В. Л. Федоренко
директор Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, доктор юридичних наук, професор, заслужений юрист України

О. К. Собін
завідувач Лабораторії авторського та суміжних прав Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України

ІНФОРМАЦІЯ ЯК ДОКАЗ, АБО ЯК ЗАХИЩАТИ СВОЇ ПРАВА, ЧЕСТЬ І ГІДНІСТЬ В ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ

Інформація має давню історію, яка збігається з історією людства. Власне, про останню ми знаємо також завдяки інформації, яка в усі епохи була важливим складником цивілізації й важливою суспільною цінністю. З кожним роком цінність інформації зростає, а її частка в життя суспільства та держави невпинно зростає. Так, XXI ст. справедливо називають епохою інформаційного суспільства.

Відомий австралійський учений Дж. Кін пише, що революційна епоха комунікаційного добробуту символізується Інтернетом. «Уперше в історії ці прилади, створені на базі дешевих мікропроцесорів, об'єднують тексти, звуки і образи у цифровій, компактній формі, що легко зберігається, відтворюється та траспортується»* ,– пише Дж. Кін.

Дійсно, на сьогодні не залишилось жодної галузі суспільного та державного життя, яка б не була охоплена інформатизацією та не використовувала потенціал глобальної мережі Інтернет: потужні програмно-апаратні комплекси, які здійснюють державну реєстрацію рухомого та нерухомого майна тощо, соціальні мережі, інтернет-магазини, платформи для поширення аудіо- та відеоінформації, онлайн-кінотеатри тощо.

Нині інформація в глобальній мережі Інтернет з'являється та поширюється блискавично. Більшість із нас не лише споживають, а й поширюють її. Репости стали правилом гарного тону для багатьох соціальних груп і середовищ, у тому числі й професійних. Судді, адвокати, нотаріуси, юрисконсульти, правозахисники і вчені правознавці діляться новелами чинного законодавства та правозастосовної практики і коментарями до них, свіжими публікаціями фахового характеру, пишуть відгуки про переваги і недоліки діяльності колег тощо.

* Кин Дж. Демократия и декаданс медиа / Дж. Кин ; пер. с англ. Д. Кралечкина ; под ред. А. Смирнова. – М. : Изд-ий дом Высшей школы экономики, 2015. – С. 8-9.

За свідченням Дж. Гліка, Бібліотека Конгресу США, створена для того, щоб збирати усі книги, вирішила зберігати і всі твіти. Можливо, недостойні та, ймовірно, такі, що повторюються, але наперед ніхто не знає. І Мережа навчилась деяким речам, які ніколи нікому не були відомими. Вона ідентифікує музичний компакт-диск за довжиною окремих треків, порівнюючи їх з об'ємною базою даних, яка роками формувалась за рахунок доповнень, спільних внесків мільйонів анонімних користувачів*. Тобто глобальна мережа Інтернет раз і назавжди змінила ландшафт світового інформаційного простору.

Однак доступність і інтенсивність спілкування людей у соціальних мережах нерідко призводить до того, що гарантовану ст. 15 Конституції України заборону цензури користувачі глобальної мережі Інтернет сприймають як заохочення до розміщення будь-якої інформації, у тому числі й такої, що порушує честь і гідність, права та свободи інших людей, наносить збитки діловій репутації фізичних і юридичних осіб. Доволі часто дописувачі соціальних мереж розміщують, або поширюють завідомо недостовірну, або неперевірену інформацію. При цьому причиною цього може бути як недбалість, так і сумнівні стратегії недобросовісної боротьби з конкурентами.

Глобальна мережа Інтернет також надає можливість розміщувати не лише будь-яку інформацію, а й зберігати анонімність, миттєво знищувати первинну інформацію після її поширення, породжуючи численні симулякри і фейки. Нині таке цілеспрямоване маніпулювання інформацією в Інтернеті перестало бути захопленням окремих аматорів, а трансформувалося в системну, професійну й оплачувану діяльність. Сама ж глобальна мережа Інтернет дозволяє робити масові лавиноподібні, або ж навпаки – точкові, розсилки інформації за допомогою т. зв. «ботів». За даними інтернет-ресурсу «ВВС.Україна», компанія ImpervaIncapsula проаналізувала і встановила, що у 2016 році 52% інтернет-трафіку згенерували боти, а реальні користувачі – 48% (http://www.bbc.com/ukrainian/news-38882435).

Практика розміщення та поширення різноманітної інформації в глобальній мережі Інтернет породжує численні спори, які стають предметом цивільної, господарської, адміністративної і навіть кримінальної юрисдикції в Україні. Чого лише варта «гібридна війна» в інформаційному просторі України з боку РФ у 2016-2017 рр.!

Тому у фізичних і юридичних осіб час від часу виникає нагальна потреба використати інформацію, що розміщена у глобальній мережі Інтернет, як доказову базу в суді або при проведенні досудового розслідування. Ідеться про докази щодо порушення честі і гідності людини, авторських прав або прав на торговельну марку, винахід чи корисну модель, а також щодо недобросовісної конкуренції тощо. У цьому випадку перед позивачами постає відразу два питання – як зробити інформацію, розміщену в глобальній мережі Інтернет, доказом і що слід зробити, щоб цей доказ не втратився після вилучення відповідної інформації з Інтернету?

Відповідь на це питання існує. Науково-дослідний центр судової експертизи з питань інтелектуальної власності Міністерства юстиції України уже декілька років поспіль проводить дослідження телекомунікаційних систем (обладнання) та засобів у формі документальної фіксації вмісту веб-сторінки (ресурсу/посилання), розміщеного в глобальній мережі Інтернет, а також вмісту інформаційного джерела (персонального комп'ютера, ноутбука, телефона тощо). Головним критерієм проведення такого дослідження є його повнота, об'єктивність та оперативність. Адже відповідні матеріали, розміщені на веб-ресурсі, чи вміщені в комп'ютері, ноутбуці або телефоні, з часом, а іноді й за лічені хвилини, можуть бути спотворені, знищені, або просто втрачають свою актуальність.

Іноді потенційні позивачі, – фізичні та юридичні особи, – звертаються до нотаріусів для оформлення відповідної доказової бази, яка може бути використана в судовому процесі. Натомість, існуюча практика засвідчує, що нотаріальне завіреня графічного відображення вмісту ресурсу (скріншоту) є неоднозначним підходом. Адже фіксація вмісту веб-ресурсу – це не лише його графічне відображення на папері. Для проведення повної та об'єктивної фіксації вмісту веб-ресурсу необхідний комплексний дослідницький підхід, застосування спеціальних знань та експертних навичок, із обов'язковим дослідженням програмного коду, маршрутизації, трафіку тощо. Це, у свою чергу, вимагає від атестованих судових експертів наступних етапів проведення експертного дослідження: 1) перевірку атрибутів доменного імені на час проведення експертного дослідження; 2) перевірку можливостей з'єднання з веб-ресурсом (з'ясування можливості подальшого дослідження вмісту, «пінг»); 3) виявлення та фіксація даних прореєстранта доменного імені, компанії, що надають послуги з хостингу тощо (зокрема,за допомогою сервісу Whois); 4) визначення IP-адреси веб-ресурсу; 5) пошук за заданими

* Глик Дж. Информация. История. Теория. Поток. / Джеймс Глик. ; пер. с англ. М. Кононенко. – М. : Изд-во АСТ : CORPUS, 2016. – С. 446-447.

параметрами та фіксація повного вмісту досліджуваного веб-ресурсу; 6) дослідження вихідного коду/тексту ресурсу (перевірка на втручання, модифікацію, редирект); 7) дослідження можливості/наявності редиректу (переадресації); 8) фіксацію вмісту веб-ресурсу, а саме даних у текстовому, графічному та інших мультимедійних форматах на матеріальному носії (із зазначенням метаданих з обов'язковим визначенням контрольної суми (хешу); 9) фіксацію повного шляху маршрутизації даних (наприклад, при дослідженні листування за допомогою поштових сервісів); 10) фіксацію розгорнутих часових показників архіву (кешу).

Отриманий за результатами експертного дослідження контент, як у вигляді скріншотів або текстових форматів, так і у формі вивантажених електронних файлів (документів), оформлюється у вигляді висновку судового експерта. У цьому разі позивач подає до суду не скріншот матеріалів, розміщених у глобальній мережі Інтернет, а висновок судового експерта, за результатами експертного дослідження чи експертизи, проведеній у науково-дослідній установі судової експертизи (НДУСЕ) Міністерства юстиції України. Такий висновок судового експерта може слугувати надійною доказовою базою у судовому процесі або ж – серйозно посилює позиції позивача у разі застосування медіаційних процедур при вирішенні спорів у досудовому порядку.

Іншою нагальною проблемою, яка виникла разом з активним листуванням за допомогою мережі Інтернет, є розповсюдження через електронні листи шкідливого програмного забезпечення, замаскованого під текстові або графічні файли. Як відомо, шкідливе програмне забезпечення – це таке програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до комп'ютерних систем. Може проявлятися у вигляді коду, скрипту, активного контенту та іншого програмного забезпечення. До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, додзвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни, шифрувальники та інше зловмисне програмне забезпечення.

Таке шкідливе програмне забезпечення може завдати значної школи не лише користувачеві локального ЕОМ, а й великим програмно-апаратним комплексам, що розташовані в органах державної влади та органах місцевого самоврядування, в установах, організаціях або на підприємствах, незалежно від форм їх власності. Це наочно продемонстрували у липні цього року в Україні масштабні атаки вірусу Petya.A. на комп'ютерні мережі та програмно-апаратні комплекси органів державної влади і органів місцевого самоврядування, а також різних підприємств, установ, організацій. У більшості випадків устаткування, що постраждало від вірусної атаки, стало непридатним для подальшого використання.

Досвіду упередження подібних масивних кібератак, а також конструктивного реагування на їх наслідки, зокрема, збитки, нанесені вірусами, в Україні фактично немає. Він лише напрацьовується на всіх ланках механізму забезпечення інформаційної безпеки. Але що ж робити державним органам та органам місцевого самоврядування, підприємствам, установам, організаціям, незалежно від форм їх власності, які вже стали жертвами атаки вірусу Petya.A.? Як можна зафіксувати факт технічного стану програмно-апаратного устаткування або обладнання (програмно-апаратного комплексу, програм, локального ЕОМ, мережевого обладнання тощо) після атаки вірусу Petya.A.? Адже у багатьох випадках програмно-апаратне устаткування та обладнання відповідних суб'єктів стає частково або повністю непридатним для подальшого використання. Відповідно, його треба знімати із балансу суб'єктів господарювання та заміняти новим. У необхідності юридичної бездоганності цих процедур, очевидно, немає потреби переконувати.

У таких випадках проведення спеціального експертного дослідження, спрямованого на перевірку та фіксацію технічного стану устаткування або обладнання, дозволяє отримати документальне підтвердження факту, який дозволяє легітимно замінювати програмно-апаратні комплекси, програми, локальні комп'ютери, мережеве обладнання тощо. Судовими експертами НДУСЕ Міністерства юстиції України (а саме НДУСЕ мають право здійснювати дослідження та експертизи за спеціальностями 10.9 – «Дослідження комп'ютерної техніки та програмних продуктів» і 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів») такі експертні дослідження проводяться в рамках комплексного комп'ютерно-технічного та телекомунікаційного дослідження, із використанням спеціалізованого програмного забезпечення та спеціальних методів дослідження.

За результатами цього дослідження надається висновок судового експерта НДУСЕ, що засвідчує факт пошкодження програмно-апаратного комплексу, програми, локального комп'ютера чи ноутбука, мережевого обладнання, що постраждало від некоректного використання або дій шкідливого програмного забезпечення, засвідчує факт втрати інформації, яка розміщувалась на відповідному обладнанні тощо. Можна встановити й факт про непошкодження локального комп'ютера чи ноутбука, мережевого обладнання, яке працівники прагнуть змінити без підстав, у межах компанії з поновлення спеціального обладнання та устаткування після атаки вірусу Petya. A. ■