УДК 343.97: 343.72

ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ РЕФАЙЛІНГУ В УКРАЇНІ

PROBLEM BREEDS OF COUNTERING REFILLING UKRAINE

Брисковська О.М.,
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник
наукової лабораторії з проблем досудового розслідування
Національної академії внутрішніх справ

Алєксєєва-Процюк Д.О.,
кандидат історичних наук, старший науковий співробітник,
провідний науковий співробітник
наукової лабораторії з проблем досудового розслідування
Національної академії внутрішніх справ

У статті встановлені основні причини розвитку рефайлінгу в Україні. Охарактеризовано особливості вчинення такого злочину. Сформульовано визначення рефайлінгу. Окреслено проблемні питання з протидії рефайлінгу та надано пропозиції щодо їх вирішення.
Ключові слова: рефайлінг, нелегальна термінація трафіку, маршрутизація міжнародного трафіку, оператори мобільного зв'язку, телеком-компанії, кіберполіція, фрод, мобільні дзвінки, шахрайство, протидія.

В статье установлены основные причины развития рефайлинга в Украине. Охарактеризованы особенности совершения такого преступления. Сформулировано определение рефайлинга. Определены проблемные вопросы по противодействию рефайлингу и представлены предложения по их решению.
Ключевые слова: рефайлинг, нелегальная терминация трафика, маршрутизация международного трафика, операторы мобильной связи, телеком-компании, киберполиция, фрод, мобильные звонки, мошенничество, противодействие.

The article identifies the main reasons for the development of refining in Ukraine. Characterized by the peculiarities of such a crime, the definition of refilling is formulated. Problematic issues of counteraction to refilling are outlined and suggestions for their solution are given.
Key words: refilling, illegal traffic termination, international traffic routing, mobile operators, telecom companies, cyberpolice, frod, mobile calls, fraud, counteraction.

Постановка проблеми. Нелегальна термінація трафіку стала однією з основних проблем будь-якого телекомунікаційного оператора. Через рефайлінг щорічно втрачається 20% прибутку телефонних компаній. Це завдає державі багатомільйонних збитків, оскільки податки з таких доходів шахрайські телеком-фірми не сплачують. Проблема такого шахрайства є загальносвітовою, тому випадки порушення маршрутизації трафіку виявлялися у різних напрямках на різних континентах Землі. Натепер найбільше потерпають оператори в тих країнах, де міжнародний зв'язок коштує значно дорожче, ніж локальний трафік. У топ держав, де найбільше вчиняється такий вид шахрайства, входять країни Африки, Балканського півострова, країни СНД [1]. Досі цей злочинний бізнес комфортно себе почуває і в Україні.

Рефайлінг – це підміна міжнародного трафіку на локальний шляхом перенаправлення VoIP дзвінка з-за кордону в місцеву GSM мережу. VoIP (Voice over Internet Protocol) – це технологія, яка забезпечує передачу голосу в мережах з пакетною комутацією по протоколу IP, окремим різновидом яких є мережа Інтернет, а також інші мережі IP (наприклад, виділені цифрові канали). Для зв'язку мережі Інтернет (мережі IP) з телефонною мережею загального користування PSTN (Public Switched Telephone Network), яка належить до глобальних мереж з комутацією каналів, використовуються спеціальні аналогові VoIP-шлюзи [13]. Виклик тарифікується як місцевий, а на різниці у вартості шахраї заробляють. Напрямок такого злочинного бізнесу, що заснований на застосуванні технології рефайлінгу, більше відомий як термінація VoIP трафіку [2]. Рефайл – це шахрайство з підміни міжнародних дзвінків псевдонаціональними.

Мета статті – встановити основні причини розвитку рефайлінгу в Україні, охарактеризувати особливості його вчинення, окреслити проблемні питання щодо його протидії в Україні та запропонувати пропозиції щодо їх вирішення.

Виклад основного матеріалу. Згідно із ч. 1 ст. 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 [3]. Відповідно до п.п. 3.10, 3.11 Порядку маршрутизації трафіку в телекомунікаційній мережі загального користування України, затвердженого рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 05.07.2012 № 324, маршрутизація міжнародного трафіку голосової телефонії повинна здійснюватися лише через міжнародний центр комунікації (далі – МЦК). Маршрутизація міжнародного трафіку з використанням технології комутації пакетів повинна здійснюватися до мереж з комутацією каналів через МЦК з функціями медіашлюзу. Маршрутизація вхідного міжнародного трафіку голосової телефонії здійснюється операторами від станцій комутації вищого ієрархічного рівня до станцій того самого або нижчого ієрархічного рівня без переходів трафіку голосової телефонії з нижчих ієрархічних рівнів на вищі у кожному з маршрутів [4]. Направлення міжнародного трафіку голосової телефонії від телекомунікаційного обладнання абонентів мережі рухомого (мобільного) зв'язку оператора, яким надані телефонні номери на телекомунікаційну мережу загального користування, здійснюються поза МЦК. Унаслідок цього оператори втрачають кошти, адже тарифікація за надані послуги здійснюється не як за надані послуги міжнародного зв'язку, а як дзвінки в межах абонентів оператора [5]. За таке правопорушення передбачена відповідальність згідно зі ст. 361 Кримінального кодексу України («Несанкціоноване втручання у 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») [6]. Попри ці законодавчі вимоги, злочинці для одержання неправомірної вигоди втручаються у роботу мереж операторів, чим завдають значної шкоди [5].

Незважаючи на те, що рефайлінг в Україні інтенсивно розвивався з 2000 р., питання протидії такому виду злочину на монографічному рівні вітчизняними науковцями не розглядалося.

На нашу думку, рефайлінг – це міжнародне шахрайство термінації трафіку (термінація трафіку – це встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіку між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання [14]) для отримання грошей за послуги мобільного зв'язку шляхом маршрутизації міжнародних дзвінків поза офіційними каналами (по каналах зв'язку місцевої мережі) для незаконного здешевлення. Розглянемо основні причини розвитку такого злочинного бізнесу в Україні:

1) незначні затрати за високого та стабільного доходу. Прибуток від рефайлінгу сягає близько $ 2 000 на місяць, беручи до уваги те, що в середньому такий бізнес окупається через 2–6 місяців. Цьому сприяють такі умови [7]:

– високі ставки термінації міжнародного трафіку;

– зростання курсу іноземних валют щодо національної;

– низька ціна стартових пакетів;

– доступна ціна СІМ-бокс обладнання;

2) наявність та можливість безперешкодного придбання обладнання та програмного забезпечення;

3) відсутність ідентифікації припейд-клієнтів;

4) недостатня взаємодія мобільних операторів з правоохоронними органами (небажання розкривати масштаби збитків через страх зашкодити репутації компанії);

5) дороговартісна і важка боротьба з нелегальною термінацією трафіку (навчання співробітників новим технологіям, закупівля та впровадження сучасних систем з виявлення шахраїв).

Отже, окреслимо нагальні проблеми протидії рефайлінгу в Україні:

1) недостатньо узгоджений обмін інформацією з правоохоронними органами телефонних компаній;

2) недостатній кваліфікаційний розподіл у кіберполіції щодо протидії сучасним видам злочинів у кіберпросторі (наприклад, створення окремого напрямку з протидії рефайлінгу з відповідними спеціалістами);

3) відсутність належного досвіду та практичних навичок у більшості працівників кіберполіції;

4) відшкодування шкоди операторам внаслідок рефайлінгу потребує доведення відповідно до п. 3 оглядового листа Вищого господарського суду України від 14.01.2014 року № 01-06/20/2014. Пред'явлення вимоги про відшкодування неодержаних доходів (втраченої вигоди) покладає на кредитора обов'язок довести, що ці доходи (вигода) не є абстрактними, а дійсно були б ним отримані в разі здійснення певної діяльності. Позивач повинен довести також, що він міг і повинен був отримати визначені доходи, але тільки неправомірні дії відповідача стали єдиною і достатньою причиною, яка позбавила його можливості отримати прибуток. Отже, саме на оператора покладається обов'язок довести розмір та реальність можливості отримати доходи [5];

5) неналежний рівень фінансування напрямку боротьби з кіберзлочинами, тому обдарована молодь вважає соціально непривабливою працю у цій сфері.

Кілька років тому цим видом фроду (фрод – вид шахрайства в галузі інформаційних технологій, несанкціоновані дії і неправомірне користування ресурсами і послугами в мережах зв'язку[15]) могли займатися тільки люди з відповідною технічною освітою. У 2011 р. в Чернігівській області затримали ОСОБУ_1, яка з 2008 р. попередньо зорганізувала трьох осіб з технічною освітою для вчинення несанкціонованого втручання у роботу мереж електрозв'язку, зокрема для створення та налаштування програмно-технічного обладнання, за допомогою якого можна несанкціоновано здійснювати перенаправлення голосового трафіку з мережі Інтернет у мережу GSM. Маючи спеціальні знання у сфері інформаційних технологій, зловмисники між собою розподілили функції та завдання: ОСОБА_1 мала займатися білінгом, орендою квартир, пошуком підприємств, на яких можна було б виготовити запчастини для обладнання, ОСОБА_2 – налагодженням програмно-технічних засобів, збіркою обладнання, а ОСОБА_3 – розробкою запчастин для обладнання, адмініструванням системи. Протягом січня – листопада 2009 р. вони виготовили та налаштували програмно-технічне обладнання для GSM рефайлу, тобто для перенаправлення вхідного міжнародного телефонного трафіку з мережі Інтернет у мережу GSM операторів мобільного зв'язку України. Вказане обладнання виконувало функції GSM-шлюзу та шлюзу IP-телефонії. Протягом 2009–2010 р. це обладнання приймало телефонний трафік (міжнародні вхідні дзвінки) через програмний IPPBX-шлюз IP-телефонії, проводило комутацію цього трафіку в мережу операторів мобільного зв'язку через GSM-шлюз, виконуючи функції термінації трафіку IP-телефонії на мережу операторів мобільного зв'язку. Для підміни номерів використовувались номери сім-карт операторів мобільного зв'язку України, зокрема ТОВ «Астеліт» [8].

Якщо кілька років тому цим видом фроду могли займатися тільки люди з відповідною технічною освітою, то сьогодні такий бізнес можна просто купити з необхідними інструкціями щодо його налаштування. В Інтернеті є безліч пропозицій за прийнятну плату продати необхідне обладнання, встановити спеціалізоване програмне забезпечення для імітації людської активності, звести з оригінаторами трафіку [1], надавати цілодобову технічну підтримку та поради щодо безпечних місць розміщення такого обладнання, навчання, щодо особливостей його налаштування для ускладнення операторам виявлення і блокування сім-карти шахрая. Тому шахраям, щоб почати таку роботу, достатньо, крім обладнання, придбати сім-карти і забезпечити їм захист від блокування антифрод-системами для імітування поведінки реального абонента в мережах GSM. Для цього існують різні програмні рішення, що дозволяють імітувати поведінку реального абонента в мережах GSM. Щоб розмістити шлюзи у певній країні, шахраї орендують приміщення, підключають швидкісний Інтернет, знаходять компанію-оригінатора, яка буде надавати трафік для термінації, і втілюють свій злочинний задум [9]. Наприклад, у Івано-Франківську викрили приватну фірму, яка за допомогою особи, яка живе за кордоном нашої держави, займалася рефайлінгом. Ця фірма купувала дешевий трафік і налагоджувала зв'язок через Інтернет, який дозволяв перетворювати аналоговий сигнал на цифровий і знову на аналоговий, завершуючи міжнародні зв'язки в українських мережах під виглядом місцевого трафіку всередині країни. Застосовувалися модеми та маршрутизатори. Обладнання, за допомогою якого здійснювалася незаконна діяльність, спеціалісти сектору кіберзлочинів знайшли і вилучили у Івано-Франківську [9].

У 2016 р. на Вінниччині викрили 33-річного киянина-гастролера, який півроку їздив країною з міні-АТС (це ноутбук зі спеціальною програмою та модемами для підключення карток мобільного оператора на прийом дзвінків). У нього було активовано 30 телефонних карток, основним завданням було бути постійно на зв'язку, за це він отримував кількасот доларів на місяць. Хакера, який запропонував йому цей заробіток, він не знає, списався з ним по Інтернету. Цей хакер керував процесом телефонних розмов через програму віддаленого доступу до його техніки [10].

Сьогодні згідно з рішенням Національної комісії регулювання зв'язку та інформатизації ставка інтерконекту за вхідні в Україну дзвінки з 1 січня 2017 р. становить 10 центів / хв, а раніше вона становила 20 центів / хв мо-

більних дзвінків в Україну з-за кордону. Це дещо знизило прибуток від крадіжки трафіку у мобільних операторів та зменшило інтерес до такого бізнесу. Але на сірому ринку термінація дзвінка на українські мережі коштує 6–8 американських центів за хвилину, а офіційна регульована ставка тепер – 10 євроцентів. У шахраїв, які займається рефайлом, витрати на хвилину рівні вартості дзвінка для абонента всередині мережі українського оператора зв'язку. Припустімо, вартість пакета з необмеженим обсягом хвилин коштує 100 грн, цей пакет працює 12 годин на добу. Вартість хвилини становитиме 0,005 грн / хв. З урахуванням вартості обладнання і електроенергії витрати особи, що займається рефайлом, не перевищуватимуть 1 американський цент за хвилину [9].

А тому, поки ставка за термінацію міжнародного трафіку не наблизиться до розміру середнього абонентського тарифу, займатися ефайлінгом буде вигідно з економічного погляду.

Такому шахрайству доцільно протидіяти різними доступними методами. Сьогодні у світовій практиці застосовуються **два основних види систем виявлення цього виду шахрайства:** через так звані *активні системи,* що виявляють фродові номери, здійснюючи сесії тестових викликів (продзвонів) з різних частин світу на номери оператора, та *пасивні системи,* що відрізняють фродові карти від живих абонентів (такі системи проводять аналіз активності абонентів на предмет «людяності») [1].

Наприклад, у період з січня 2014 року на телекомунікаційній мережі загального користування м. Запоріжжя та Запорізької області невстановленими особами здійснювалося незаконне завершення міжнародного телефонного трафіку під виглядом національного з'єднання з використанням телефонних номерів оператора мобільного зв'язку ТОВ «Астеліт», (НОМЕР_1, НОМЕР_2, НОМЕР_3, НОМЕР_4, НОМЕР_5, НОМЕР_6, НОМЕР_7, НОМЕР_8, НОМЕР_9, НОМЕР_10, НОМЕР_11, НОМЕР_12), які за низкою ознак ідентифікувались як підмінні номери, які були підставлені замість оригінального номеру абонента «А». Під час деталізації дзвінків було встановлено, що з вказаних номерів здійснюються тільки вихідні дзвінки по всій Україні, вхідні дзвінки відсутні взагалі. Також за допомогою спеціального обладнання було встановлено, що ці номери функціонують у межах Запорізької області. Була виявлена схема маршрутизації вхідного міжнародного трафіку, в якій невідомою особою за допомогою спеціального телекомунікаційного обладнання (комп'ютерна програма) здійснювалася підміна оригінального номера «А» (номер абонента, який здійснює вихідний міжнародний дзвінок) на номер ТОВ «Астеліт» у національному форматі для зниження ціни розмови.

Під час проведення досудового розслідування було встановлено, що телефонні виклики з номерів мобільного оператора зв'язку ТОВ «Астеліт» з ознаками рефайлінгу надходили на телекомунікаційну мережу загального користування м. Запоріжжя на такі номери: НОМЕР_13, НОМЕР_14, НОМЕР_15, НОМЕР_16, НОМЕР_17, НОМЕР_18, НОМЕР_19, НОМЕР_20, НОМЕР_21, НОМЕР_22, НОМЕР_23, НОМЕР_24, НОМЕР_25. Особи, які користуються вказаними номерами, є свідками у цьому проваджені, оскільки можуть підтвердити факти отримання міжнародних телефонних дзвінків. Слідчий звернувся з клопотанням до слідчого судді щодо отримання реєстраційних даних вищезазначених користувачів (абонентів) телефонних номерів ЗФ ПАТ «Укртелеком». Вказана інформація є персональними даними особи, що перебувають у базі персональних даних ЗФ ПАТ «Укртелеком», та може бути отримана лише у представника ЗФ ПАТ «Укртелеком». Крім того, у ній буде міститись інформація щодо імені абонента та його місцезнаходження, що дозволить встановити контакти вказаного абонента та його особу. Зазначені дані мають суттєве значення для встановлення важливих обставин на стадії досудового розслідування [11].

Отже, щоб встановити персональні дані свідків, які містяться у ЗФ ПАТ «Укртелеком», необхідно слідчому звернутися з клопотанням до слідчого судді для отримання дозволу про тимчасовий доступ до речей і документів. Згідно зі ст. 159 КПК України тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої перебувають такі речі і документи, можливості ознайомитися з ними, зробити їх копії та у разі прийняття відповідного рішення слідчим суддею або судом вилучити їх. Відповідно до вимог ст. 163 КПК слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, якщо сторона кримінального провадження, крім обставин, передбачених частиною п'ятою цієї статті, доведе можливість використання як доказів відомостей, що містяться у цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів. Слідчий суддя, суд в ухвалі про надання тимчасового доступу до речей і документів може дати розпорядження про надання можливості вилучення речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що без такого вилучення існує реальна загроза зміни або знищення речей чи документів (або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів). Відповідно до ст. 166 КПК України у разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями цього Кодексу для відшукання та вилучення зазначених речей і документів.

На нашу думку, знизити рівень рефайлінгу можливо лише активними, безперервними діями, працюючи на випередження. Будь-які засоби протидії будуть породжувати зустрічну протидію. Це замкнуте коло, яке неможливо розірвати. Можна лише постійно вдосконалювати засоби боротьби [10].

Для цього, на нашу думку, необхідно вживати таких заходів:

– постійно підвищувати кваліфікацію кіберполіцейських з навчання співробітників новим технологіям. Впроваджувати у програми підвищення кваліфікації працівників ОВС, які проводяться на базі вищих навчальних закладів, теми щодо протидії сучасним кіберзлочинам, їх виявлення, документування та особливостей розслідування;

– проводити інформаційно-агітаційні заходи з випускниками цивільних навчальних закладів (інститутів, факультетів) інформаційно-технічного спрямування щодо їх залучення до роботи в органах внутрішніх справ [12];

– організовувати постійний обмін досвідом із провідними фахівцями правоохоронних органів та інших установ у сфері попередження комп'ютерної злочинності, припинення випадків фінансових шахрайств у мережі Інтернет. У рамках такого обміну доцільною є організація стажування практичних працівників у відповідних правоохоронних органах та інших установах, організаціях, що спеціалізуються на цьому питанні [12].

– проводити постійний обмін досвідом із закордонними фахівцями правоохоронних органів у сфері виявлення та документування особливостей розслідування таких злочинів;

– закуповувати та впроваджувати сучасні системи з виявлення шахраїв;

– постійно співпрацювати з телеком-компаніями, що потерпають від такого злочину;

– моніторити пропозиції в Інтернеті щодо продажу обладнання для рефайлінгу, програмного забезпечення, щодо проведення навчання.

Висновок. Отже, вчинення рефайлінгу в Україні зумовлене багатьма факторами, що зазначені у статті, ключові із них такі: привабливість такого «бізнесу» високими доходами за незначних матеріальних затрат; відсутність належного досвіду та практичних навичок працівників кіберполіції для протидії такій злочинності; недостатнє фінансування напрямку боротьби з кіберзлочинами в правоохоронних органах; низька профорієнтаційна робота щодо залучення обдарованої молоді до роботи у кіберполіції; відсутність належної взаємодії мобільних операторів з працівниками кіберполіції. У статті розкрито поняття рефайлінгу, надано характеристику особливостям його вчинення, встановлено основні причини розвитку рефайлінгу в Україні, визначено та окреслено проблемні питання щодо його протидії. Також надані пропозиції щодо перешкоджання такій злочинності. Для зниження цього злочинного прояву потрібно не тільки активно і безперервно вирішувати зазначені нагальні питання, але й працювати на попередження таких проявів шляхом постійного вдосконалення методів та засобів з протидії таким кіберзлочинам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Пассивные методы выявления нелегальной терминации трафика. Финансы в IT, Исследования и прогнозы в IT. URL: https://habrahabr.ru/post/320716/.
2. Что такое рефайлинг голосового трафика. URL: https://goantifraud.com/ru/blog/529-chto-takoe-refayling-golosovogo-trafika.html.
3. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV. Ст. 2644. URL: https:// zakon.rada.gov.ua/go1280-15.
4. Порядок маршрутизації трафіку в телекомунікаційній мережі загального користування України: рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 05.07.2012 № 324. Офіційний вісник України, 2012. № 60. Ст. 2452.
5. 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 II Міжнар. наук.-практ. конф. (Тернопіль, 21–22 квіт. 2017 р.). Тернопіль: Економічна думка, 2017. С. 341–344.
6. Кримінальний кодекс України від 05 квітня 2001 р. Відомості Верховної Ради України, 2001. № 25–26. Ст. 131.
7. Мобильные мошенники: как обворовывают сотовых операторов. URL: http://forbes.net.ua/business/1427285-mobilnye-moshenniki-kak-obvorovyvayut-sotovyh-operatorov.
8. Вирок Деснянського районного суду м. Чернігова від 21. січ. 2011 року. Справа № 4/2506/44/11. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/46177402.
9. Кушніренко Н. Вони традиційно заробляють на людських слабостях. Галицький кореспондент. 2014. URL: http://cripo.com.ua/print.php?sect_id=6&aid=170782.
10. Боровський В. Злочини хакерів у Вінниці: за якими схемами крадуть гроші через інтернет. URL: https://vn.20minut.ua/Kryminal/zlochini-hakeriv-u-vinnitsi-za-yakimi-shemami-kradut-groshi-cherez-int-10497697.html.
11. Вирок Комунарського районного суду м. Запоріжжя від 21 травня 2014 року. Справа № 333/4018/14-к. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/38856973.
12. Ліненко Ю.О., Фурашев В.М. Кіберзлочинність. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: тези доп. Міжнарод. науково-практ. конф.(Київ, 21 квітня 2017 р.): в 2-х частинах. Частина друга. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». Київ, 2017. С. 38–41.
13. VoIP или IP-телефония IP-коммуникации в бизнесе. URL: http://www.lessons-tva.info/edu/trainbus/1_1.html.
14. Термінація трафіку. URL: http://kodeksy.com.ua/dictionary/t/terminatsiya_trafika.htm.
15. Фрод // Вікіпедія: вільна енциклопедія. URL https://ru.wikipedia.org/wiki/Фрод.