



**Малахова О. В.,**  
кандидат юридичних наук,  
асистент кафедри кримінального процесу  
Національного університету  
«Одеська юридична академія»

## ДО ПИТАННЯ ОГЛЯДУ СТОРОНАМИ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЗМІСТУ ІНТЕРНЕТ-СТОРІНОК

Визначено можливості використання у кримінальному процесуальному доказуванні відомостей, одержаних з мережі Інтернет. Досліджено правовий порядок одержання інформації з Інтернет простору відповідно до КПК України. Проаналізовано судову практику використання у кримінальному провадженні фактичних даних, отриманих з мережі Інтернет. Запропоновано надати захиснику право проводити огляд Інтернет-сторінок, доступ до яких не обмежений. Запропоновано правовий порядок виявлення та фіксації відомостей з мережі Інтернет, доступ до яких не обмежений.

**Ключові слова:** Інтернет, доказування, огляд, захисник, змагальність.

Определены возможности использования в уголовном процессуальном доказывании сведений, полученных из сети Интернет. Исследован правовой порядок получения информации из Интернет-пространства в соответствии с УПК Украины. Проанализирована судебная практика использования в уголовном производстве фактических данных, полученных из сети Интернет. Предложено предоставить защитнику право проводить осмотр Интернет-страниц, доступ к которым не ограничен. Предложен правовой порядок выявления и фиксации сведений из сети Интернет, доступ к которым не ограничен.

**Ключевые слова:** Интернет, доказывание, осмотр, защитник, состязательность.

Сьогодні в Україні відбувається потужний розвиток інформаційних технологій, що супроводжується зростаючим рівнем використання мережі Інтернет для розповсюдження інформації. В Стратегії кібербезпеки України, що затверджена Указом Президента України від 15 березня 2016 року № 96/2016, вказується, що відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий

глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці [1]. Незважаю-

чи на стрімкий розвиток обсягів обміну інформації у Інтернет-просторі, у вітчизняній практиці залишаються невирішеними ряд правових питань щодо можливостей та особливостей використання інформації з мережі Інтернет, у кримінальному процесуальному доказуванні.

Дослідженням використання у кримінальному провадженні інформації, отриманої з мережі Інтернет, займалися такі науковці, як: Н.М. Ахтирська, С.Й. Гонгало, В.А. Динту, І.С. Краскова, А.М. Новицький, Д.В. Пашнев, Є.Д. Скулиш, О.С. Старенький, В.Г. Уваров, Д.М. Цехан та ін.

Разом з тим порядок виявлення та фіксації з Інтернет-простору відомостей, доступ до яких не обмежується, та використання їх у кримінальному процесуальному доказуванні досі залишається не врегульованим кримінальним процесуальним законодавством і малодослідженим питанням у теорії кримінального процесу.

Головною метою цієї роботи є дослідження правового порядку виявлення та фіксації сторонами кримінального провадження інформації з мережі Інтернет, доступ до якої не обмежується, в контексті змагальності кримінального провадження.

Відповідно до ст. 2 Модельного закону про основи регулювання Інтернету, Інтернет – це глобальна інформаційно-телекомунікаційна мережа, що зв'язує інформаційні системи і мережі електрозв'язку різних країн за допомогою глобального адресного простору, заснована на використанні комплексів Інтернет-протоколів (Internet Protocol, IP) і протоколу передачі даних (Transmission Control Protocol, TCP) і надає можливість реалізації різних форм комунікації, в тому числі розміщення інформації для необмеженого кола осіб [2]. Можливість використання отриманої з мережі Інтернет інформації як доказу у кримінальному провадженні визначається ст. 99 Кримінального процесуального кодексу України (далі – КПК України), відпо-

відно до якої документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [3]. До документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні). Слушно з цього приводу зазначає Н.М. Ахтирська, що законодавець допускає використання електронних носіїв інформації, проте уточнює, що доказ має бути матеріальним об'єктом. Цифрові технології використовують віртуальний простір, а тому носієм (фіксатором) інформації може бути беззаперечно матеріальний об'єкт, однак при цьому варто уточнити, що навіть сама інформація у віртуальному просторі також має визнаватися доказовою [4, с. 124].

Для того, щоб фактичні дані в подальшому могли використовуватися у кримінальному провадженні як докази, вони мають отримуватися в передбаченому процесуальним законом порядку, у протилежному випадку вони будуть визнаватися очевидно недопустимими доказами [5]. Кримінальний процесуальний кодекс України передбачає право сторони обвинувачення отримувати інформацію з Інтернет-простору шляхом проведення зняття інформації з електронних інформаційних систем (ст. 264 КПК України). Слід звернути увагу на ч. 2 ст. 264 КПК України, відповідно до якої не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Проте КПК України залишив не розкритим порядок виявлення та фіксації такої інформації. На нашу

думку, отримання з мережі Інтернет фактичних даних, доступ до яких необмежений, не може здійснюватися шляхом провадження такої дії, як зняття інформації з електронних інформаційних систем, оскільки порядок виявлення та фіксації таких відомостей не пов'язаний з подоланням захисту інформації від втручання інших осіб, а тому не відповідає суті негласної слідчої (розшукової) дії. Даний різновид інформації має виявлятися та фіксуватися шляхом проведення такої слідчої (розшукової) дії, як огляд.

Можливість здійснювати огляд веб-сторінки, з подальшим використанням результатів такого огляду як доказів, передбачена у господарському процесі України. Так, у п. 46 Постанови Пленуму Вищого Господарського суду України № 12 від 17 жовтня 2012 року «Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності» веб-сторінки з огляду на положення ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг» є електронними документами, які не можуть бути доставлені в суд; однак вони можуть містити відомості про обставини, які мають значення для справи (наприклад, якщо вони виступають об'єктами авторського права чи суміжних прав). Відтак згідно з ч. 1 ст. 32, ч. 1 ст. 36 та приписом ч. 1 ст. 39 ГПК суд з урахуванням конкретних обставин справи не позбавлений права провести огляд і дослідження цих доказів в місці їх знаходження з фіксацією відповідних процесуальних дій у протоколі, який повинен відповідати вимогам ст. 81–1 ГПК. Як засіб доказування може бути використаний відео-, аудіозапис процесу дослідження будь-якою заінтересованою особою сайта, стосовно якого є відомості використання його з порушенням авторських чи суміжних прав; такий запис, здійснений на електронному чи іншому носії (жорсткому диску комп'ютера, дискеті, диску для лазерних систем зчитування, іншому носії інформації), подається до суду із за-

значенням того, коли, ким і за яких умов цей запис здійснено і може бути речовим доказом у справі. Письмовими доказами можуть бути також довідки, отримані від провайдерів і мережевих пошукових служб [6]. Окрім того, в Україні є законодавча ініціатива щодо огляду нотаріусом змісту веб-сторінок для забезпечення доказів в Інтернеті. Так, Проект Закону про внесення змін до деяких законодавчих актів України щодо захисту авторського права і суміжних прав у мережі Інтернет від 23 жовтня 2015 р. № 3353 передбачає доповнення Закону України «Про нотаріат» положенням, відповідно до якого на звернення заінтересованих осіб нотаріус має право забезпечувати докази в Інтернеті; забезпечення доказів в Інтернеті здійснюється шляхом складення нотаріусом відповідного протоколу, що містить опис інформації, розміщеної в Інтернеті, та до якого додаються документи, в яких зафіксована інформація, розміщена в Інтернеті [7]. Подібна норма закріплена в Законі Республіки Білорусь від 18 липня 2004 року «Про нотаріат і нотаріальну діяльність». Так, відповідно до ч. 2 ст. 96–2, ч. 2 ст. 96–4 зазначеного Закону, в порядку забезпечення письмових доказів нотаріус проводить огляд письмових доказів, наданих особою, яка звернулася за вчиненням нотаріальної дії, в тому числі загальнодоступної інформації, записаної буквами або виконаної у формі цифрового, графічного запису, розміщеної в глобальній комп'ютерній мережі Інтернет. Такий огляд фіксується протоколом [8].

Незважаючи на те, що КПК України не передбачає процесуального порядку проведення огляду змісту Інтернет-сторінок, аналіз судової практики дає підстави зробити висновок, що такий огляд проводиться стороною обвинувачення під час досудового розслідування. Так, у вироку Соснівського районного суду м. Черкаси від 17 лютого 2016 року вказано, що вина обвинуваченого у вчиненні кримінальних правопорушень, передбачених ч. 2 ст. 258–5, ч. 2 ст. 110,

ч. 2 ст. 109 КК України, підтверджується: актом огляду від 8 липня 2014 року з додатком згідно з даними якого користувач соціальної мережі «Вконтакте» з логіном «Мах Іvко» розміщував на своїй сторінці заклик щодо дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади; протоколами огляду сторінки з логіном «Мах Іvко» соціальної мережі «Вконтакте» та груп адміністрування яких здійснюються зі сторінки з логіном «Мах Іvко» від 16 липня 2014 року; від 22 липня 2014 року з додатком, від 08 серпня 2014 року, від 04 вересня 2014 року, від 07 вересня 2014 року, згідно з даними яких ОСОБА\_2 здійснював матеріальне забезпечення терористичної організації «ІНФОРМАЦІЯ\_1», шляхом збору та направлення матеріальної допомоги у вигляді: цивільного та військового одягу і медичних препаратів та виробів медичного призначення, представникам вказаної терористичної організації для послідуного її використання (т. 2 а. п. 1–21, а. п. 22–41, а. п. 42–44, а. п. 45–49, а. п. 62, т. 2) [9]. Окрім того, у судовій практиці є приклади використання відомостей, отриманих з мережі Інтернет, для підтвердження факту вручення особі повістки про виклик або ознайомлення з її змістом. Так, ухвалою слідчого судді Печерського районного суду м. Києва від 28 листопада 2014 року було надано дозвіл на здійснення приводу підозрюваного ОСОБА\_3, який в судове засідання не з'явився з причин, які слідчим суддею були визнані як неповажні. Однією із підстав такого рішення був рапорт, в якому зазначено, що переглядом сторінки в мережі Інтернет «Фейсбук» встановлено, що гр. ОСОБА\_3 знає про те, що СВ Печерського РУ ГУ МВС України в м. Києві відкрито кримінальне провадження і з даного приводу він викликається, але останній коментує свої виклики до правоохоронних органів і викладає вручені йому повістки на своїй сторінці в мережі «Фейсбук» [10]. Про проведення стороною обвину-

вачення огляду змісту Інтернет-сторінок і використання такої інформації у процесі доказування вказується також й в інших вироках [11–14]. Вважаємо, що така практика відповідає сучасним реаліям кримінального судочинства в умовах розвитку інформаційних технологій. Зважаючи на те, що законодавець не визначив порядку провадження огляду змісту Інтернет-сторінок, який би враховував специфіку досліджуваного об'єкта, видається за доцільне доповнити КПК України відповідною правовою нормою.

У зв'язку зі стрімким ростом Інтернет-технологій вважаємо за необхідне також передбачити право сторони захисту здійснювати огляд веб-сторінок, доступ до яких не обмежується власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, з метою забезпечення використання у процесі доказування такого роду виправдувальної інформації. Закріплення за стороною захисту права проводити таку процесуальну дію сприятиме подоланню декларативного характеру основ змагальності кримінального провадження, оскільки виключить необхідність звернення підозрюваного, його захисника до сторони обвинувачення з клопотанням про проведення огляду веб-сторінки, а також залежність від рішення слідчого, прокурора використання виправдувальних доказів, отриманих з мережі Інтернет, у кримінальному процесуальному доказуванні. Враховуючи те, що огляд – це слідча (розшукова) дія, яка має бути проведена з чітким дотриманням процесуальної форми, вважаємо, що дану дію може проводити виключно професійний учасник кримінального провадження, яким зі сторони захисту є адвокат-захисник.

Відповідно до чинного кримінального процесуального законодавства України проведення будь-якої слідчої (розшукової) дії повинно супроводжуватися протоколюванням. Не є винятком і огляд Інтернет-сторінок. У нормах КПК України не передбачена можливість складан-

ня протоколу захисником. Належний порядок фіксації проведення процесуальної дії є одним із критеріїв допустимості доказів, отже, для того, щоб одержані стороною захисту фактичні дані в подальшому могли бути використані як допустимі докази, вважаємо за доцільне передбачити право сторони захисту складати протокол, виклавши п. 11 ч. 3 ст. 42 КПК України у такій редакції: «11) під час проведення процесуальних дій, що передбачені ч. 3 ст. 93 цього Кодексу, складати протокол і застосовувати з додержанням вимог цього Кодексу технічні засоби при проведенні процесуальних дій, в яких він бере участь». Складений захисником в результаті огляду Інтернет-сторінок протокол з дотриманням вищевказаної процедури має визнаватись допустимим доказом і може використовуватися на підтвердження чи спростування обставин, що мають значення для кримінального провадження.

В протоколі огляду змісту веб-сторінок, окрім відомостей, що зазначені в ст. 104 КПК України, обов'язково має вказуватись інформація про доменне ім'я, а також IP-адреси з DNS-серверу. Вважаємо, що огляд Інтернет-сторінок повинен супроводжуватися застосуванням безперервного відеозапису. До про-

токолу огляду слідчий, прокурор, захисник зобов'язані надати роздруковану веб-сторінку та її скріншоти на електронному носії.

Подальший процес реформування кримінального процесуального законодавства України повинен здійснюватися з урахуванням розвитку технічних можливостей використання Інтернет-простору. Для того, щоб отримані з мережі Інтернет відомості, доступ до яких не обмежений, використовувалися у кримінальному провадженні як допустимі докази, необхідно доповнити ст. 237 КПК України частиною 8 у наступній редакції: «Огляд веб-сторінки проводиться слідчим, прокурором, захисником, якщо доступ до неї не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Про проведення огляду веб-сторінки складається протокол згідно з вимогами цього Кодексу. Крім того, у протоколі вказується доменне ім'я, а також IP-адреси з DNS-серверу. До протоколу огляду веб-сторінки додаються роздрукована веб-сторінка та її скріншоти на електронному носії. Під час огляду веб-сторінки слідчий, прокурор, захисник зобов'язаний застосовувати безперервний відеозапис проведення огляду».

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]: Указ Президента України від 15 берез. 2016 р. № 96/2016. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/96/2016>.
2. Модельный закон об основах регулирования Интернета от 16 мая 2011 г. [Электронный ресурс]. – Режим доступа: [http://zakon2.rada.gov.ua/laws/show/997\\_o14](http://zakon2.rada.gov.ua/laws/show/997_o14).
3. Кримінальний процесуальний кодекс України від 13 квіт. 2012 року (із змінами та доповненнями) // Відомості Верховної Ради України. – 2013. – № 9–10, 11–12, 13. – Ст. 88.
4. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження / Н. М. Ахтирська // Науковий вісник Ужгородського національного університету. Серія: Право. – 2016. – Вип. 36(2). – С. 123–125.
5. Про деякі питання порядку здійснення судового розгляду в судовому провадженні у першій інстанції відповідно до Кримінального процесуального кодексу України [Електронний ресурс]: Інформаційний лист Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 5 жовт. 2012 р. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/v1446740-12>.
6. Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності [Електронний ресурс]: постановою Пленуму Вищого Господарського суду України № 12 від 17 жовт. 2012 р. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/v0012600-12>.
7. Про внесення змін до деяких законодавчих актів України щодо захисту авторського права і суміжних прав у мережі Інтернет [Електронний ресурс]: проект Закону України від 23 жовт. 2015 р. № 3353. – Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=56869](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=56869).

8. О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам нотариальной деятельности [Электронный ресурс]: Закон Республики Беларусь от 4 янв. 2014 г. № 105-3. – Режим доступа: [http://www.pravo.by/upload/docs/op/H11400105\\_1389387600.pdf](http://www.pravo.by/upload/docs/op/H11400105_1389387600.pdf).

9. Вирок Соснівського районного суду м. Черкаси 17 лют. 2016 р. (справа № 712/8363/15-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/56349134>.

10. Ухвала слідчого судді Печерського районного суду м. Києва від 28 листоп. 2014 р. (справа № 757/35248/14-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/54843539>.

11. Вирок Жовтневого районного суду м. Кривого Рогу від 17 берез. 2014 року (справа № 212/1921/14-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/37722075>.

12. Вирок Олександрійського міськрайонного суду Кіровоградської області від 1 квіт. 2015 р. (справа № 398/1423/15-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/43772579>.

13. Вирок Ужгородського міськрайонного суду Закарпатської області від 30 верес. 2013 р. (справа № 308/13872/13-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/33963118>.

14. Вирок Ужгородського міськрайонного суду Закарпатської області від 9 груд. 2015 р. (справа № 308/9944/15-к) / [Електронний ресурс]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/54286731>.

---

**Malakhova O. To the issue of inspection of Internet pages' content by the parties of criminal proceedings**

*The article is devoted to research of the legal order of the use of information obtained from the Internet, in the criminal procedural proving. It was determined that the Criminal Procedural Code of Ukraine does not provide a legal identification and recording of information from web pages the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection. The receipt of such information cannot be accessed by removing Collecting information from electronic information systems, because the procedure for identifying and fixing such data are not associated with overcoming the protection of information from interference by other persons, and therefore not to the essence of covert investigative (detective) actions. This type of information should be identified and recorded by conducting such investigative (search) actions, as inspection. Analysis of judicial practice gives reason to conclude that the prosecution inspects the content of web pages during the pre-trial investigation, despite the fact that the criminal procedure code of Ukraine does not provide a procedure for this operation. The adversarial nature of criminal proceedings necessitates to provide the right of defender to inspect web pages the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection. The course and results of inspection of web pages shall be entered in the record. Therefore, it is necessary to give the defender the right to make the record. Inspection of web pages shall be accompanied by continuous video recording. Investigator, prosecutor, defender must provide a printed web page and its screenshots on an electronic device to record of inspection.*

**Keywords:** *Internet, proving, inspection, defender, adversarial.*

*Стаття надійшла до редакції журналу 14.04.2017 р.*