УДК 343.985

О.Б. Сахарова,
кандидат юридичних наук,
старший науковий співробітник

ОСОБЛИВОСТІ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННИХ ЗАСОБІВ ДОСТУПУ ДО ІНФОРМАЦІЇ БАНКІВСЬКИХ УСТАНОВ

У статті автор намагається розкрити особливості вчинення злочинів, пов'язаних з використанням електронних засобів доступу до інформації банківських установ, а саме шахрайських операцій з банківськими рахунками за допомогою системи дистанційного банківського обслуговування "Клієнт-банк", та визначити способи вчинення неправомірного заволодіння грошовими коштами з картрахунку фізичної особи за допомогою використання банкоматів. Особлива увага приділяється розгляду злочину, пов'язаного із встановленням на банкоматах незаконних пристроїв для зчитування інформації ("скіммерів").

***Ключові слова**: кіберзлочин, кібершахрай, скіммінг, скіммер, хакер, банкомат, Інтернет-банкінг, лог-файли, траппінг, картридер, ПІН-код, слот, ПІН-ПАД, кардінг, кардер, дамп, шаттер, шіммінг.*

В статье автор пытается раскрыть особенности совершения преступлений, связанных с использованием электронных средств доступа к информации банковских учреждений, а именно мошеннических операций с банковскими счетами с помощью системы дистанционного банковского обслуживания "Клиент-банк", и определить способы совершения неправомерного завладения денежными средствами с картсчета физического лица посредством использования банкоматов. Особое внимание уделяется рассмотрению преступления, связанного с установкой на банкоматах незаконных устройств для считывания информации ("скиммеров").

***Ключевые слова**: киберпреступление, кибермошенник, скимминг, скиммер, хакер, банкомат, Интернет-банкинг, лог-файлы, траппинг, картридер, ПИН-код, слот, ПИН-ПАД, кардинг, кардер, дамп, шаттер, шимминг.*

In the paper the author tries to reveal the features of committing crimes related to the use of electronic means of an access to information banking institutions, namely fraudulent transactions from Bank accounts via the remote banking system "Client-Bank", and to determine the ways of committing illegal appropriation of funds from the card account of an individual through the use of ATMs. Special attention is paid to the crimes associated with the installation of the ATMs of illicit devices for the reading of information ("skimmers").

***Keywords:** cybercrime, cyber fraudster, skimming, skimmer, hacker, ATM, Internet Banking, log files, trapping, card reader, PIN code, PIN PAD, carding, carder, dump, shutter, schimming.*

Останнім часом набула глобального масштабу проблема кіберзлочинності. Серед найбільш уразливих до кіберзлочинів сфер суспільного життя належить фінансовий сектор економіки, а саме банки та їх послуги. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв.

Швидкі темпи розвитку фінансових ринків та все більш зростаюча масштабність проведення розрахунків у міжнародних платіжних системах супроводжуються одночасним виникненням різних ризиків, пов'язаних з вчиненням шахрайств із застосуванням електронних засобів доступу до інформації банківських установ та з використанням платіжних карток. У зв'язку з цим акцентування уваги на особливостях вчинення злочинів у банківській системі здійснення електронних платежів, оцінювання ризиків шахрайства в цій системі, а також обґрунтування необхідності розробки ефективної системи заходів щодо протидії зазначеним злочинам є досить актуальними в умовах інтернаціоналізації систем масових електронних платежів, що і визначило тему цієї статті.

Питанням розвитку платіжних систем та аналізу ризиків, що виникають у них, присвячена велика кількість наукових робіт вітчизняних та зарубіжних вчених, зокрема таких як Л.В. Бистров, П.Г. Грабовий, В.М. Желіховський, А.О. Єпіфанов, Т. Ііварінен, О.О. Карпов, О.І. Лаврушин, Х. Лейнонен, Дж. Мак-Ендрюс, Ф.Х. Найт, Б.І. Скородумов, В.П. Страхарчук та ін. Проблематика розкриття способів вчинення злочинів у банківській сфері досліджувалась у роботах: Д.В. Березіна, А.Ф. Волобуєва, О.В. Волохової, В.І. Гаєнка, В.П. Лаврова, В.Д. Ларичева, Т.А. Пазинич, Г.М. Спіріна, С.Ю. Шарова, С.С. Чернявського, П.С. Яні, Р.С. Сатуєва, Д.А. Шраера та ін. Проблему злочинних дій з використанням банківських платіжних карток вивчали А.В. Реуцький, В.Ю. Шепітько, О.В. Курман, А.Ю. Ільницький, Л.В. Бистров, С.І. Ніколаюк, Г.А. Матусовський тощо. Однак, незважаючи на велику кількість публікацій з цієї тематики, питання аналізу особливостей вчинення кримінальних правопорушень, пов'язаних з використанням електронних засобів доступу до інформації банківських установ, та мінімізації ризиків шахрайства учасників міжнародних платіжних систем в Україні залишається відкритим.

У 2012 р., за даними НБУ та Незалежної асоціації банків України, загальна кількість шахрайських операцій з банківськими рахунками в Україні збільшилась на 47 %, а сума збитків зросла на 20 % [1]. З 35 до 57 збільшилась кількість банків, з рахунків яких викрадались кошти [2]. Так, за 2012 рік у фізичних осіб було викрадено 11,4 млн грн. При цьому за обсягами вкрадених сум лідирують юридичні особи: за допомогою системи дистанційного банківського обслуговування (ДБО) "Клієнт-банк" за 2012 рік з їх рахунків було вкрадено 116 млн грн. У 2012 р. в Україні було зафіксовано 139 таких випадків шахрайства з використанням системи "Клієнт-банк", при цьому 75 % викрадених коштів (87 млн грн) було повернуто постраждалим особам [1]. Отже, у 2012 р. злочинцям вдалося вкрасти 29 млн грн через систему ДБО, що складає 25 % загального обсягу шахрайських операцій.

Загалом у 2012 р. 40 % від загальної кількості українських банків постраждали від кіберзлочинів [1].

Однак у 2013 р. скоротився обсяг вдалих крадіжок з банківських рахунків за допомогою системи "Клієнт-банк" [3]. За даними МВС України, у 2013 р. всього 12,5 % спроб злочинців увінчалися успіхом – в результаті їм удалося вкрасти 10,5 млн грн, сума заблокованих або повернених клієнтам коштів склала 76,5 млн грн [3]. Експерти зазначають, що такі кримінальні правопорушення найчастіше вчиняються віддалено за допомогою комп'ютерних вірусів, які дозволяють красти паролі доступу до банківських рахунків.

Незважаючи на скорочення в 2013 р. порівняно з 2012 р. числа вкрадених злочинцями сум з використанням системи "Клієнт-банк", кількість кіберзлочинів значно зросла. Якщо в 2013 р. було зафіксовано 468 фактів несанкціонованого

переведення грошей клієнтів при роботі з системами віддаленого доступу, то роком раніше – всього 139 випадків (див. вище).

Крім того, у 2013 р. було зафіксовано понад 350 випадків використання скіммінгових пристроїв, які на банкоматах зчитують дані з платіжних карток клієнтів [3]. У МВС України повідомили про вилучення 37 одиниць скіммінгового обладнання. Нерідко один й той же скіммінговий пристрій міг бути встановлений на декількох банкоматах, що належать різним банкам.

Кількість вчинених злочинів зі встановленням на банкоматах незаконних пристроїв для зчитування інформації також зросла й у м. Києві. Так, у 2012 р. співробітниками УБК ГУ МВС України у м. Києві було виявлено та вилучено два "скіммінгових" пристрої. Затриманий злочинець зі своїм спільником встановлювали пристрої для зчитування магнітних стрічок банківських платіжних карток та відеокамеру для запису ПІН-кодів у місцях значного скупчення громадян. Станом на 10 червня 2013 р. в м. Києві вже було виявлено та вилучено п'ять встановлених "скіммінгових" пристроїв та затримано четверо громадян [7; 8].

Значно поширились випадки крадіжок грошей із банкоматів. За словами начальника відділу департаменту Держслужби охорони МВС України Світлани Павлівської, у 2011 р. шляхом пограбування банкоматів було викрадено майже 9 млн грн, у 2012 р. – майже 12 млн грн, у першому півріччі 2013 р. збитки склали біля 2 млн грн. При цьому якщо за весь 2012 р. було вчинено 24 розкрадання із банкоматів, то з початку 2013 р. і до липня цього року – вже біля 20 таких злочинів. Кількість зазначених злочинів постійно зростає [5].

За даними МВС України, із практично 37 тис. банкоматів, зареєстрованих в Україні, підрозділами ДСО охороняється лише менше 10 %, а недержавними охоронними структурами – ще менша кількість АТМ. Таким чином, понад 80 % усіх банкоматів у країні функціонують без охорони та є легкою здобиччю для злочинців. Відповідно до статистики останніх років пристрої для зчитування магнітних стрічок банківських платіжних карток здебільшого встановлюють на банкоматах, які навіть не обладнані камерами спостереження.

Проте найбільш розповсюдженим серед кіберзлочинів, за даними начальника Управління боротьби з кіберзлочинністю МВС України Максима Литвинова, є шахрайство в системах дистанційного банківського обслуговування, коли злочинці зламують комп'ютер, підключений до банківської системи "Клієнт-банк", та здійснюють несанкціонований платіж нібито від імені клієнта [6].

У процесі вчинення шахрайства в системі електронних переказів "Клієнт-банк" злочинцями "запускається" вірус. Учасників злочинного угруповання щонайменше троє: хакер – розробляє шкідливу програму і запускає її; "фінансист" – створює систему переказу коштів; третій (фіктивна фірма або фізична особа) – отримує готівку. Добровольців, які одержують у банку незаконно здобуті кошти, часто знаходять в Інтернеті, на форумах – зазвичай це безробітні, студенти тощо.

Останнім часом також досить розповсюдженими є факти "зламування" систем Інтернет-банкінгу за допомогою спеціальних вірусів, які зчитують з ПК банківських клієнтів інформацію про карткові рахунки. Найчастіше використовується вірус типу back-door, що дозволяє зловмисникам дистанційно контролювати комп'ютери жертв. Як правило, у проміжок часу між зараженням комп'ютерів та проведенням несанкціонованої трансакції протягом декількох тижнів злочинці відстежують стан рахунків та аналізують технічні особливості з'єднання комп'ютерів клієнтів з серверами банків (лог-файли).

У цілому рівень розкриття крадіжок, що вчиняються за допомогою систем дистанційного банківського обслуговування, в органах внутрішніх справ досить

високий: за 2012 р. органи внутрішніх справ спільно з банками та Держфінмоніторингом змогли компенсувати 54 % збитків юридичних осіб в 74 випадках із 139 зафіксованих. Зазвичай відстежити кошти вдавалося після того, як вони починали стихійно переводитися з рахунку на рахунок у різних банках.

Слід зазначити, що ці злочини вчиняються як хакерами, які не мають жодного стосунку до банку, так і співробітниками банків, які мають доступ до персональних даних клієнтів. Так звані інсайдери досить часто надають конфіденційну інформацію шахраям, отримуючи за це відсоток від викрадених коштів.

Нижче розглянемо більш детально особливості вчинення неправомірного заволодіння грошовими коштами з картрахунку фізичної особи за допомогою використання банкоматів, яке, як вже підкреслювалося, є досить розповсюдженим кримінальним правопорушенням. Можна виділити такі способи його вчинення.

• "Ліванська петля" (траппінг). Спеціальним пристроєм блокується вікно подачі картки (картридер) так, щоб вона застрягла в банкоматі. Зловмисник попередньо підглядає ПІН-код, а потім співчуває та рекомендує терміново подзвонити в банк або сервісну службу. Як тільки власник картки відходить, злочинець витягує картку, звільняє вікно банкомату та знімає гроші.

"Ліванська петля" виготовляється з магнітної плівки аудіокасети для витягування банківської пластикової платіжної картки після її заковтування. Вона непомітна для неозброєного ока.

Таке діяння слід кваліфікувати за сукупністю відповідних частин ст.ст. 190 (шахрайство) та 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) Кримінального кодексу (КК) України.

• Фальшиві банкомати ("фантом"). Спосіб, який нечасто використовується, оскільки вимагає технічного обладнання. Шахраї виготовляють фальшиві банкомати, які виглядають як справжні, або переробляють старі та розміщують їх у людних місцях. Такий банкомат приймає картку, вимагає введення ПІН-коду, після чого видає повідомлення про неможливість видачі грошей (нібито через їх відсутність у банкоматі або технічну помилку) та повертає картку. У банкоматі відбувається копіювання даних з картки та ПІН-коду, що надалі дозволяє шахраям виготовити дублікат та зняти за його допомогою гроші з рахунку клієнта.

Створення фальшивих банкоматів необхідно кваліфікувати за сукупністю відповідних частин ст.ст. 190 (шахрайство) та 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) КК України.

• Копіювання магнітної смуги банківської картки (skimming (скіммінг)) за допомогою підставних пристроїв зчитування. Такі пристрої встановлюють на банкомат (зчитувач – на картоприймач, додатковою "клавіатурою" накривають справжню).

Скіммери відносяться до спеціальних технічних засобів негласного отримання та реєстрації інформації з технічних засобів її зберігання, обробки та передачі. Їх функціональне призначення – зчитування та запам'ятовування інформації, що міститься на магнітних стрічках банківських платіжних карток, та даних про їхні ПІН-коди.

Отже, скіммінгові пристрої – це так звані накладки, зчитувальний пристрій, який недосвідченому або навіть досвідченому користувачеві дуже складно зовні визначити: це деталь банкомата чи ні, адже зовні скіммери нагадують деталь банкомата. При користуванні таким банкоматом зчитувач зберігає дані з карток,

які вставляються в банкомат, а клавіатура – ПІН-коди. Як і в попередньому випадку (фальшиві банкомати), вкрадених даних достатньо для виробництва дубліката картки та зняття грошей з рахунку власника.

Таким чином, для скіммінга злочинці приєднують до банкомату спеціальний пристрій – скіммер. Для цього на картрідер встановлюють рамку з магнітною головкою, що зчитує інформацію з магнітної смуги та записує дампи карт на вбудовану мікросхему пам'яті. Для крадіжки карткових даних також застосовують накладну клавіатуру, яку приклеюють на звичайні клавіші. Така конструкція запам'ятовує натиснення клавіш при введенні ПІН-коду та записує інформацію на вбудовану мікросхему. Рухи руки людини, що вводить ПІН-код, може зняти і маленька відеокамера, прикріплена до банкомату. Дані передаються, наприклад, на дистанційний ноутбук шахраїв.

Розрізняють два типи скіммінгового обладнання. У першому випадку скіммінгове обладнання приєднується до слоту карткового приймача терміналу і зчитує інформацію замість самого пристрою. У цьому випадку користувач картки доступу до рахунку не отримує. В іншому випадку людина отримує доступ до рахунку, але згодом дізнається про несанкціоноване зняття коштів. В обох випадках зловмисники різними способами також дізнаються про ПІН-код картки, наприклад, шляхом використання прихованих камер, накладних клавіатур тощо. Інформація з магнітної стрічки переноситься на нову пластикову картку і використовується при безпосередньому знятті грошей через банкомат, оплаті товарів чи послуг через Інтернет або продається третім особам.

Відповідно до статистики зловмисники не залишаються на одному місці. Дані зчитуються і майже одразу виготовляється клон-картка та відбувається нелегальне знімання коштів, злочинець(ці) переїжджає(ють) на інше місце (іншу країну).

У більшості випадків несанкціоновані операції здійснюються у вечірній або нічний час, а також у вихідні дні, коли банківські установи не працюють і факт крадіжки встановлюється згодом.

Безперечно, факт невиявлення скіммінгового обладнання клієнтом не виключає відповідальності банківської установи стежити за відсутністю нелегально встановленого обладнанням на власному терміналі: картрідерів, накладок на клавіатуру, камер тощо.

Вчинення злочину, пов'язаного з незаконним встановленням та використанням скіммерів, кваліфікується за ст. 359 ("Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації") КК України.

• Підроблений ПІН-ПАД (пристрій для вводу ПІН-коду в платіжних терміналах) або додатковий елемент на електронний замок в приміщення з банкоматом, який відкривається за допомогою картки.

• Встановлення поруч з банкоматом мініатюрних відеокамер для викрадання ПІН-кодів. Така камера може бути замаскована під встановлений поруч із ним чи прикріплений до банкомату або стіни предмет.

Таке діяння слід кваліфікувати за сукупністю відповідних частин ст.ст. 190 КК України (шахрайство) та 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) КК України.

• Крадіжка (зняття) ПІН-коду за тепловим відбитком на клавіатурі банкомату з використанням високочутливої інфрачервоної камери. Зловмисник, який стоїть у черзі, робить знімок клавіатури, на якій попередній користувач набирав ПІН-код. Клавіші, до яких торкалися, трохи тепліші, причому остання

натиснута клавіша тепліша від передостанньої і т.п. Причому успішність цього методу залежить від типу клавіатури (металеві клавіатури мають більшу теплопровідність, і температура їх клавіш швидко вирівнюється) і від того, чи не набирав клієнт ще якісь комбінації, наприклад, суму.

• Кардінг. Існують спеціальні сайти кардерів – шахраїв з дампами – копіями платіжних карток з треками магнітних смуг. У середовищі карткових шахраїв цей бізнес називається кардінг.

Найпростіший спосіб отримати копію банківської картки – через працівників магазинів, ресторанів, салонів краси, перукарень, тренажерних залів, інших об'єктів сфери обслуговування, де при оплаті клієнти часто використовують банківські платіжні картки.

Усі перераховані технічні пристрої складно помітити непрофесіоналу. Отримавши за допомогою таких пристроїв необхідні відомості про картку, шахраї виготовляють із звичайного пластика копію картки. Деякі ділки на пластик накладають зображення, щоб зробити його більш впізнаваним для банкомату.

Втім, багато сучасних банкоматів не пропускають цей фальшивий "білий пластик". Тоді кардери зафарбовують його, і фальшива, вже зафарбована і близька до оригіналу картка проходить через банкомат. Але якщо і після цього йде невдала трансакція, то шахраї, знаючи номер картки, її CVC/CVV код (три останні цифри, вказані на зворотній стороні картки), все одно можуть скористатися чужими грошима: оплатити через Інтернет мобільні рахунки, послуги ЖКГ тощо.

Для виготовлення дампа потрібно непогано розбиратися в сучасних ІТ-технологіях, мати сучасний потужний комп'ютер. Нерідко злочинці придбають вже готові дампи через сайти кардерів.

• Шаттер. Шахраї можуть блокувати неповернення не тільки картки в картоприймач банкомату, а й самих грошей. Для цього на шаттер (проріз / слот, через який відбувається видача грошей) наклеюється сторонній пристрій, блокуючий видачу купюр банкоматом власнику картки. Відбувається це за рахунок розміщення липкої стрічки на внутрішній частині пристрою, до якої і пристають купюри. Відповідно цей чужорідний елемент не дасть банкомату і забрати гроші назад[1].

Перевлаштування справжніх банкоматів таким чином, щоб кошти, які видає банкомат відповідно до запитів клієнтів, застрягали в слоті отримання готівки, слід кваліфікувати за сукупністю відповідних частин ст.ст. 190 КК України (шахрайство) та 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) КК України.

• Шіммінг – використання злочинцями пристрою, який зчитує інформацію з банківської платіжної картки та який повністю знаходиться у щілині картоприймача банкомату. Цей пристрій, щоб поміститися в отворі банкомату і не заважати при цьому зануренню туди ж банківської картки, є дуже мініатюрним (менше 0,1 мм), проте високотехнологічним, коштовним та відповідно менш поширеним ніж класичні скіммери.

Як повідомили в ГУМВС України в м. Києві, станом на кінець листопада 2012 р. працівниками Управління боротьби з кіберзлочинністю було порушено 40 (у порівнянні з 2011 р. – 20) кримінальних справ за ознаками злочинів, пов'язаних з привласненням грошових коштів шляхом незаконного доступу до

[1] Банкомати оснащені функцією втягування назад незатребуваних купюр по закінченню певного часу.

банкоматів та електронних рахунків. У період з 20 листопада 2012 р. до середини 2013 р. в Києві вже було порушено 43 кримінальні справи цієї категорії [7; 8].

Необхідно зазначити, що шахрайський обман у сфері функціонування банківських платіжних систем реалізується за допомогою використання електронно-обчислювальної техніки, що потребує наявності в злочинців відповідних знань, рівня підготовки, навичок. Він може проявлятися в застосуванні злочинцем програмних засобів, які дають змогу здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах банківських установ, з метою введення в оману автоматизованої системи і, видавши себе за законного користувача, здійснити ті чи інші корисливі операції. При цьому злочинець впливає на процес обробки інформації, він здатен змінити її зміст чи знищити, задати необхідну для заволодіння майном/грошима команду. У зв'язку з цим постає нагальна проблема необхідності підвищення рівня підготовки оперативних працівників органів внутрішніх справ з метою ефективного розслідування кримінальних правопорушень, пов'язаних з використанням електронних засобів доступу до інформації банківських установ.

Перші кроки в напрямі поліпшення ситуації з виявленням та розкриттям злочинів цієї категорії вже є. Серед них можна, зокрема, виділити те, що 5 лютого 2013 р. правоохоронці та банкіри підписали Меморандум про співпрацю, що дасть можливість банкам в оперативному режимі обмінюватися інформацією про нові види шахрайств, про шкідливі віруси та пристрої для викрадення конфіденційної інформації [9]. Слід зазначити, що позитивним моментом у протидії кіберзлочинності є також запуск сайту "Антикібер", який надає практичні поради про те, як не стати жертвою кіберзлочинців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Омельченко О.С.* Проблеми протидії кіберзлочинності в кредитно-банківській сфері / О.С. Омельченко // Протидія кіберзлочинності в фінансово-банківській діяльності : матеріали Всеукр. наук.-практ. конф. – 2013. – 23 квітня. – С. 74.

2. *Шидловська Є.* Україна відстає у розвитку інформаційних технологій, натомість лідирує у піратстві та хакерстві / Є. Шидловська // Український тиждень. – 2013 [Електронний ресурс]. – Режим доступу : http : // tyzhden.ua/News/77138/PrintView.

3. У 2013 році скоротився обсяг вдалих крадіжок з банківських рахунків [Електронний ресурс]. – Режим доступу : http : // lohotron.in.ua/2014/02/u-2013-rotsi-skorotyvsya-obsyah-vdalyh-kradizhok-z-bankivskyh-rahunkiv/.

4. *Головко О.М.* Підвищення практичної спрямованості підготовки фахівців по боротьбі з кіберзлочинністю / О.М. Головко // Протидія кіберзлочинності в фінансово-банківській діяльності : матеріали Всеукр. наук.-практ. конф. – 2013. – 23 квітня. – С. 28–29.

5. *Гриньков Д.* В разводном ключе / Д. Гриньков // Бизнес. – 2013. – № 26. – С. 37.

6. Щоб не стати жертвою шахраїв, найчастіше достатньо пильності (Ексклюзивне інтерв'ю начальника Управління боротьби з кіберзлочинністю МВС України Максима Литвинова агентству "Інтерфакс-Україна"). – 06.07.2013 [Електронний ресурс]. – Режим доступу : http : // www.mvs.gov.ua/.

7. Сезон кібершахрайств. – 18.06.2013 [Електронний ресурс]. – Режим доступу : http : // anticyber.com.ua/article_detail.php?id=79 (сайт Незалежної асоціації банків України).

8. В Україні зростає фінансова кіберзлочинність – 17.12.2013 [Електронний ресурс]. – Режим доступу : http : // anticyber.com.ua/news_detail.php?id=522 (сайт Незалежної асоціації банків України).

9. Правоохоронці та банкіри підписали Меморандум про співпрацю (прес-служба МВС України) [Електронний ресурс]. – Режим доступу : http : // www.kmu.gov.ua/control/uk/publish/article?art_id=246030781.