УДК 343.9:519.72+351.74

Гавловський Владислав Данилович –
начальник відділу Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук,

Тітуніна Катерина Вікторівна –
науковий співробітник відділу Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України

Деякі сучасні проблеми протидії комп'ютерній злочинності та комп'ютерному тероризму

У статті розглядаються окремі організаційно-правові питання взаємодії правоохоронних органів України з провайдерами та операторами зв'язку при протидії комп'ютерній злочинності та комп'ютерному тероризму в Україні.

На сучасному етапі спостерігається зростання проявів комп'ютерної злочинності, внаслідок чого вона набуває все більш масштабного характеру та носить транснаціональний характер. Відбувається процес формування транснаціональних організованих злочинних груп, які здійснюють протиправну діяльність у мережі Інтернет. Разом з тим, новітні технології все частіше використовуються терористичними організаціями в усьому світі. Так, терористичні організації активно використовують мережу Інтернет як засіб пропаганди своїх ідей, прихованого фінансування своєї діяльності, зв'язку між своїми членами тощо.

Зазначене, з урахуванням постійного відставання рівня забезпечення захисту інформації в інформаційних та інформаційно-телекомунікаційних системах вітчизняних суб'єктів інформаційної діяльності від методів скоєння комп'ютерних злочинів, а також досить частої слабкої підготовки персоналу, який їх обслуговує, не виключає можливості створення передумов до проведення акцій комп'ютерного тероризму та виникнення надзвичайних подій на об'єктах підвищеної небезпеки, промисловості, транспорту, зв'язку тощо.

Для підвищення ефективності заходів з протидії комп'ютерній злочинності та комп'ютерному тероризму в Україні необхідно створювати умови для реалізації правоохоронними органами оперативно-розшукових, технічних заходів та інших видів документування протиправної діяльності.

В цьому контекстному питанні особливу увагу слід приділити відсутності достатнього рівня взаємодії між правоохоронними органами та приватним бізнесом (телекомунікаційними компаніями та компаніями, що надають послуги Інтернет) з питань надання необхідної інформації (доказів у електронному вигляді) та її збереження в комп'ютерних системах.

Сьогодні в Україні у питаннях взаємодії між провайдерами, операторами зв'язку та правоохоронними органами основним регулюючим документом стала Постанова Пленуму Верховного Суду України № 2 від 28 березня 2008 р. "Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства" [1], якою роз'яснюється порядок застосування судами законодавства України, яке

регулює порядок надання дозволу на проникнення до житла чи іншого володіння особи, зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією, застосування інших технічних засобів одержання інформації, пов'язане з обмеженням конституційних прав громадян. Але ця Постанова сьогодні не вирішує ту низку проблем, що виникла.

З метою вирішення проблеми адекватної протидії новим викликам і загрозам у цій сфері, потрібно внести відповідні зміни до національного законодавства.

У країнах Західної Європи, США та деяких країнах СНД основні акти законодавства у сфері протидії комп'ютерним збули прийняті у 2001–2005 роках лише у відповідь на прояви міжнародного та регіонального тероризму: Акт патріота-2001 у США, який передбачає моніторинг мереж та плідну взаємодію між операторами та провайдерами зв'язку; Стратегія з питань боротьби з кіберзлочинністю у Франції, метою якої є співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з обміну інформацією та питаннях в об'єднанні зусиль у боротьбі з кіберзлочинністю; Проект "СОРМ" у Росії тощо. Виходячи з транскордонності, організованості, швидкоплинності та латентності комп'ютерних злочинів та проявів комп'ютерного тероризму, основними загальновизнаними напрямами розвитку законодавства за кордоном є:

– введення у національне законодавство вимог, що дозволяють здійснювати авторизацію усіх користувачів Інтернету;

– спрощення процедур документування правоохоронними органами протиправної діяльності у сфері кіберзлочинності;

– встановлення додаткових вимог до провайдерів телекомунікацій та суб'єктів, що надають послуги колективного доступу до мережі Інтернет, у частині забезпечення збереження даних про трафік від 6 місяців до 3 років, а також забезпечення належного та прозорого для правоохоронних органів рівня контролю за користувачами мережі Інтернет (у тому числі, за відвідувачами пунктів колективного доступу);

– виконання державними органами заходів щодо блокування шкідливого або протиправного контенту.

Однак, незважаючи на загострення нових викликів і загроз, підходи, які на сьогодні застосовуються при виконанні завдань у згаданій сфері в Україні, негативно різняться з загальносвітовою практикою, що негативно впливає на стан інформаційної безпеки держави.

З огляду на вказане, існує необхідність приведення діяльності операторів і провайдерів телекомунікацій у відповідність до вимог сучасності та міжнародних актів, ратифікованих Верховною Радою України.

Зокрема, необхідно чітко прописати на законодавчому рівні не тільки права, але й обов'язки операторів та провайдерів телекомунікацій, які б відповідали положенням Декларації про свободу комунікацій в мережі Інтернет, затвердженої Комітетом Міністрів на 840-му засіданні заступників міністрів Ради Європи 28 травня 2003 року в м. Страсбурзі (Франція) [2], Конвенції Ради Європи про кіберзлочинність [3], Додаткового протоколу відносно криміналізації дій расистського і ксенофобного характеру, що здійснюються за допомогою комп'ютерних мереж [4], Директиви 2000/31/ЄС Європейського парламенту та Ради (Директива про електронну комерцію) [5]. Вказані міжнародні нормативні акти необхідно покласти в основу розробки власної законодавчої бази в інформаційній сфері та сфері комп'ютерних технологій.

Так, Конвенцією Ради Європи про кіберзлочинність встановлені наступні обов'язкові вимоги для врахування у законодавстві країн, які приєдналися:

– надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які необхідні для розкриття злочину (ч. 1 ст. 16 та ст. 17 Конвенції про кіберзлочинність);

– збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16 Конвенції про кіберзлочинність);

– встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язань не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, який визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції про кіберзлочинність);

– розкриття провайдером в інтересах органу дізнання або слідства технічної інформації, достатньої для ідентифікації підприємств чи фізичних осіб, що надавали послуги, та шлях, яким інформація передавалась (ч. 1 ст. 17 Конвенції про кіберзлочинність);

– надання органам дізнання та слідства права терміново здійснити обшук (огляд, виїмку) комп'ютерної інформації [3].

Пропонується доповнити Закон України "Про телекомунікації" положеннями, задекларованими у частині 4 (ст. 12–15) вищевказаної Директиви Європейського парламенту № 2000/31/ЄС, а на операторів телекомунікацій покласти відповідальність за збережену, передану та отриману інформацію, лише у випадках, за яких вони мають можливість впливати на зміст та наповнення інформаційних повідомлень, а також за ненадання правоохоронним органам інформації про підозрілу незаконну діяльність, що здійснюється з використанням інформаційної складової.

На сьогодні необхідність реєстрації установочних даних абонентів операторів мобільного зв'язку та операторів телекомунікацій закріплена на юридичному рівні багатьох європейських країн. Така реєстрація використовується безпосередньо для прив'язки мобільних номерів, IP-адрес та інших ідентифікаторів до фізичних і юридичних осіб з метою документування можливих порушення чинного законодавства і притягнення конкретних осіб до відповідальності без проведення довгострокових оперативно-розшукових заходів по їх виявленню та документуванню протиправності в їхніх діях. Аналогічні підходи необхідно запроваджувати і в Україні.

З огляду на досвід провідних європейських країн, необхідно також внести зміни до відповідних нормативно-правових актів (у т. ч. внутрішніх), що стосуються необхідності створення єдиної бази даних усіх наявних абонентів операторів телекомунікацій, яка б розміщувалась на захищеному сервері в МВС України та адмініструвалась відповідним підрозділом. Використання цієї бази даних суттєво зменшить час встановлення особи зловмисників при проведенні оперативно-розшукових заходів, а також унеможливить завчасне виявлення злочинцями відповідного інтересу до них з боку правоохоронних органів, що на сьогодні є характерним у разі офіційного звернення до оператора або провайдера телекомунікацій.

Таким чином, імплементація до національного законодавства положень Конвенції Ради Європи про кіберзлочинність та інших наведених нормативно-правових актів, розроблення на їх основі відповідної нормативно-правової бази в Україні, надасть можливість забезпечити на міждержавному та внутрішньодержавному рівні взаємодію та координацію з протидії комп'ютерній злочинності за наступними напрямами:

– правоохоронні органи та спеціальні служби, з чітким нормативно-правовим закріпленням розмежування їх повноважень, з метою запобігання дублювання функцій;

– громадські та приватні структури (фонди, асоціації, служби безпеки фінансових, банківських і комерційних структур), що здійснюють практичні заходи щодо забезпечення безпеки і захисту інформації, яка оброблюється в електронній формі, з державними структурами, що здійснюють протидію комп'ютерній злочинності;

– обмін інформацією між правоохоронними органами України і міжнародними організаціями та іноземними правоохоронними органами, що ведуть боротьбу з комп'ютерною злочинністю;

– надання необхідної інформації (доказів у електронному вигляді) та її збереження в комп'ютерних системах з боку приватного бізнесу (телекомунікаційних компаній та компаній, що надають послуги Інтернет) правоохоронним органам.

Список використаних джерел

1. *Про деякі питання* застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства. Постанова Пленуму Верховного Суду України № 2 від 28 березня 2008 р. <http://www.scourt.gov.ua/clients/vs.nsf/0/EC7A77690 6EDFD5DC225742F003D4548?OpenDocument&CollapseView&RestrictToCategory=EC7A7769 06EDFD5DC225742F003D4548&Count=500&>.

2. *Інформаційне* законодавство: Збірник законодавчих актів: У 6 т. / За заг. ред. Ю.С. Шемшученка, І.С. Чижа. – Т. 5. Міжнародно-правові акти в інформаційній сфері. – К.: ТОВ "Видавництво "Юридична думка", 2005. – 328 с.

3. *Конвенція* Ради Європи про кіберзлочинність <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi? page=1&nreg=994_575>.

4. *Додатковий* протокол до Конвенції Ради Європи про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi? nreg=994_687>.

5. *Про деякі правові* аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку ("Директива про електронну комерцію"). Директива Європейського парламенту та Ради 2000/31/ЄС від 8 червня 2000 року <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi? nreg=994_224>.

The article is dedicated to the examination of some organizational legal questions of co-operation of law enforcement bodies of Ukraine with the providers and operators of connection in counteraction of computer crime and computer terrorism in Ukraine.

Стаття надійшла до редакції журналу 25 грудня 2008 року.