УДК 343.132 (477)

***Олашин М. М.**, к.ю.н., доцент кафедри*
кримінального права та процесу,
Львівський торговельно-економічний університет,
м. Львів.
***Гапяк С.С.,** студент 3-го курсу Інституту права*
та психології НУЛП

КРИМІНАЛЬНІ ПРОЦЕСУАЛЬНІ АСПЕКТИ ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

***Анотація:** у статті визначено поняття права на приватність та проаналізовано новелу Кримінального процесуального кодексу України, прийнятого у 2012 році, негласну слідчу (розшукову) дію «Зняття інформації з електронних інформаційних систем». Визначено що саме відноситься до інформаційних електронних систем. Досліджено процесуальний порядок призначення та проведення негласної слідчої (розшукової) дії.*

З'ясовано особливості застосування зняття інформації з електронних інформаційних систем у Сполучених Штатах Америки та новітні розробки щодо негласного перехоплення електронної інформації. Встановлено прогалини у вітчизняному законодавстві, які стосуються зняття інформації з електронних інформаційних систем.

Запропоновано класифікацію способів отримання інформації шляхом зняття її з електронних інформаційних систем. Виокремлено найважливіші відомості, які обов'язково повинні бути вказані в протоколі негласної слідчої (розшукової) дії для визнання в подальшому такого процесуального документу в судовому провадженні.

Ключові слова: електронна інформаційна система, негласна слідча (розшукова) дія, інформація, протокол.

***Maryna Olashyn**, PhD, Associate Professor*
Department of Criminal Law and Procedure,
Lviv University of Trade and Economics, Lviv.

CRIMINAL PROCESSUAL ASPECTS TAKE OFF INFORMATION FROM ELECTRONIC INFORMATION SYSTEMS

***Abstract.** The article defines the notion of the right to privacy and analyzes the story of the Criminal Procedure Code of Ukraine, adopted in 2012, the uncensored investigation (wanted) action "Withdrawal of information from electronic information systems". It is determined what exactly relates to information electronic systems. The procedural procedure for the appointment and conducting of an unclassical investigative (wanted) action.*

The peculiarities of the application of the removal of information from electronic information systems in the United States of America and the latest

developments concerning the tacit interception of electronic information are revealed. There are gaps in the domestic legislation regarding the removal of information from electronic information systems.

The classification of ways to obtain information by removing it from electronic information systems is proposed. The most important information, which must be specified in the protocol of the unconscientious investigative (wanted) action for the further recognition of such a procedural document in the court proceeding, is set out.

Key words: electronic information system, secret investigative (wanted) action, information, protocol.

DOI: https://doi.org/10.36477/2616-7611-2018-07-25

Постановка проблеми. Прийняття нового Кримінального процесуального кодексу України, який відповідав би стандартам Ради Європи, було умовою виконання зобов'язань, взятих нашою державою. Основними напрямами реформування кримінального судочинства, відповідно до Кримінального процесуального кодексу України (далі — КПК України), прийнятого 13 квітня 2012 року є створення рівних можливостей для кожної із сторін у кримінальному провадженні та реальне впровадження у кримінальне судочинство принципу змагальності, за якого результат розгляду судом конкретного випадку притягнення особи до кримінальної відповідальності залежатиме виключно від обґрунтованості позиції сторін та доказів, отриманих на стадії досудового розслідування шляхом проведення гласних та негласних слідчих (розшукових) дій.

Активні дискусії точаться з приводу введення такого інституту кримінального провадження як негласні слідчі (розшукові) дії, що фактично викликало появу питання про співвідношення заходів оперативно-розшукової діяльності та негласних слідчих (розшукових) дій у кримінальному провадженні. Однією з таких негласних слідчих (розшукових) дій є зняття інформації з електронних інформаційних систем.

Аналіз останніх досліджень. Окремі питання застосування негласних слідчих (розшукових) дій висвітлені у працях Р.С. Веприцького, С. Є. Кучерина, М. А. Погорецького, О. І. Полюхович, Ю. Г. Севрука, М. Старовойтової, В. Г. Уварова та інших. Однак, така негласна слідча (розшукова) дія як зняття інформації з електронних телекомунікаційних систем потребує детальнішого дослідження та аналізу.

Постановка завдання. Метою цієї статті є дослідження кримінального процесуального законодавства яке регулює порядок проведення та застосування негласної слідчої (розшукової) дії "Зняття інформації електронних інформаційних систем".

Виклад основного матеріалу дослідження. У ст. 264 КПК України визначається: "Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або її частині, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в

електронній інформаційній системі або її частині, що має значення для певного досудового розслідування" [1].

Відповідно до п. 1.11.6. Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні (далі — Інструкція) — зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі [4]. Тобто, це означає що органи досудового розслідування за допомогою проведення такої негласної слідчої (розшукової) дії мають можливість отримати доступ до будь-якої інформації, яка знаходиться в комп'ютерній мережі та не доступна для загального користування, якщо така інформація може містити відомості про кримінальне правопорушення.

З таким визначенням погоджуємось частково, оскільки одержання інформації, що міститься в комп'ютерній мережі за загальним правилом повинно охоплюватись такою негласної слідчою (розшуковою) дією, як зняття інформації з транспортних телекомунікаційних мереж. Отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в тому випадку, коли жоден з елементів локальної мережі не під'єднаний до глобальної мережі [5].

Сутність такої негласної слідчої (розшукової) дії полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частинах, без відома власника, володільця або утримувача системи. Зазначена негласна слідча (розшукова) дія проводиться у разі, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування [9]. Однак, не варто виключати можливість отримання доступу органам досудового розслідування до приватної інформації особи, щодо якої здійснюється дана слідча (розшукова) дія.

Стаття 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає, що під інформаційною (автоматизованою) системою розуміється організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [3]. Окрім того, у статті використовується таке поняття, як власник електронної інформаційної системи, під яким слід розуміти фізичну або юридичну особу, якій належить право власності на електронну інформаційну систему. Володілець — фізична або юридична особа, яка має право на законних підставах фактично використовувати річ відповідно до її призначення. Утримувач — фізична чи юридична особа, яка постійно або тимчасово володіє, застосовує та несе відповідальність за використання предмета утримання [10, с. 11]. Тому залишається відкритим питання чи правомірно буде отримана інформація і чи дана інформація буде містити дані

володільця чи утримувача. Адже таким способом конституційні права одного з них будуть порушені.

Електронні інформаційні системи можуть бути як локальними, в яких всі їх компоненти (база даних, система управління базою даних, клієнтське програмне забезпечення) знаходяться на одному комп'ютері, так і розподіленими, в яких компоненти розподілені по кількох комп'ютерах.

Як локальні, так і розподілені електронні інформаційні системи можуть бути відкритими і закритими для громадян, тобто доступ до яких обмежений їх власником, володільцем або утримувачем шляхом розміщення файлових серверів та робочих станцій інформаційної системи у публічно недоступних місцях, житлі чи іншому володінні особи та встановленням систем логічного захисту доступу до електронної інформаційної системи з робочих станцій локальної мережі підприємства, установи, організації тощо, або з робочих станцій, зв'язаних з файловим сервером через мережу Інтернет [9].

Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення із застосуванням спеціальних знань та професійних спеціалістів у цій галузі, які володіють такими знаннями.

Негласне зняття інформації із засобів електронно-обчислювальної техніки полягає у застосуванні засобів спеціальної техніки із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диска (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого, що можуть містити інформацію, яка має значення у кримінальному провадженні [10, с. 11]. Відтак дана інформація має бути опрацьована і долучені тільки ті дані, які мають відношення до кримінального провадження та можуть бути доказом.

Зокрема, поява даної слідчої дії зумовлена формуванням нового типу соціальної парадигми — інформаційного суспільства.

Застосування інформаційних технологій у судочинстві має бути дозволено при виконанні будь-яких процесуальних дій як у звичайному, так і в інтерактивному (дистанційному) режимі, з одночасним веденням документообігу і діловодства на паперових та електронних носіях, з яких для учасників процесу у випадках, передбачених процесуальним законодавством, виготовляються автентичні копії процесуальних документів [8, с. 192–193].

Підставами для зняття інформації з електронних інформаційних систем є відомості, що в електронній інформаційній системі або її частині є інформація, що має значення для досудового розслідування та подальшого проведення відповідних гласних та негласних слідчих (розшукових) дій, що дозволить розкрити вчинене кримінальне правопорушення.

Частина 1 статті 264 КПК України також визначає, що відомості можуть міститися як в електронній інформаційній системі, так і в її частинах. Частинами електронної інформаційної системи, як правило, можуть бути: база даних, система управління базою даних, клієнтське програмне забезпечення тощо.

Програмне проникнення до електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують копіювання інформації, що обробляється на ПЕОМ підозрюваного, обвинуваченого, на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю негласну слідчу (розшукову) дію [9]. Комп'ютери можуть зберігати, аналізувати, кодувати і декодувати інформацію в такому об'ємі, що це все більше перетворює їх на могутній і водночас вразливий інструмент, за допомогою якого можуть здійснюватися збір і розповсюдження інформації; віртуальний простір став самостійним місцем існування людського інтелекту і, як будь-яка об'єктивна реальність, породив безліч проблем, у тому числі і правових [6, с. 28]. На сьогоднішній день немає чіткого алгоритму правового захисту персональних даних користувачів електронно-обчислювальною технікою та дієвих засобів забезпечення відшкодування шкоди, якщо вона буде заподіяна шляхом проведення таких негласних слідчих (розшукових) дій і, на нашу думку потребує швидкого вирішення шляхом внесення змін у відповідне законодавство.

Сучасні новітні технології дозволяють оперативно відстежувати діяльність злочинних угруповань на принципово іншому рівні. Так, наприклад, представляє значний інтерес досвід спецслужб США в розробці і застосуванні систем "Oasis" (ЦРУ) і "Magic Lantern" (ФБР), які уможливлюють не тільки контролювати інформаційний обмін злочинних угруповань, але і "зламувати" комп'ютери підозрюваних, упроваджувати в них "трояни" (програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері) тощо [6, с. 57].

Відповідно до чинного законодавства, зокрема, ч. 2 КПК України не передбачає дозволу слідчого судді на видобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту. Уповноваженими органами у процесі збору і фіксації інформації, що має значення для кримінального провадження, може проводитись цілеспрямований пошук серед комп'ютерних систем та мереж відкритої інформації, у тому числі всесвітньої мережі Інтернет, з метою виявлення необхідних у справі відомостей [9]. Серед великих об'ємів інформації, що локалізуються в соціальних мережах Інтернет, може бути отримана інформація щодо окремих осіб, які підозрюються в підготовці та вчиненні злочинів, їх зв'язків, та багато інших відомостей, що можуть сприяти вирішенню завдань досудового розслідування. Оскільки ця інформація є загальнодоступною, дозволу слідчого судді на її пошук та фіксацію кримінальний процесуальний закон не передбачає, через те, що не відбувається обмеження приватності спілкування окремих осіб [10, с. 12]. Як можна зрозуміти, мова йде про загально доступні чати, які не закриті та не є приватними повідомленнями.

Проведення цієї негласної слідчої (розшукової) дії без дозволу слідчого судді допускається в тому випадку коли потрібно:

- отримати інформацію розміщену особою у соціальних мережах, тематичних форумах;

- встановити ідентифікаційні ознаки електронної інформаційної системи за допомогою спеціальних програмних утиліт;

- поспілкуватися з особою за допомогою технології IRC (Internet Relay Chat) або ICQ;

- ознайомитись з інформацією на робочому комп'ютері працівника, за умови, що користувач не використовує системи логічного захисту інформації (паролі, криптографічні або інші програми захисту інформації) [10, с. 13].

Важливим є процесуальний порядок прийняття рішення про застосування такої негласної слідчої (розшукової) дії. До прикладу, в ухвалі слідчого судді про дозвіл на негласне втручання у приватне спілкування додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, у яку може здійснюватися втручання у приватне спілкування (найменування електронної інформаційної системи, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець або утримувач) та спосіб, яким обмежений доступ до неї. Ідентифікаційними ознаками електронної інформаційної системи є:

- IP-адреса (IP-Internet Protocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету;

- доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти;

- серійний номер та характеристики автоматизованої системи та ЕОМ [2, с. 150].

Зняття інформації з електронних інформаційних систем може мати як характер розвідувальної чи контррозвідувальної інформаційно-пошукової діяльності, так і характер пізнавально-фіксуючої, засвідчувальної, доказової діяльності, яка найчастіше застосовується у сфері кримінального процесуального судочинства. Але і тут також виникає питання не з законодавчим регламентуванням слідчої (розшукової) дії, а фактично лише з дозволом на її проведення. Процесуальний порядок її проведення залишається не закріпленим чинним законодавством а також відсутній регламентований порядок зберігання та знищення інформації, яка була отримана під час зняття інформації з електронних інформаційних систем, однак, не має значення для досудового розслідування.

Всі способи зняття інформації з електронних інформаційних систем можна об'єднати в дві основні групи. Перша група — це способи безпосереднього доступу. При їх реалізації інформація отримується шляхом видачі відповідних команд з комп'ютера, на якому ця інформація знаходяться. Друга група включає способи опосередкованого (віддаленого) доступу до комп'ютерної інформації. До них можна віднести:

- підключення до лінії зв'язку користувача (наприклад, до телефонної лінії або оптоволоконної лінії) і отримання цим шляхом доступу до електронної інформаційної системи;
- проникнення в комп'ютерну систему за допомогою підбору паролів тощо.

До числа способів опосередкованого (віддаленого) доступу до комп'ютерної інформації належать способи безпосереднього та електромагнітного перехоплення.

Безпосереднє перехоплення — найпростіший спосіб доступу до електронної інформаційної системи. Перехоплення здійснюється або прямо через зовнішні комунікаційні канали системи, або шляхом безпосереднього підключення до ліній периферійних пристроїв. При цьому об'єктами безпосереднього перехоплення є кабельні і провідні системи, наземні мікрохвильові системи, системи урядового зв'язку.

Зокрема, електромагнітне перехоплення являється досить цікавою річчю в руках правоохоронних органах. Сучасні технічні засоби дозволяють отримати інформацію без безпосереднього підключення до електронної інформаційної системи, за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера тощо. Всі ці дії можна вчинити перебуваючи на значній відстані від об'єкта перехоплення. Наприклад, використовуючи спеціальну апаратуру можна «знімати» інформацію з електронної інформаційної системи, розташованої в сусідньому приміщенні, будівлі. Сучасні технічні засоби дозволяють знімати і розшифрувати випромінювання працюючого принтера на відстані до 150 м., а випромінювання моніторів і з'єднувальних кабелів — до 500 м [5, с. 156–157].

Важливо підкреслити, що у протоколі негласної слідчої (розшукової) дії підлягають відображенню такі відомості:

- в пам'яті якого пристрою виявлено віртуальні сліди;
- кому належить пристрій; чи має пристрій вихід в мережу Інтернет, інші телекомунікаційні або локальні мережі;
- яка оперативна система функціонує на пристрої (Windows, Linux — на комп'ютері, Windows mobile, Android, Symbian на мобільному телефоні, комунікаторі, планшеті і т.п.);
- в яких файлах виявлені сліди втручання, які саме;
- коли файл був створений, змінений, відкривався востаннє.

Щоб уникнути вивчення кожного файлу комп'ютера (кількість файлів може вимірюватися сотнями тисяч) до проведення негласної слідчої (розшукової) дії необхідно залучати спеціаліста (програміста, системного адміністратора тощо), який може встановити спеціальні фільтри для виявлення інформації, яка може мати відношення до кримінального правопорушення, щодо якого здійснюється досудове розслідування.

Погорецький М. А. зауважує, що в умовах, коли Україна посідає одне з провідних місць у світі за рівнем корумпованості, "при реформуванні кримінально-процесуального законодавства на цьому етапі розвитку держави слід максимально звужувати можливості прийняття процесуальних рішень на

власний розсуд особами, які ведуть кримінальний процес, водночас всебічно розробляючи, розширюючи та удосконалюючи процесуальну форму. Оскільки саме недосконаліть процесуальної форми, як показує практика, є однією з причин зловживань у кримінальному процесі, а також однією з причин судово-слідчих помилок…" [7, с. 273]. Тому дотримання процесуальної форми негласної слідчої (розшукової) дії є важливим гарантом достовірності отриманої інформації (доказів) та забезпечення верховенства права, виступає запорукою захисту прав і свобод людини.

Висновки і перспективи подальших досліджень у даному напрямі. Регламентація зняття інформації з електронних інформаційні систем потребує суттєвого удосконалення, враховуючи те, що дана слідча (розшукова) дія нова і немає сталої практики її застосування, а детальна регламентація її проведення зможе хоча б трішки зменшити можливі помилки.

Підсумовуючи, варто зауважити, що зняття інформації з електронних інформаційних систем набуває широкого застосування у практиці, що зумовлено широким використанням електронної інформації у різних сферах суспільного життя, розширення сфери кримінальних правопорушень, які вчиняються за допомогою комп'ютерної техніки, а дана негласна слідча (розшукова) дія дозволяє правоохоронним органам ефективно розслідувати злочини, хоча й потребує детального дослідження та удосконалення порядку її застосування.

Література:

1. Кримінальний процесуальний кодекс України: Верховна Рада України; Кодекс України, Кодекс, Закон від 13.04.2012 р. [Електронний ресурс] — Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17
2. Кримінальний кодекс України : Верховна Рада України; Кодекс України, Кодекс, Закон від 5 квітня 2001 р. [Електронний ресурс] — Режим доступу: http://zakon2.rada.gov.ua/laws/show/2341-14
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 : [із змінами і доповненнями на 23.02.2014] // Відомості Верховної Ради України. — 1994. — №31. — Ст. 286
4. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України 16.11.2012 № 114/1042/516/1199/936/1687/5 [Електронний ресурс] — Режим доступу: http://zakon4.rada.gov.ua/laws/show/v0114900-12.
5. Луцик В. В. Зняття інформації з електронних інформаційних систем / В. В. Луцик. Електронний ресурс] — Режим доступу: https://goo.gl/Db2Cnv.

6. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. канд. юр. наук / Михальчук Т. В. — Київ, 2010.
7. Погорецький М. А. Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні / М. А. Погорецький. // Юрид. часопис Нац. акад. внутр. справ. — 2013. — № 1. — С. 270–277.
8. Сегай М. Я. Сучасна парадигма інформатизації судочинства і питання захисту прав і законних інтересів учасників кримінального процесу / М. Я. Сегай // Вісник Академії правових наук України. — 2001. — № 4. — С. 190-198.
9. Тертишник В. М. Науково-практичний коментар кримінального процесуального кодексу України [Електронний ресурс] / В. М. Тертишник // Алерта. — 2016. — Режим доступу: http://pidruchniki.com/1233090949171/pravo/kriminalniy_protsesualniy_kodeks_ukrayini_naukovo-praktichniy_komentar.
10. Уваров В. Г. Втручання у приватне життя шляхом зняття інформації з електронних інформаційних систем: новели нового КПК України та євростандарти / В. Г. Уваров. // Форум права. — 2012. — № 3. — С. 9–13.

References:

1. Kryminal’nyj protsecual’nyj kodekc Ukrainy: Verxovna Rada Ukrainy; Kodekc Ukrainy, Kodekc, Zakon vid 13.04.2012 r. [Elektronnyj recurc] — Rezhym doctupu: http://zakon5.rada.gov.ua/laws/show/4651-17
2. Kryminal’nyj kodekc Ukrainy : Verxovna Rada Ukrainy; Kodekc Ukrainy, Kodekc, Zakon vid 5 kvitnia 2001 r. [Elektronnyj recurc] — Rezhym doctupu: http://zakon2.rada.gov.ua/laws/show/2341-14
3. Zakon Ukrainy «Pro zakhyst informatsii v informatsijno-telekomunikatsijnykh systemakh» vid 5 lypnia 1994 : [iz zminamy i dopovnenniamy na 23.02.2014] // Vidomosti Verkhovnoi Rady Ukrainy. — 1994. — №31. — st. 286
4. Instruktsiia pro orhanizatsiiu provedennia nehlasnykh slidchykh (rozshukovykh) dij ta vykorystannia ikh rezul’tativ u kryminal’nomu provadzhenni, zatverdzhena Nakazom Heneral’noi prokuratury Ukrainy, Ministerstva vnutrishnikh sprav Ukrainy, Sluzhby bezpeky Ukrainy, Administratsii Derzhavnoi prykordonnoi sluzhby Ukrainy, Ministerstva finansiv Ukrainy, Ministerstva iustytsii Ukrainy 16.11.2012 № 114/1042/516/1199/936/1687/5 [Elektronnyj resurs] — Rezhym dostupu: http://zakon4.rada.gov.ua/laws/show/v0114900-12.
5. Lutsyk V. V. Zniattia informatsii z elektronnykh informatsijnykh system / V.V. Lutsyk. Elektronnyj resurs] — Rezhym dostupu: https://goo.gl/Db2Cnv.
6. Mykhal’chuk T. V. Vykorystannia informatsii, otrymanoi telekomunikatsijnym shliakhom, u rozsliduvanni zlochyniv : dys. kand. iur. nauk / Mykhal’chuk T. V. — Kyiv, 2010.

7. Pohorets'kyj M. A. Nehlasni slidchi (rozshukovi) dii: problemy provadzhennia ta vykorystannia rezul'tativ u dokazuvanni / M. A. Pohorets'kyj. // Yuryd. chasopys Nats. akad. vnutr. sprav. — 2013. — №1. — S. 270–277.
8. Sehaj M. Ya. Suchasna paradyhma informatyzatsii sudochynstva i pytannia zakhystu prav i zakonnykh interesiv uchasnykiv kryminal'noho protsesu / M. Ya. Sehaj // Visnyk Akademii pravovykh nauk Ukrainy. — 2001. — № 4. — S. 190-198.
9. Tertyshnyk V. M. Naukovo-praktychnyj komentar kryminal'noho protsesual'noho kodeksu Ukrainy [Elektronnyj resurs] / V. M. Tertyshnyk // Alerta. — 2016. — Rezhym dostupu do resursu: http://pidruchniki.com/1233090949171/pravo/kriminalniy_protsesualniy_kodeks_ukrayini_naukovo-praktichniy_komentar.
10. Uvarov V. H. Vtruchannia u pryvatne zhyttia shliakhom zniattia informatsii z elektronnykh informatsijnykh system: novely novoho KPK Ukrainy ta ievrostandarty / V. H. Uvarov. // Forum prava. — 2012. — №3. — C. 9-13.