо, яка сприяє ефективному вчиненню суспільно небезпечного діяння. Не випадково, що науковці (наприклад, М.І. Панов) справедливо стверджують про те, що спосіб завжди притаманний дії, утворює її зміст, а в деяких випадках — стає окремою дією стосовно основної [19, с. 91—95]. При цьому зауважимо, що ні основний, ні кваліфікований склад злочину, передбаченого ст. 361 КК України, не виділяють якісь специфічні способи його вчинення, а отже зазначений спосіб має лише факультативне значення та не впливає на кваліфікацію вчиненого, відтак в теорії та на практиці може існувати чимало інших способів, за допомогою яких вчинюються «комп'ютерні» злочини, і рефайлінг є лише одним із них. Звідси ми не вбачаємо за необхідність пропонувати спеціально вказувати на рефайлінг у ст. 361 КК України, оскільки некримінальне законодавство дає чітке уявлення про те, що такий спосіб апріорі цілком можливий, а також розкриває його зміст.

Здійснюючи рефайлінг, винні особи передусім порушують встановлений національним законодавством порядок надання телекомунікаційних послуг, який відбувається з використанням комп'ютерних мереж та мереж

електрозв'язку, що слід вважати об'єктом складу несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

З об'єктивної сторони злочин, передбачений ст. 361 КК України, що супроводжується рефайлінгом, передбачає вчинення дій, спрямованих на несанкціоноване втручання в роботу комп'ютерних мереж чи мереж електрозв'язку, які призводять до витоку, втрати, підробки, блокування, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації. Між вказаними діями та наслідками має бути обов'язково прямий причинний зв'язок, а отже, склад аналізованого злочину є матеріальним [15, с. 831—834].

Зазвичай вчинення зазначеного злочину способом рефайлінгу полягає у побудові власної автоматичної телефонної станції. Здебільшого в Україні ці системи спрямовані на розшифровку та виведення рефайлінгового дзвінку, отриманого через Інтернет. Особі потрібно зареєструватись на сайті по обміну голосовим трафіком (наприклад, «http://voipforums.com»), щоб отримати VoIP шлюз — своєрідний Інтернет-канал передачі даних, по якому будуть отримуватись дзвінки з-за кордону для їх подальшого декодування та виведення в національну мережу, або ж навпаки цей шлюз може використовуватись для кодування дзвінків в Україні в цифровий сигнал та передачі в мережу Інтернет для направлення за кордон.

Потрібно також встановити та налаштувати відповідне програмне забезпечення на власні комп'ютери з підключенням їх до мережі Інтернет, підключити 3G-модеми та встановити сім-банки, в які поміщується велика кількість сім-карт, що дає можливість здійснювати кілька з'єднань одночасно. Чим більше сім-карт, тим більше дзвінків, а відповідно й більший прибуток. При цьому інстальоване програмне забезпечення потрібно не просто налаштовувати на прийом та вихід сигналу з сім-карт у відповідний Інтернет-канал, а воно ще повинно імітувати дії людини, так як це було б з використанням сім-карток у мобільному телефоні. Рефайлери рекомендують здійснювати не більше 20 дзвінків удень з однієї сім-карти, при цьому не більше 10 з одного місця, оскільки довготривале перебування абонента в одній точці із здійсненням великої кількості лише вихідних дзвінків призведе до виникнення підозр у мобільного оператора та виявлення зловмисників системами моніторингу активності абонентів, що направлені на моніторинг випадків рефайлу. Для імітації переміщення абонента використовуються кілька GSM-шлюзів, які передають сигнал один одному, створюючи ілюзію переміщення абонента.

Суб'єкт несанкціонованого втручання в роботу мереж електрозв'язку способом рефайлінгу є загальним — фізична, осудна особа, яка досягла шістнадцятирічного віку. Аналіз правозастосовної практики дозволяє стверджувати, що типовий рефайлер (той, хто здійснює рефайлінг) — це особа чоловічої статі, яка має на меті особисте збагачення в незаконний спосіб, не є телекомунікаційним оператором з правом на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів зв'язку, не має відповідної ліцензії, виданої НКРЗ, не має права встановлювати та відповід-

ним чином налагоджувати програмно-апаратні комплекси, діє на порушення вимог Закону України «Про телекомунікації», Правил надання та отримання телекомунікаційних послуг, Порядку маршрутизації трафіка в телекомунікаційній мережі загального користування України, Положення про діяльність операторів міжміського, міжнародного зв'язку телефонної мережі загального користування України та їх взаємодію між собою, наказів Державного комітету зв'язку та інформатизації України тощо.

Із суб'єктивної сторони злочин, передбачений ст. 361 КК України, який вчиняється способом рефайлінгу, характеризується виною у формі прямого умислу. При кваліфікації суспільно небезпечних діянь суди нерідко звертають увагу на наявність корисливих мотивів та такої саме мети (наживи) в діях обвинувачених, хоча на кваліфікацію злочину ці ознаки суб'єктивної сторони складу злочину не впливають, оскільки вони не передбачені у нормі закону про кримінальну відповідальність в якості основних чи кваліфікуючих. Наприклад, Московський районний суд м. Харкова своїм вироком від 16.05.2016 р. визнав винним ОСОБА_3, який, діючи умисно, з корисливих мотивів, переслідуючи мету наживи, здійснив несанкціоноване втручання в роботу мережі електрозв'язку ПрАТ «МТС Україна» [20].

Щодо кваліфікованого складу несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що супроводжується рефайлінгом, то його утворюють такі ознаки, як: 1) вчинення повторно; 2) вчинення за попередньою змовою групою осіб або 3) якщо ті саме дії заподіяли значну шкоду. Так, наприклад, 31.05.2016 р. Вижницьким районним судом Чернівецької області ОСОБА_1 визнано винним у вчиненні злочину, передбаченого ч. 2 ст. 361 КК України, як несанкціоноване втручання в роботу мереж електрозв'язку, що призвело до спотворення процесу обробки інформації та до порушення встановленого порядку її маршрутизації, вчинене повторно. Суд визнав наявність повторності вчинення діяння, оскільки винним протягом 23 — 27.07.2015 р. здійснювалося неодноразове несанкціоноване втручання в роботу мереж електрозв'язку з різних номерів до різних країн світу [21]. На відміну від наведеної судової позиції Галицький районний суд м. Львова у своєму вироку від 29.06.2017 р. не погодився з кваліфікацією дій підсудного ОСОБА_3 за ч. 2 ст. 361 КК України і констатував, що дії винного слід кваліфікувати за ч. 1 ст. 361 КК України, як несанкціоноване втручання в роботу комп'ютерних мереж електрозв'язку та в порушенні встановленого порядку маршрутизації міжнародного трафіку, оскільки дії ОСОБА_3 носили характер продовжуваного злочину, який складається з двох або більше тотожних діянь об'єднаних єдиним злочинним умислом, що свідчить про відсутність ознак повторності [22]. Наведені вище приклади з правозастосовної практики свідчать про неоднозначність трактування судами змісту такої кваліфікуючої ознаки злочину, передбаченого ст. 361 КК України, як повторність при вчиненні злочинного діяння через рефайлінг.

Звернемося до іноземного досвіду кваліфікації аналізованих нами дій. Так, наприклад, у Російській Федерації (далі — РФ), де рефайлінг є досить

поширеним, вказані дії часто визнаються незаконною підприємницькою діяльністю (ст. 171 КК РФ) [23], при цьому робиться акцент не на втручанні в роботу комп'ютерних мереж та мереж електрозв'язку, а на діяльність, що здійснюється без відповідної ліцензії. На нашу думку, такий підхід є хибним, оскільки в КК РФ існує аналог ст. 361 КК України — ст. 272 «Незаконний доступ до комп'ютерної інформації», в ч. 2 якої передбачено таку кваліфікуючу ознаку, як «вчинення злочину з корисливих мотивів». Скоріш за все неоднозначність підходів у кваліфікації злочинів зумовлена відсутністю в ст. 272 КК РФ прямої вказівки на такий вид наслідку, як «спотворення процесу обробки інформації». В іншому випадку у ст. 213 «Неправомірні зміна ідентифікаційного коду абонентського пристрою стільникового зв'язку, пристрою ідентифікації абонента, а також створення, використання, поширення програм для зміни ідентифікаційного коду абонентського пристрою» КК Республіки Казахстан, яка міститься у самостійній главі 7 «Кримінальні правопорушення у сфері інформатизації і зв'язку» Особливої частини, передбачена відповідальність за: 1) зміну ідентифікаційного коду абонентського пристрою стільникового зв'язку, створення дубліката картки ідентифікації абонента стільникового зв'язку, якщо ці дії вчинені без згоди виробника або законного власника; 2) неправомірні створення, використання, поширення програм, що дозволяють змінювати ідентифікаційний код абонентського пристрою стільникового зв'язку або створювати дублікат карти ідентифікації абонента стільникового зв'язку [24].

Глава 31 Закону про мобільні телефони (перепрограмування) 2002 р. Великої Британії передбачає, що за незаконну зміну IMEI-коду пристрою стільникового зв'язку передбачено до п'яти років тюремного ув'язнення [25]. Тоді як за КК Республіки Білорусь дії щодо зміни ідентифікаційного коду абонентського пристрою кваліфікують за ст. 350 «Модифікація комп'ютерної інформації», якою встановлено відповідальність за зміну інформації, що зберігається в комп'ютерній системі, мережі чи на машинних носіях, або внесення завідомо неправдивої інформації, що заподіяла значну шкоду, до чого також відносять і зміну IMEI-коду пристроїв [26].

На наш погляд, окремі приклади зарубіжного досвіду є позитивними та потребують подальшої ґрунтовної розробки задля удосконалення положень чинного законодавства України. Так, на сьогодні Правила надання та отримання телекомунікаційних послуг встановлюють обов'язок споживачів не фальсифікувати мережеві ідентифікатори, не використовувати неіснуючі мережеві ідентифікатори або такі, що належать іншим особам, не здійснювати підробку (дублювання) ідентифікаційних карток, електронного коду (ідентифікатора) кінцевого обладнання (підпункт 13 п. 36) [4]. Проте ці Правила не містять прямої вказівки на характер протиправності таких дій. Звідси вважаємо за необхідне внести зміни, зокрема, до п. 3 цих Правил, доповнивши перелік дій, які становлять «несанкціоноване втручання в роботу та/або використання телекомунікаційних мереж», вказівкою на «несанкціоновану зміну електронного коду (ідентифікатора) кінцевого обладнання». Це дозволить розглядати зміну IMEI-коду як несанкціоноване втручання в роботу телекомунікаційних мереж не тільки як складову рефайлінгу, але і як самостійні завершені дії, що

нерідко вчиняються з метою унеможливлення відстеження правоохоронними органами викрадених пристроїв, обладнаних IMEI-кодами (мобільні телефони, планшети, модеми, і т.д.). Поряд із цим слід покласти на НКРЗ повноваження щодо ведення єдиного реєстру ідентифікаторів кінцевого обладнання, внісши зміни до Закону України «Про радіочастотний ресурс України», де ст. 14 доповнити пунктом щодо встановлення порядку та ведення єдиного реєстру міжнародних ідентифікаторів кінцевого обладнання.

Викладені пропозиції, на нашу думку, повинні усунути недоліки внесених постановою КМУ від 20.09.2017 р. № 703 змін до Правил надання та отримання телекомунікаційних послуг, а також зменшити кількість випадків несанкціонованої зміни міжнародних ідентифікаторів кінцевого обладнання, що повинно полегшити працівникам правоохоронних органів діяльність щодо виявлення рефайлінгового обладнання, а також викрадених мобільних телефонів та інших девайсів.

Також в багатьох країнах світу сьогодні запроваджена обов'язкова реєстрація абонентів мобільного зв'язку (зокрема, в Німеччині, Польщі, Франції та Бельгії), а відтак сім-карту мобільного оператора не можливо придбати без паспорту. В 2013 р. об'єднання мобільних операторів та інших компаній мобільного зв'язку Groupe Speciale Mobile Association (GSMA) встановило, що концепція ідентифікації абонентів в першу чергу впроваджується правоохоронними органами для боротьби з тероризмом та полегшення виявлення злочинів, проте вона не завжди допомагає виявити чи розкрити злочин [27, p. 17]. Натомість зазначена концепція вписується в умови запровадження в Україні системи «mobile ID», правову основу для якої склав Закон України «Про електронні довірчі послуги» від 05.10.2017 р. № 2155-VIII (набрання чинності відбудеться 07.11.2018 р.) [28]. Зазначена система дозволить використовувати сім-карту мобільного оператора як документ, що підтверджує особу, її потрібно буде зареєструвати за допомогою паспорта на своє ім'я, після чого на неї буде записано електронний цифровий підпис, який дозволить отримувати адміністративні послуги та підписувати документи прямо зі свого смартфону чи іншого пристрою. При цьому гарантом справжності процедури ідентифікації виступатиме мобільний оператор, у якого будуть міститися копії документів, що підтверджують особу відповідного абонента. До речі, в наш час, для повноцінного функціонування «mobile ID» вже створюється відповідна інфраструктура. Зокрема, вона успішно використовується частиною абонентів кількох операторів мобільного зв'язку в тестовому режимі. Тому найближчим часом можемо спостерігати ситуацію, за якої значна частина абонентів реєструватиме свої номера абсолютно добровільно.

З урахуванням позитивного іноземного досвіду та сучасних тенденцій в національному інформаційному середовищі не виключаємо можливості запропонувати доповнити ст. 18 Закону України «Про телекомунікації» положенням про обов'язкову реєстрацію абонентів, які отримують телекомунікаційні послуги без укладення договору в письмовій формі, поклавши на НКРЗ обов'язок проводити реєстрацію абонентів мобільного зв'язку. Це дозволить суттєво зменшити неконтрольовану кількість анонімних мобільних номерів

(сім-карток), які дуже часто використовуються в цілях рефайлінгу. Крім того, у зв'язку із збільшенням кількості зареєстрованих працівниками правоохоронних органів випадків рефайлінгу, потрібно чітко визначити механізм скоєння цього злочину та своєчасно запобігати його вчиненню. Для цього, на нашу думку, варто розробити комплексні методичні рекомендації для правоохоронців, які протидіють кіберзлочинам (зокрема, працівників Національної поліції).

Висновки. Підсумовуючи викладене, слід наголосити під «рефайлінгом (рефайлом)» слід розуміти незаконну підміну телефонного трафіку, а точніше — зміну виду трафіку з метою отримання максимального прибутку за рахунок його маршрутизації за іншою розрахунковою таксою. Специфіка рефайлінгу полягає в тому, що він є способом вчинення несанкціонованого втручання в роботу мереж електрозв'язку (телекомунікаційних мереж), при цьому йому властиві система складних прийомів, методів, рухів, схем, зв'язків тощо (зокрема, побудова власної автоматичної телефонної станції), а також корислива мотивація. Типовий рефайлер (той, хто здійснює рефайлінг) — це чоловік, який прагне незаконно збагатитися, не є телекомунікаційним оператором, не має права на технічне обслуговування та експлуатацію телекомунікаційних мереж, надання в користування каналів зв'язку, встановлення та налагодження програмно-апаратних комплексів, не має відповідної ліцензії, виданої НКРЗ, діє на порушення вимог відповідних нормативно-правових актів тощо.

На сьогодні некримінальне законодавство дає чітке уявлення про те, що собою становить такий спосіб несанкціонованого втручання в роботу мереж електрозв'язку (телекомунікаційних мереж), як рефайлінг, а тому, заради уникнення переобтяження положень КК України, не вбачаємо за доцільне виділяти його в якості основної чи кваліфікуючої ознаки складу злочину, передбаченого ст. 361 КК України. Натомість пропонуємо, у т.ч. з урахуванням позитивного зарубіжного досвіду, здійснити «точкові» зміни задля запобігання та протидії рефайлінгу в Україні, зокрема: а) у Правилах надання та отримання телекомунікаційних послуг зробити вказати на «несанкціоновану зміну електронного коду (ідентифікатора) кінцевого обладнання», що вважатиметься несанкціонованим втручанням у роботу та/або використання телекомунікаційних мереж; б) на НКРЗ слід покласти повноваження щодо ведення єдиного реєстру ідентифікаторів кінцевого обладнання, внісши зміни до Закону України «Про радіочастотний ресурс України», де ст. 14 доповнити пунктом щодо встановлення порядку та ведення єдиного реєстру міжнародних ідентифікаторів кінцевого обладнання; в) підняти питання про обов'язкову реєстрацію абонентів мобільного зв'язку; г) розробити комплексні методичні рекомендації для правоохоронців, які протидіють рефайлінгу та іншим проявам кіберзлочинів (зокрема, працівників Національної поліції).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Аваков Арсен* Кіберполіція (крок реформі) : 11 жовтня 2015 року / Арсен Аваков [Електронний ресурс]. — Режим доступу : http://blogs.pravda.com.ua/authors/avakov/561a92c183c27/.

2. *La Rue Frank* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression / Frank La Rue / Seventeenth session. Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development / UN General Assembly / A/HRC/17/27. — 22 p.

3. Top 50 Countries by Smartphone Users and Penetration / Newzoo [Електронний ресурс]. — Режим доступу : https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.

4. Про затвердження Правил надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів України від 11 квітня 2012 року № 295 [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/295-2012-п.

5. Про ліцензування видів господарської діяльності : Закон України від 2 березня 2018 року № 222-VIII [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/222-19.

6. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV [Електронний ресурс]. — Режим доступу :http://zakon3.rada.gov.ua/laws/show/1280-15.

7. *Горбачевский Сергей* О рефайле, ip-телефонии и фроде / Сергей Горбачевский [Електронний ресурс]. — Режим доступу : https://www.g-news.com.ua/news/9-it/-/6343-ip.html.

8. Мобільні шахраї: як обкрадають стільникових операторів [Електронний ресурс]. — Режим доступу : http://forbes.net.ua/ua/business/1427285-mobilni-shahrayi-yak-obkradayut-stilnikovih-operatoriv.

9. Про радіочастотний ресурс України : Закон України від 1 червня 2000 року № 1770-II [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/1770-14.

10. Про затвердження Порядку маршрутизації трафіка в телекомунікаційній мережі загального користування України : Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, від 5 липня 2012 року № 324 [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/z1252-12.

11. Про затвердження Основних вимог до договору про надання телекомунікаційних послуг та визнання таким, що втратило чинність, рішення НКРЗ від 26.03.2009 № 1420 : Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, від 29 листопада 2012 року № 624 [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/z2150-12.

12. Про внесення змін до Правил надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів України від 20 вересня 2017 року № 703 [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/703-2017-%D0%BF.

13. Справа 465/1205/17 (1-кп/465/458/17) // Архів Франківського районного суду м. Львова.

14. Справа № 591/5282/17 // Архів Зарічного районного суду м. Суми.

15. Науково-практичний коментар Кримінального кодексу України / Д.С. Азаров, В.К. Грищук, А.В. Савченко [та ін.] ; за заг. ред. О.М. Джужі, А.В. Савченка, В.В. Чернєя. — К. : Юрінком Інтер, 2016. — 1064 с.

16. Конституція України від 28 червня 1996 року (у редакції від 30 вересня 2016 року) [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

17. Руководство пользователя по работе с сервисом GoAntiFraud [Електронний ресурс]. — Режим доступу : https://goantifraud.com/files/manualRu.pdf/.

18. *Висоцька В.В.* Поняття способу вчинення злочину / В.В. Висоцька // Правова держава. — № 13. — 2011. — С. 102—105.

19. *Панов Н.И.* Способ совершения преступления и уголовная ответственность. — Харьков : Вища школа, 1982. — 160 с.

20. Справа № 643/2730/16-к // Архів Московського районного суду м. Харкова.

21. Справа № 713/331/16-к // Архів Вижницького районного суду Чернівецької області.

22. Справа № 1-26/11 // Архів Галицького районного суду м. Львова.

23. Уголовный кодекс РФ 2017 (актуальная редакция с комментариями по состоянию на 05.02.2018) [Електронний ресурс]. — Режим доступу : http://ukodeksrf.ru/ch-2/rzd-8/gl-22/st-171-uk-rf.

24. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-IV (с изменениями и дополнениями по состоянию на 11 июля 2017 года) [Електронний ресурс]. — Режим доступу : https://online.zakon.kz/Document/?doc_id=31575252#pos=2430;-99.

25. Mobile Telephones (Re-programming) Act 2002 [Електронний ресурс]. — Режим доступу : https://www.legislation.gov.uk/ukpga/2002/31/introduction.

26. IMEI-номера. Изменение идентификационных IMEI-номеров телефонов // Управление внутренних дел Брестского облисполкома [Електронний ресурс]. — Режим доступу : http://uvd.brest.gov.by/struktura-ovd/180/2807/.

27. The Mandatory Registration of Prepaid SIM Card Users / A White paper — November 2013 // GSMA 2013. — 31 p.

28. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 року № 2155-VIII [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/2155-19.

REFERENCES

1. *Avakov Arsen* Kiberpolitsiya (krok reformi) : 11 zhovtnya 2015 roku / Arsen Avakov [Elektronnyy resurs]. — Rezhym dostupu : http://blogs.pravda.com.ua/authors/avakov/561a92c183c27/.

2. *La Rue Frank* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression / Frank La Rue / Seventeenth session. Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development / UN General Assembly / A/HRC/17/27. — 22 p.

3. Top 50 Countries by Smartphone Users and Penetration / Newzoo [Elektronnyy resurs]. — Rezhym dostupu : https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.

4. Pro zatverdzhennya Pravyl nadannya ta otrymannya telekomunikatsiynykh posluh : Postanova Kabinetu Ministriv Ukrayiny vid 11 kvitnya 2012 roku № 295 [Elektronnyy resurs]. — Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/295-2012-p.

5. Pro litsenzuvannya vydiv hospodarskoyi diyalnosti : Zakon Ukrayiny vid 2 bereznya 2018 roku № 222-VIII [Elektronnyy resurs]. — Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/222-19.

6. Pro telekomunikatsiyi : Zakon Ukrayiny vid 18 lystopada 2003 roku № 1280-IV [Elektronnyy resurs]. — Rezhym dostupu : http://zakon3.rada.gov.ua/laws/show/1280-15.

7. *Horbachevskyy Serhey* O refayle, ip-telefonyy i frode / Serhey Horbachevskyy [Elektronnyy resurs]. — Rezhym dostupu : https://www.g-news.com.ua/news/9-it/ /6343-ip.html.

8. Mobilni shakhrayi: yak obkradayut stilnykovykh operatoriv [Elektronnyy resurs]. — Rezhym dostupu : http://forbes.net.ua/ua/business/1427285-mobilni-shahrayi-yak-obkradayut-stilnikovih-operatoriv.

9. Pro radiochastotnyy resurs Ukrayiny : Zakon Ukrayiny vid 1 chervnya 2000 roku № 1770-II [Elektronnyy resurs]. — Rezhym dostupu : http://zakon3.rada.gov.ua/laws/show/1770-14.

10. Pro zatverdzhennya Poryadku marshrutyzatsiyi trafika v telekomunikatsiyniy merezhi zahalnoho korystuvannya Ukrayiny : Rishennya Natsionalnoyi komisiyi, shcho zdiysnyuye derzhavne rehulyuvannya u sferi zvyazku ta informatyzatsiyi, vid 5 lypnya 2012 roku № 324 [Elektronnyy resurs]. — Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/z1252-12.

11. Pro zatverdzhennya Osnovnykh vymoh do dohovoru pro nadannya telekomunikatsiynykh posluh ta vyznannya takym, shcho vtratylo chynnist, rishennya NKRZ vid 26.03.2009 № 1420 : Rishennya Natsionalnoyi komisiyi, shcho zdiysnyuye derzhavne rehulyuvannya u sferi zvyazku ta informatyzatsiyi, vid 29 lystopada 2012 roku № 624 [Elektronnyy resurs]. — Rezhym dostupu :http://zakon3.rada.gov.ua/laws/show/z2150-12/.

12. Pro vnesennya zmin do Pravyl nadannya ta otrymannya telekomunikatsiynykh posluh : Postanova Kabinetu Ministriv Ukrayiny vid 20 veresnya 2017 roku № 703 [Elektronnyy resurs]. — Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/703-2017-%D0%BF.

13. Sprava 465/1205/17 (1-kp/465/458/17) // Arkhiv Frankivskoho rayonnoho sudu m. Lvova.

14. Sprava № 591/5282/17 // Arkhiv Zarichnoho rayonnoho sudu m. Sumy.

15. Naukovo-praktychnyy komentar Kryminalnoho kodeksu Ukrayiny / D.S. Azarov, V.K. Hryshchuk, A.V. Savchenko [ta in.] ; za zah. red. O.M. Dzhuzhi, A.V. Savchenka, V.V. Chernyeya. — K. : Yurinkom Inter, 2016. — 1064 s.

16. Konstytutsiya Ukrayiny vid 28 chervnya 1996 roku (u redaktsiyi vid 30 veresnya 2016 roku) [Elektronnyy resurs]. — Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

17. Rukovodstvo polzovatelya po rabote s servysom GoAntiFraud [Elektronnyy resurs]. — Rezhym dostupu : https://goantifraud.com/files/manualRu.pdf/.

18. Vysotska V.V. Ponyattya sposobu vchynennya zlochynu / V.V. Vysotska // Pravova derzhava. — № 13. — 2011. — S. 102—105.

19. Panov N. I. Sposob sovershenyya prestuplenyya y uholovnaya otvetstvennost. — Kharkov : Vyshcha shkola, 1982. — 160 s.

20. Sprava № 643/2730/16-k // Arkhiv Moskovskoho rayonnoho sudu m. Kharkova.

21. Sprava № 713/331/16-k // Arkhiv Vyzhnytskoho rayonnoho sudu Chernivetskoyi oblasti.

22. Sprava № 1-26/11 // Arkhiv Halytskoho rayonnoho sudu m. Lvova.

23. Uholovnyi kodeks RF 2017 (aktualnaya redaktsiya s kommentariyami po sostoyaniyu na 05.02.2018) [Elektronnyy resurs]. — Rezhym dostupu : http://ukodeksrf.ru/ch-2/rzd-8/gl-22/st-171-uk-rf.

24. Uholovnyi kodeks Respubliki Kazakhstan ot 3 iyulya 2014 hoda № 226-IV (s izmeneniyamy i dopolneniyamy po sostoyaniyu na 11 iyulya 2017 hoda) [Elektronnyy resurs]. — Rezhym dostupu : https://online.zakon.kz/Document/?doc_id=31575252-#pos=2430;-99.

25. Mobile Telephones (Re-programming) Act 2002 [Elektronnyy resurs]. — Rezhym dostupu : https://www.legislation.gov.uk/ukpga/2002/31/introduction.

26. IMEI-nomera. Izmenenie identifikatsionnykh IMEI-nomerov telefonov // Upravlenie vnutrennikh del Brestskoho oblispolkoma [Elektronnyy resurs]. — Rezhym dostupu : http://uvd.brest.gov.by/struktura-ovd/180/2807/.

27. The Mandatory Registration of Prepaid SIM Card Users / A White paper — November 2013 // GSMA 2013. — 31 p.

28. Pro elektronni dovirchi posluhy : Zakon Ukrayiny vid 5 zhovtnya 2017 roku № 2155-VIII [Elektronnyy resurs]. — Rezhym dostupu : http://zakon3.rada.gov.ua/laws/show/2155-19.

Савченко А.В., Воробей П.А., Бельський Ю.А. Рефайлінг (рефайл) як спосіб вчинення несанкціонованого втручання в роботу мереж електрозв'язку

У статті розкрита сутність рефайлінгу (рефайлу) як способу вчинення несанкціонованого втручання в роботу мереж електрозв'язку (телекомунікаційних мереж). Визначено специфіку механізму рефайлінгу та наголошено, що йому властива система складних прийомів, методів, рухів, схем, зв'язків тощо (зокрема, побудова власної автоматичної телефонної станції), а також корислива мотивація. Проаналізовано низку положень вітчизняного та зарубіжного законодавства, акцентовано увагу на питаннях кваліфікації судами України кіберзлочинів, що вчиняються через рефайлінг. Запропоновано зміни та доповнення до чинних нормативно-правових актів України задля посилення запобігання та протидії рефайлінгу.

Ключові слова: *рефайлінг (рефайл), спосіб вчинення злочину, несанкціоноване втручання, мережі електрозв'язку, телекомунікаційні мережі, підміна телефонного трафіку, телекомунікаційні послуги.*

Савченко А.В., Воробей П.А., Бельский Ю.А. Рефайлинг (рефайл) как способ совершения несанкционированного вмешательства в работу сетей электросвязи

В статье раскрыта сущность рефайлинга (рефайла) как способа совершения несанкционированного вмешательства в работу сетей электросвязи (телекоммуникационных сетей). Определено специфику механизма рефайлинга и отмечено, что ему свойственна система сложных приемов, методов, движений, схем, связей и т.п. (в частности, построение собственной автоматической телефонной станции), а также корыстная мотивация. Проанализирован ряд положений отечественного и зарубежного законодательства, акцентировано внимание на вопросах квалификации судами Украины киберпреступлений, совершаемых через рефайлинг. Предложены изменения и дополнения в действующие нормативно-правовые акты Украины для усиления предотвращения и противодействия рефайлингу.

Ключевые слова: *рефайлинг (рефайл), способ совершения преступления, несанкционированное вмешательство, сети электросвязи, телекоммуникационные сети, подмена телефонного трафика, телекоммуникационные услуги.*

Savchenko A., Vorobei P., Belskyi Yu. Refiling (refile) as a Method of Committing of Unauthorized Interference in the Work of Telecommunication Networks

The article reveals the essence of refiling (refile) as a method of committing unauthorized interference in the work of telecommunication networks (electrical connection networks). The specificity of the refiling mechanism is determined and it is noted that among its inherent features are the presence of a system of complex dodges, modes, movements, schemes, connections, etc. (in particular, the construction of its own automatic telephone exchange), as well as selfish motivation. A number of provisions of the domestic and foreign legislation are analyzed; attention is focused on questions of qualification of cybercrime by the courts of Ukraine, which are carried out through refiling. The amendments and additions to the current normative legal acts of Ukraine are proposed to strengthen the prevention and counteraction of refiling.

Keywords: *Refiling (Refile), Method of Committing a Crime, Unauthorized Interference, Telecommunication Networks, Electrical Connection Networks, Substitution of Telephone Traffic, Telecommunication Services*

Стаття надійшла до редакції: 11.12. 2017.