

НАУКОВІ ДИСПУТИ ЩОДО КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ, ТА ПОБУДОВИ ЇХ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ

SCIENTIFIC DISPUTES REGARDING CRIMINAL OFFENSES RELATED TO THE USE OF INTERNET BANKING AND THE CONSTRUCTION OF THEIR FORENSIC CHARACTERISTICS

Сисолятин В.В., здобувач

Науково-дослідного інституту публічного права

Наукова стаття присвячена висвітленню окремих аспектів розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу. Розглядається їх розвиток в нормативно-правовому плані та побудова криміналістичної характеристики вказаної категорії протиправних діянь.

Зазначається, що кримінальні правопорушення, пов'язані з використанням інтернет-банкінгом, з кожним роком збільшуються як в своїй кількості, так і в якості. Адже розвиток комп'ютерних технологій та мережі Інтернет не зупиняється ні на мить. Тому й правопорушники, які вчиняють досліджувані протиправні діяння, застосовують все новіші засоби та способи їх скоєння. В той же час, працівники правоохоронних органів повинні не відставати від вказаної категорії осіб, а навпаки – намагатися їх випереджати та передбачати їх наступні кроки. В свою чергу, це вимагає від науковців здійснювати сучасні дослідження з практичними рекомендаціями для попередження та розслідування визначених протиправних діянь.

Визначено, що ще на початку 2000-их років міжнародні законодавці розуміли необхідність визначити конкретні протиправні діяння, які можуть здійснюватись з використанням комп'ютерних систем. Вказані положення були закріплені в ряді міжнародних нормативно-правових актах, серед яких необхідно виокремити Конвенцію про кіберзлочинність та Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Аналіз Кримінального кодексу України та ряду інших нормативно-правових актів дозволив зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані в правове поле нашої держави. Стосовно криміналістичної характеристики правопорушень, пов'язаних з використанням інтернет-банкінгу, зазначено, що для неї головним є побудова правильних кореляційних зв'язків, які будуть допомагати уповноваженим особам у плануванні розслідування кримінальних правопорушень та проведенні окремих слідчих (розшукових) дій, а також інших процесуальних заходів. Сформульовано авторське визначення криміналістичної характеристики.

Ключові слова: кримінальні правопорушення, інтернет-банкінг, кіберзлочинність, криміналістична характеристика, кореляційні зв'язки, слідча (розшукова) дія.

The scientific article is devoted to the coverage of certain aspects of the investigation of criminal offenses related to the use of Internet banking. Their development in the regulatory and legal plan and the construction of the forensic characteristics of the specified category of illegal acts are considered.

It is noted that criminal offenses related to the use of Internet banking are increasing every year both in number and quality. After all, the development of computer technologies and the Internet does not stop for a moment. That is why the offenders who commit the investigated illegal acts use more and more new means and ways of committing them. At the same time, law enforcement officers must keep up with the specified category of persons, and on the contrary, try to anticipate them and predict their next steps. In turn, this requires scientists to carry out modern research with practical recommendations for the prevention and investigation of certain illegal acts.

It was determined that even at the beginning of the 2000-s, international legislators understood the need to define specific illegal acts that can be carried out using computer systems. These provisions were enshrined in a number of international legal acts, among which it is necessary to single out the Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of racist and xenophobic acts committed through computer systems. The analysis of the Criminal Code of Ukraine and a number of other normative legal acts made it possible to conclude that the measures defined by both the Convention and the Additional Protocol to it are almost completely implemented in the legal field of our state. With regard to the forensic characteristics of offenses related to the use of Internet banking, it is stated that the main thing for it is the construction of correct correlations, which will help authorized persons in planning the investigation of criminal offenses and conducting separate investigative (search) actions, as well as other procedural measures. The author's definition of forensic characteristics is formulated.

Key words: criminal offenses, internet banking, cybercrime, forensic characteristics, correlations, investigative (search) action.

Постановка проблеми. Кримінальні правопорушення, пов'язані з використанням інтернет-банкінгом, з кожним роком збільшуються як в своїй кількості, так і в якості. Адже розвиток комп'ютерних технологій та мережі Інтернет не зупиняється ні на мить. Тому й правопорушники, які вчиняють досліджувані протиправні діяння, застосовують все новіші засоби та способи їх скоєння. В той же час, працівники правоохоронних органів повинні не відставати від вказаної категорії осіб, а навпаки – намагатися їх випереджати та передбачати їх наступні кроки. В свою чергу, це вимагає від науковців здійснювати сучасні дослідження з практичними рекомендаціями для попередження та розслідування визначених протиправних діянь. Тобто вбачаємо за нагальну потребу дослідити криміналістичну характеристику як елемент методики розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу.

Аналіз останніх досліджень і публікацій. Розробкою криміналістичної характеристики протиправних

діянь займалися наступні відомі вітчизняні вчені-криміналісти, зокрема, В. П. Бахін, А. В. Іщенко, В. О. Коновалова, Б. Є. Лук'янчиков, Р. Л. Степанюк, В. В. Тіщенко, К. О. Чаплинський, Ю. М. Черноус, В. Ю. Шепітько та інші. Але потрібно зазначити, що наше дослідження є комплексним підходом до опрацювання генези наукових поглядів стосовно кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, а також побудовою їх криміналістичної характеристики.

Метою даної статті є дослідження кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, та побудовою їх криміналістичної характеристики.

Виклад основного матеріалу дослідження. Загалом, в Конвенції про кіберзлочинність, ратифікованої Україною 07.09.2005 року визначено, які правопорушення вчиняються за допомогою комп'ютерних систем. В зазначеному документі вказано наступні групи протиправних діянь: правопорушення проти конфіденційності, ціліс-

ності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6)); правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8)); правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією (ст. 9)); правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10) [5]. Як бачимо, ще на початку 2000-их років міжнародні законодавці розуміли необхідність визначити конкретні протиправні діяння, які можуть здійснюватись з використанням комп'ютерних систем.

Також у визначенні Конвенції передбачено, що сторонами вживаються: законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів (ст. 11); законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи (ст. 12); законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань (ст. 14); встановлення, імплементація і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини (ст. 15) [5].

З огляду на зазначене, можна зробити висновок, що вказані заходи відображають максимально широкі повноваження кожної держави, яка ратифікувала зазначену конвенцію (у тому числі, й України).

Крім того, менше ніж через два роки було підписано Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, ратифікований Україною 21.07.2006 року. В даному документі надано визначення расистського та ксенофобного матеріалу, а саме вказано, що це будь-який письмовий матеріал, будь-яке зображення чи будь-яке інше представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій (ст. 2) [3]. Тобто в Додатковому протоколі визначено нагальні на той час питання дискримінації осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання. Вказані аспекти є і зараз актуальними в Україні, адже на часі неодноразово виникають ситуації пов'язані з нетерпимістю осіб через національне або етнічне походження та віросповідання.

В додатковому протоколі теж передбачено, що сторонами вживаються наступні заходи: законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу (ст. 3); законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: погроза, зроблена через комп'ютерну систему, вчинення злочину, визначеного в її національному законодавстві, проти (і) осіб з причини їх

належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (і) групи осіб, яка відрізняється за будь-якою з цих характеристик (ст. 4); законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: публічна образа через комп'ютерну систему (і) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (і) групи осіб, яка відрізняється за будь-якою з цих характеристик (ст. 5); законодавчих й інших заходів, які можуть бути необхідними для визнання таких дій кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства (ст. 6); законодавчих й інших заходів, які можуть бути необхідними для визнання кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це, пособництва або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до цього Протоколу, з наміром вчинити такий злочин [3].

Аналіз Кримінального кодексу України [7] та ряду інших нормативно-правових актів дозволяє зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імplementовані в правове поле нашої держави. Зокрема, в Законі України «Про основні засади забезпечення кібербезпеки України» надано ряд основоположних визначень: індикатори кіберзагроз; інформація про інцидент кібербезпеки; інцидент кібербезпеки (кіберінцидент); кібератака; кібербезпека; кіберзагроза; кіберзахист; кіберзлочин (комп'ютерний злочин); кіберзлочинність; кібероборона; кіберпростір; кіберрозвідка; кібертероризм; кібершпигунство; критична інформаційна інфраструктура та інші. Також у вказаному законодавчому акті визначено відповідних суб'єктів, «...які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом». Крім того, у вказаному Законі зазначено основних суб'єктів національної системи кібербезпеки, а саме: «...Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України» [10]. Як бачимо, на законодавчому рівні сформовано досить широке коло підрозділів, на які покладено обов'язок забезпечувати національну систему кібербезпеки.

Говорячи про криміналістичну характеристику правопорушень, пов'язаних з використанням інтернет-банкінгу, для початку необхідно визначитись з формулюванням її поняття. Наприклад, В. В. Тіщенко наголошував про те,

що «...у розслідуванні нерозкритих кримінальних правопорушень корисливо-насилницької спрямованості криміналістичний аналіз встановлених обставин дозволяє виявити між ними спільні та особливі риси, зробити висновок про можливе скоєння цих протиправних діянь однією і тією ж особою або однією і тією ж групою осіб. Такий висновок може бути зроблений не лише на основі повної криміналістичної характеристики кожного окремого кримінального правопорушення, а й на основі криміналістичного аналізу їх окремих обставин» [13, с. 19].

Також в розрізі зазначеного вважаємо доречним навести твердження В. В. Лисенка, який вказує на те, що значення криміналістичної характеристики має практичне призначення не лише у випадку встановлення типових зв'язків між її елементами. Автор зазначає, що вказана категорія може бути також ефективно застосована у діяльності правоохоронних органів за наявності нетипових особливостей окремих елементів чи зв'язків. Наостанок науковець зробив висновок, що до змісту криміналістичної характеристики необхідно включати інформацію про кримінальні правопорушення, яка має одиничні прояви, адже зазначені нетипові прояви злочинної діяльності можуть мати поширення у майбутньому [8, с. 234].

В свою чергу, окрема група вчених-криміналістів (Ю. М. Черноус, А. В. Самодін) визначають криміналістичну характеристику кримінальних правопорушень як систему узагальнених даних про найбільш типові ознаки певного виду (групи) кримінальних правопорушень, закономірний взаємозв'язок яких слугує основою наукового і практичного вирішення завдань розслідування [6, с. 579]. Зі свого боку, Г. А. Матусовський зауважує, що досліджувана наукова категорія, як накопичення та джерело відомостей про певні види кримінальних правопорушень, виконуючи інформаційну функцію, становить собою єдину інформаційну систему. Використання останньої можливо шляхом одержання й аналізу відомостей щодо окремих елементів і встановлення зв'язків між ними, адже у цьому розумінні всі елементи системи теоретично рівнозначні і поділяти їх на основні та другорядні недоцільно. У той же час, Г. А. Матусовський зауважує, що використання такої інформаційної системи вимагає в кожному конкретному випадку виокремлення ключового елемента, через який можна здійснити «вхід» у систему з метою одержання необхідної інформації. Автор досить точно зазначає, що виокремлення ключового елемента для конкретного випадку залежить від конкретної слідчої ситуації, що склалася на даному етапі розслідування, а також від того, які вихідні дані має уповноважена особа та які з них необхідно встановити [9, с. 149].

Цікавою вважаємо думку А. Ф. Волобуєва, який засвідчує те, що «...криміналістична характеристика як кримінально-правова й кримінологічна містить у собі інформацію про злочин у цілому, а також елементи, що його складають (об'єкт і об'єктивну сторону, суб'єкт і суб'єктивну сторону). На відміну від інших характеристик вона являє собою, по-перше, систему тільки криміналістично значимих відомостей про ознаки злочину, а не будь-яких однакових для всіх видів злочинів. У межах певного виду вони можуть сприяти його розкриттю. По-друге, відомості про ознаки елементів злочину описують на якісно-кількісному рівні. Таким чином підвищується практичне значення даної категорії криміналістики» [2, с. 32]. Як бачимо, автор в структуру визначеної наукової категорії в криміналістичному контексті включає як кримінально-правові, так і кримінологічні характеристики.

Досить влучним вважаємо твердження В. Д. Берназа, який вказував на те, що без опрацювання великого масиву кримінальних проваджень не представляється можливим визначити систему узагальнених відомостей групи протиправних діянь. З огляду на це, автор сформулював наступне визначення криміналістичної характеристики –

«...це основана на державних статистичних даних науково-обґрунтована система узагальненої інформації та їх джерел про обставини, які були доказані, та інші, які мали значення для попередження, виявлення, розслідування та судового розгляду досліджуваних злочинів зазначеної категорії» [1, с. 17]. В свою чергу, М. М. Єфімов, даючи формулювання досліджуваної наукової категорії зробив це наступним чином: «...це система відомостей про криміналістично значущі ознаки кримінально караного діяння, яка відображає закономірні зв'язки між ними і слугує побудові та перевірці слідчих версій для вирішення основних завдань розслідування» [3, с. 14-15].

А вже А. В. Старушкевич зазначає, що «...однією з причин неефективної боротьби з окремими видами злочинів є недостатнє дослідження саме криміналістичного аспекту пошуково-пізнавальної діяльності. Невипадково слідчі одноставно зазначають, що наявні у їх розпорядженні методичні рекомендації мають суттєві недоліки, не вміщують у достатньому об'ємі інформації, що необхідна для їх практичної діяльності. Все це висуває вказану багатопланову проблему в коло актуальних напрямків, як теоретичних, так і прикладних криміналістичних досліджень. До вказаних досліджень і слід віднести роботи, пов'язані з розробкою теоретичних засад криміналістичної характеристики; формуванням криміналістичних характеристик окремих видів злочинів і їх використання для оптимізації попереднього слідства, підвищення його ефективності» [12, с. 3-4]. Тобто науковець наголошує на важливості зведення методичних рекомендацій практичним підрозділам до сухої алгоритмізації їх діяльності. У той же час, В. Л. Синчук, на нашу думку, досить точно та правильно вказує на те, що практичне значення криміналістичної характеристики зводиться до того, що «...вона є робочим інструментом слідчого, який він може використати у процесі розслідування конкретного злочину на підставі порівняння отриманих відомостей з тими типовими, що відображені у криміналістичній характеристиці і притаманні саме цьому виду злочинної діяльності» [11, с. 9]. Як бачимо, автор засвідчує те, що для досліджуваної наукової категорії головним є побудова правильних кореляційних зв'язків, які будуть допомагати уповноваженим особам у плануванні розслідування кримінальних правопорушень та проведенні окремих слідчих (розшукових) дій, а також інших процесуальних заходів.

З огляду на вищезазначене, можемо зробити висновок, що криміналістична характеристика правопорушень, пов'язаних з використанням інтернет-банкінгу, – це сукупність даних, отриманих із судово-слідчої практики, про криміналістично значимі ознаки певної категорії протиправних діянь, яка зводиться до кореляційних зв'язків між ними та забезпечує побудову і перевірку криміналістичних версій для вирішення основних завдань кримінального провадження, а також надає додаткову інформацію, необхідну для ефективного проведення слідчих (розшукових) дій.

Висновок. Констатуємо вищенаведене, зазначимо, що на початку 2000-их років міжнародні законодавці розуміли необхідність визначити конкретні протиправні діяння, які можуть здійснюватись з використанням комп'ютерних систем. Вказані положення були закріплені в ряді міжнародних нормативно-правових актах, серед яких необхідно виокремити Конвенцію про кіберзлочинність та Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Аналіз Кримінального кодексу України та ряду інших нормативно-правових актів дозволив зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані в правове поле нашої держави. Стосовно криміналістичної характеристики правопорушень, пов'язаних з викорис-

танням інтернет-банкінгу, зазначено, що для неї головним є побудова правильних кореляційних зв'язків, які будуть допомагати уповноваженим особам у плануванні роз-

слідування кримінальних правопорушень та проведенні окремих слідчих (розшукових) дій, а також інших процесуальних заходів.

ЛІТЕРАТУРА

1. Берназ В.Д. Криміналістична характеристика як наукова категорія. *Південноукраїнський правничий часопис*. 2006. № 1. С. 16–18.
2. Волобуєв А.Ф. Криміналістична характеристика розкрадань майна у сфері підприємницької діяльності. *Вісник Університету внутрішніх справ*. 1997. Вип. 2. Харків. С. 26–37.
3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : підписаний в м. Страсбург 28 січня 2003 року. URL : http://zakon0.rada.gov.ua/laws/show/994_687 (дата звернення – 06.03.2020р.).
4. Єфімов М.М. Розслідування злочинів проти громадського порядку та моральності : навч. посібник. 2-е вид., доп. і перероб. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 188 с.
5. Конвенція про кіберзлочинність : підписана в м. Будапешт 23 листопада 2001 року. URL : http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення – 06.03.2020р.).
6. Криміналістика : підручник / [В.В. Пясковський, Ю.М. Черноус, А.В. Самодін та ін.]; за заг. ред. В.В. Пясковського. 2-ге вид., перероб. і допов. Харків : Право, 2020. 752 с.
7. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14/page#Text> (дата звернення – 06.03.2020р.).
8. Лисенко В.В. Криміналістичне забезпечення діяльності податкової міліції (Теорія та практика) : монографія. Київ : Логос, 2004. 324 с.
9. Матусовский Г.А. Структура криміналістичної характеристики злочинів. Криміналістика : Криміналістична тактика і методика розслідування злочинів. За ред. В.Ю. Шепітька. Харків : Право, 1998. 368 с.
10. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL : <http://zakon2.rada.gov.ua/laws/show/2163-19> (дата звернення – 06.03.2020р.).
11. Синчук В.Л. Кореляційні залежності між елементами криміналістичної характеристики та їх використання у методиці розслідування вбивств : автореф. дис. ... канд. юрид. наук. 12.00.09 / Харків, 2004. 20 с.
12. Старушкевич А.В. Криміналістична характеристика злочинів : навч. посібник. Київ, 1997. 44 с.
13. Тищенко В.В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права* : зб. наук. праць. 2008. Вип. 44. С. 18–24.