УДК 004.738.5:347.122(477)

О. І. ГОРОШКО
доктор філологічних наук, професор,
завідувач кафедри міжкультурної комунікації та іноземної мови
Національного технічного університету «Харківській політехнічний інститут»

ПРОБЛЕМИ БЕЗПЕКИ ФУНКЦІОНУВАННЯ ІНТЕРНЕТУ В УКРАЇНІ

Інтернет став невід'ємною частиною нашого повсякдення. У 2008 р. вже кожен шостий мешканець України був користувачем мережі Інтернет. Кількість сайтів у мережі зростає в середньому від 40 до 60 сайтів на день [1]. У зв'язку з цим проблема інформаційної (і не тільки) безпеки в Інтернеті стає дедалі більш актуальною [2; 3; 4].

Слід окремо наголосити, що поява новітніх технологій у нашому житті впливає на юридичну практику неоднозначно. З одного боку, створюються можливості для вчинення за допомогою новітніх інформаційно-комунікаційних технологій (далі – ІКТ) дій, які порушують захищені законом права інших осіб. З іншого боку, виникають цілком нові, які не існували раніше, законні інтереси, які також вимагають захисту, а отже, і подальшої розробки законодавства в цьому напрямку [5].

Законодавство кожної країни має свої специфічні особливості, однак можна виділити ряд спільних моментів, характерних для країн «західної» демократії, де ІКТ розвинені найбільш потужно.

Так, правопорушення у сфері ІКТ зазвичай класифікують за трьома основними напрямками:

– правопорушення, метою яких є інформаційно-комунікаційні об'єкти;

– правопорушення в комп'ютерній сфері;

– кіберзлочини [5; 6].

Перший тип правопорушень мало відрізняється від передбачених будь-яким кримінальним законодавством випадків розкрадань, крадіжок, незаконного привласнення майна, порушень недоторканності особистого життя людини тощо. Їх особливістю є лише те, що об'єктом цих протизаконних дій є самі ІКТ. Якщо хтось розбиває чужий комп'ютер, завдаючи по ньому удари, то таке правопорушення буде розглядатися як «заподіяння матеріальних збитків», а викрадення вінчестера – як крадіжка й порушення недоторканності приватного життя тощо.

Другий тип правопорушень охоплює собою як дії з використанням комп'ютерів (під'єднаних до комп'ютерної мережі і не під'єднаних до неї), так і дії у сфері ІКТ, які є способом для вчинення інших злочинів, наприклад, шахрайств, фальсифікацій тощо.

Нарешті, третій тип правопорушень – кіберзлочини – пов'язаний із діями, спрямованими проти нових реальностей і нових інтересів, які відрізняються від тих, що існували дотепер, оскільки вони виникли завдяки утворенню кіберпростору. Ця нова реальність вимагає вироблення певних норм поведінки й діяльності, які мають виходити з таких умов:

– специфічність (здійснення винятково в кіберпросторі);

– неврегульованість законодавством;

– відмінності у структурі й складі, що відрізняють їх від інших злочинних дій, які порушують недоторканність приватного життя;

– зв'язок із новими реальностями, новими інтересами, новими конфліктами й новими формами соціальних відносин, які не є поки що стабільними чи визнаними [4; 6].

Однак у наведеній вище класифікації напрямків правопорушень недостатньо чіткими є розходження між правопорушеннями в комп'ютерній сфері та кіберзлочинами. Єдина відмінність, на нашу думку, полягає

в тому, що за другим із поданих у цій класифікації напрямком можуть застосовуватися передбачені існуючим законодавством заходи, а щодо третього – законодавчих заходів не існує. Аналіз юридичної практики свідчить, що дуже часто правопорушення в комп'ютерній сфері досить складно довести [3; 5].

У доповіді Ю. Добриніна на VII Міжнародній конференції «Право та Інтернет», подано перелік найпоширеніших на сьогодні комп'ютерних злочинів [7]. Ю. Добринін відносить до них такі види:

– *хакінг* — злом інтернет-сайтів із подальшим «дефейсом», тобто зміною змісту сайту, або без нього;

– *кардинг* — викрадення реквізитів, що ідентифікують користувачів у мережі Інтернет як власників банківських кредитних карток із можливим подальшим використанням цих реквізитів для здійснення незаконних фінансових операцій (останнім часом у соціальній царині знання це називають *крадіжкою ідентичності*);

– *крекінг* — зняття захисту із програмного забезпечення з метою його подальшого безоплатного використання або піратське поширення законно куплених копій програмного забезпечення;

– незаконне одержання й використання чужих облікових даних для користування мережею Інтернет;

– *нюкінг* або «d.o.s.»-атаки – дії, що викликають «зависання» комп'ютера;

– *спамінг* — масове несанкціоноване розсилання електронних повідомлень рекламного чи іншого характеру або «засмічення» електронної скриньки безліччю повідомлень;

– несанкціоноване читання чужих електронних повідомлень [7].

Із юридичної точки зору дана класифікація є аж ніяк не безперечною. У плані «правової коректності» більш цікавою є класифікація, запропонована ООН. Ця організація до числа комп'ютерних злочинів відносить такі правопорушення:

– шахрайські дії за допомогою комп'ютерних маніпуляцій;

– комп'ютерна фальсифікація документів і даних (зазвичай, за допомогою комп'ютерів або копіювальних пристроїв);

– псування або модифікація програм і комп'ютерних даних (до них відносять комп'ютерний саботаж, використання вірусів, «хробаків», «логічних бомб» тощо);

– незаконне проникнення у комп'ютерні системи й служби;

– незаконне відтворення комп'ютерних ліцензійних програм [6; 7].

Хочемо відзначити, що на сьогодні у світі спостерігаються дві основні тенденції щодо регулювання Інтернету й нових ІКТ взагалі: позиція необхідності втручання й позиція збереження свободи дій і безцензурності інформаційного простору [8].

Прихильники першої позиції активно виступають за законодавчі й технічні заходи щодо регулювання інформаційного простору Мережі. Наприклад, у Франції заборонено пропаганду фашизму, так що інтернет-ресурс, на якому пропагуються фашистські ідеї, підлягає закриттю за санкцією судових органів цієї країни [1]. Однак в Україні бракує законів, які регламентували б поширення інформації в Інтернеті, хоча формально таке поширення регулюється існуючим законодавством. Прецеденти закриття сайтів за рішенням суду в Україні внаслідок незаконності їх змісту авторові цієї статті не відомі.

До технічних заходів обмеження доступу до небажаної інформації відносять:

1) фільтрацію інформації на комп'ютері користувачів;

2) фільтрацію інформації на сервері провайдера або компанії;

3) обмеження на одержання посилань на певну інформацію [2].

Для фільтрації на комп'ютері одержувача використовуються програми-фільтри. Найбільш відомими з них є: CyberPatrol, WebSense, CYBERsitter, Net Nanny, Surf Watch, PureSight. Принцип дії цих про-

[1] Під «закриттям» розуміють комплекс заходів, у результаті застосування якого інформація стає недосяжною в мережі. Зазвичай ідеться про видалення інформації з комп'ютерів компанії, що надає послуги хостингу.

грам однаковий. Вони містять усередині себе закодований список web-сайтів, доступ до яких заборонено. Список розподілено за категоріями («оголені тіла», «насильство», «культи й сатанізм», «наркотики» тощо), під час настроювання програми можна заборонити доступ до сайтів тільки частини категорій. Список щодня або щотижня оновлюється, підписка на оновлення є статтею доходу компанії-виробника. Деякі програми (наприклад, CYBERsitter й PureSight) містять засоби динамічного визначення «заборонного» характеру інформації й блокують доступ до неї, навіть якщо вона розміщена на сайті, якого немає у списку програми. Механізм «динамічного визначення» компанія-виробник програми завжди тримає в таємниці, як і точний список сайтів, вбудований у програму. Механізм «динамічного визначення» оновлюється при виході нової версії програми (приблизно раз на півроку).

Паралельно із програмами-фільтрами в Інтернеті існує альтернативна схема фільтрації інформації, заснована на тому, що власники сайтів (контент-провайдери) будуть самі оцінювати свої сайти за змістом (наприклад, «дитячий сайт», «порнографічний сайт»). Така самоідентифікація запропонована міжнародною організацією ICRA (Internet Content Rating Assosiation). Запропонований спосіб ідентифікації відповідає стандарту, відомому як PICS (Platform for Internet Content Selection). ICRA утворилася з Recreational Software Advisory Council (RSAC), що брала участь у розробці цього стандарту, створеного консорціумом World Wide Web Consortium. Система RSACi (RSAC on the internet) вбудовується в Netscape Navigator та Microsoft Internet Explorer. Користувачі (наприклад, батьки неповнолітніх) вищезгаданих браузерів можуть просто увімкнути в цих програмах настроювання «не заходити на порнографічні сайти», внаслідок чого інші користувачі (скажімо, діти) не зможуть потрапити на сайти, позначені їх власниками як «порнографічні». Цей спосіб придатний тільки для блокування доступу до законослухняних акторів порнобізнесу. Зараз тільки деякі великі компанії ідентифікують свої сайти відповідно до цього стандарту [2].

Другий спосіб обмеження доступу до небажаної інформації – фільтрація інформації на сервері провайдера одержувача. Для цього використовують так звані «проксі-сервери». Деякі із цих програм (наприклад, WinProxy, Squid) можуть виконувати кілька функцій, а саме – кешування (збереження в оперативній пам'яті) запитів інформації, блокування доступу до інформації, моніторинг запитів користувачів. Цими програмами можуть користуватися не тільки провайдери, але й компанії у своїй корпоративній мережі. Ці програми здійснюють блокування доступу до сайтів, віднесених до списку «заборонених». Список зазвичай складає співробітник компанії-провайдера або адміністратором мережі компанії. Доступність і відкритість такого списку – питання політики провайдера або менеджменту компанії. В Інтернеті існують відкриті для всіх списки «заборонних» сайтів (наприклад, за адресою http://www.squidguard.org/). У разі публікації відкритих списків їх укладачі повідомляють, що вони не несуть ніякої відповідальності за зміст списку, тому що він складається програмою, що апріорі може помилятися. За відповідним запитом вони можуть виключити помилково внесену адресу зі списку. Відкриті списки також можуть частково збігатися із закритими, однак різні програми використовують різні списки, незалежно від ступеня їх відкритості.

Якщо інформація фільтрується на сервері провайдера, клієнт звичайно може звернутися з проханням відфільтрувати або зовсім не фільтрувати інформацію, одержувану особисто ним. Під час використання фільтрувального програмного забезпечення сервером компанії спів робітник компанії змушений підкорятися прийнятим у компанії правилам. Конфлікти, пов'язані з такими обмеженнями у доступі до інформації, зазвичай вирішуються на користь провайдера або компанії, тому що

клієнт вправі обрати іншого провайдера, а співробітник – звільнитися з компанії, якщо корпоративні правила для нього неприйнятні.

Провайдери рідко проводять моніторинг інтернет-запитів клієнтів, хоча мають таку технічну можливість. У той же час компанії часто здійснюють моніторинг інтернет-запитів співробітників. Більше того, базуючись на опублікованих правилах роботи в компанії та даних моніторингу, компанії звільняють службовців, які, за даними моніторингу, порушують ці правила.

Стан справ у цій сфері залишається практично незмінним протягом останніх кількох років. Однак удосконалюються системи контекстної фільтрації. Крім того, до програм фільтрації вносяться доповнення для фільтрації нових засобів одержання інформації (чати, гостеві книги, дошки оголошень, інтернет-конференції тощо).

Деякі пошукові системи (наприклад, Altavista, Яндекс) пропонують можливість фільтрації результатів пошуку, тобто вводять обмеження на одержання посилань на запитувану інформацію. На Altavist'і (http://ims2002.nw.ru/www.altavista.com) цей процес включає фільтрацію фотозображень, виключення з результатів пошуку посилань на матеріали сексуального або образливого характеру. Матеріали характеризуються за допомогою автоматизованого контекстного аналізу, вручну редакторами Altavista і за результатами коментарів користувачів.

Фільтр Altavista обмежує доступ не тільки до тих матеріалів, що мають сексуальний характер, але й до тих, що містять пропаганду насильства тощо («hate speech»). На жаль, Altavista може фільтрувати тільки англомовні тексти.

Пошукова система Яндекс (http://ims2002.nw.ru/www.yandex.ru) дозволяє фільтрувати нецензурну лексику й порнографію, тобто те, що не дозволено «дітям до 16». Сьогодні фільтр будується напівавтоматично – до його бази даних включаються «дорослі» сайти, а також усі сторінки, що містять «негарні» слова. Яндекс фільтрує тільки російськомовні тексти, при цьому фільтрація «hate speech» поки не реалізована.

Методики, використовувані Яндексом й Altavist'ою, подібні: однакові методи збору інформації (аналіз текстів, звіти співробітників і користувачів) та методи фільтрації (потрібне мінімальне настроювання програми-браузера користувача на його комп'ютері, щоб фільтр запрацював). Сам аналіз текстів, звичайно, відрізняється, насамперед, через різницю в мовах та об'єктах фільтрації (американська неполіткоректність і російська ненормативна лексика, як правило, відчутно різняться за змістом, емоційною напруженістю та спрямованістю текстів). На жаль, подібних програм, що працювали б українською мовою, ще не створено й залишається заспокоювати себе лише тим, що понад 90 % національного сегмента Мережі становлять російськомовні сайти [9].

У цей час у країнах Євросоюзу динамічно розвивається мережа інформаційних та інтерактивних інтернет-порталів, мета яких – забезпечити користувачеві відповідну безпеку в Мережі (наприклад, Internet Watch Foundation або сторожовий робот WebSite-Watcher).

У рамках програми Європейської комісії з питань інформаційного суспільства та ЗМІ (European Commision of Information Society and Media) у країнах ЄС організуються національні відділення, діяльність яких зосереджується на інформуванні користувачів про небезпеки, які можуть виникнути в Мережі, й підвищенні їх відповідальності та свідомості. Нині відділення працюють у 21 країні. Також у програмі беруть участь шість асоційованих членів. Співробітництво між відділеннями координує загальноєвропейська організація Safer Internet [2].

У липні 1996 р. Рада ЄС почала роботу щодо протидії нелегальній інформації в Мережі, ухваливши план боротьби з расизмом і ксенофобією. У 1997 р. Рада у справах телекомунікацій прийняла резолюцію з приводу небезпечної або нелегальної інформації в Інтернеті, затверджену в січні 1999 р. Європарламентом та Радою Європи. Цей документ ініціював та увів у дію про-

граму SIAP (Safer Internet Action Plan), що пропагує безпечне користування Інтернетом, а також новими засобами ІКТ – стільниковими телефонами останнього покоління, онлайн-іграми, соціальними мережами та комунікаторами. Головна мета програми – підвищення поінформованості усіх користувачів Інтернету про безпечне та ефективне користування Мережею. Робота у рамках програми SIAP здійснюється за чотирма напрямками:

1) підвищення рівня поінформованості про безпечне користування Інтернетом (Internet Awareness);

2) розвиток європейської мережі пунктів HOTLINE, що виявляє небезпечну й нелегальну інформацію в Інтернеті (Hotlines);

3) розвиток технологій, що фільтрують та оцінюють зміст інтернет-сторінок (Filtering and Rating);

4) підтримка саморегуляції Мережі (Self Regulation).

Ефективність цієї програми підтверджує досвід її застосування. Досить яскравим є приклад Великобританії, де програма діє з 1996 р. Так, портал Internet Watch Foundation (буквально «Фонд інтернет-сторож») являє собою інтерактивний веб-сайт http://www.iwf.org.uk, на якому постійно працює «гаряча лінія», куди можна повідомити про інтернет-сторінки із протизаконним змістом, а також про злочинні інтернет-товариства. В організації Internet Watch Foundation зареєстровані усі великі британські інформаційні портали, так, як Google, AOL, Yahoo, MSN, Vodafone та ін. Медіапортали також входять до числа учасників Internet Watch Foundation (наприклад, всесвітньо відома служба BBC). На порталі розміщені нормативні акти й документи з даної тематики, координати урядових і державних організацій, що займаються питаннями безпеки в Інтернеті. Є посилання на ЗМІ, що підтримують безпечний Інтернет. Результативність програми відбита в резюме організації (листопад 2006 р.): «IWF – єдина офіційно діюча організація в Об'єднаному Королівстві з оперативною «гарячою лінією» для громадськості та професіоналів IT, за якою можна повідомляти про можливо злочинний контент інтернет-ресурсів... Наша мета – мінімізувати доступ нелегального контенту до користувачів мережі. Ми співробітничаємо з департаментами уряду Об'єднаного Королівства, такими, як Home Office та The Department of Trade and Industry, що дозволяє посилити впливовість та ефективність наших ініціатив та програм щодо боротьби з інтернет-злочинами і зловживаннями. Також ми підтримуємо діалог «Об'єднане Королівство – Європа», щоб посилити усвідомлення глобальних причин проблеми й колективної відповідальності. ... Ми співробітничаємо зі службами безпеки й поліції. Ми передаємо їм відомості, що надходять на нашу «гарячу лінію». ... За перший рік роботи «гарячої лінії» надійшло 615 повідомлень. У десятий рік роботи Internet Watch Foundation розглянуло 27250 повідомлень стосовно сумнівного контенту інтернет-ресурсів, при цьому лише за перший рік функціонування «гарячої лінії» обсяг нелегальної інформації знизився на 18 %. На цей час тільки 0,2 % від можливого кримінального контенту, розміщуваного в британській інтернет-мережі, доходить до користувачів» [2].

Прихильники позиції саморегуляції мережі Інтернет стверджують, що в мережі вже існують певні норми поведінки – так звана етика користувача або «мережний етикет» («netiquette»), недотримання якого засуджується всіма іншими користувачами, і закони її внутрішнього саморегулювання є цілком достатнім механізмом неформального контролю. Для здійснення надійного контролю необхідно також створити відповідне програмне забезпечення. Але, як відомо із практики, поява будь-якої програми цього типу викликає в багатьох бажання розробити нову програму, що нейтралізує ефективність контролюючої. І, нарешті, контролю протистоять не тільки міркування економічного характеру, поганого смаку або етичної незрілості. У разі встановлення занадто жорсткого контролю свобода висловлення може

перетворитися на таку цінність, яку слід буде всебічно захищати.

Утім, здається, недостатньо наявності лише такого «неформального» контролю, особливо у зв'язку з експонентним зростанням Мережі. Яким шляхом піде Україна у сфері розвитку інформаційної безпеки, поки що незрозуміло, хоча ця проблема для нашої країни є настільки ж актуальною, як і для будь-якої іншої європейської держави. Що стосується Росії, то ця країна поки що не поспішає приєднуватися до програми Safer Internet Action Plan, хоча на папері і є асоційованим учасником програми. Єдиним російським партнером SIAP є челябінська НКО «Ангел» [2, с. 157]. Тим часом безпека в Інтернеті – злободенна для Росії проблема. Як свідчить звіт IWF за листопад 2006 р., близько 20 % виявлених інтернет-ресурсів із кримінальним контентом мають російський хостинг [2].

Література

1. World Internet Users. March 2008 [Електронний ресурс] // Internet Usage Statistics. – Режим доступу : http://www.internetworldstats.com/stats.htm.
2. Балашова Е. С. К вопросу о безопасности в Интернете: стратегия ЕС на примере европейского общества / Е. С. Балашова // Онлайн-исследования в России: тенденции и перспективы. – М. : ООО «РИЦ Северо-Восток», 2007. – С. 151–158.
3. Сейник В. Борьба с киберпреступностью – одна из составляющих международной безопасности [Електронний ресурс] / В. Сейник // Центр исследования компьютерной преступности. – Режим доступу : http://www.crime-research.ru/articles/seinick08/.
4. Маркин А. В. Взаимовлияние информационных потоков и роста социальных девиаций в социуме: к постановке проблемы / А. В. Маркин // Социологический анализ девиантного интернет-поведения: криминология, наркотизация, алкоголизация. – М. : Изд-во института социологии РАН, 2007. – С. 4–15.
5. Карчевский Н. Проблемы гармонизации украинского и международного законодательства о компьютерных преступлениях [Електронний ресурс] / Н. Карчевский // Цент исследования компьютерной преступности. – Режим доступу : http://www.crime-research.ru/articles/karchevsk08/.
6. Человек и новые информационные технологии. Завтра начинается сегодня. – СПб. : Речь, 2007. – 320 с.
7. Добрынин Ю. Классификация компьютерных преступлений, взгляд хакера и юриста [Електронний ресурс] / Ю. Добрынин // Центр исследования компьютерной преступности. – Режим доступу : http://www.crime-research.ru/news/01.11.2005/2311.
8. Шурыгина И. И. Интернет – пространство свободы выбора / И. И. Шурыгина // Онлайн-исследования в России: тенденции и перспективы. – М.: ООО «РИЦ Северо-Восток», 2007. – С. 129–140.
9. Ukr.net заговорил на украинском? [Електронний ресурс]. – Режим доступу : http://www.ain.com.ua.

Надійшла до редколегії 05.05.2009

Анотації

У статті розглядаються основні види комп'ютерних злочинів. Характеризуються деякі технічні заходи обмеження доступу до небажаної інформації.

В статье рассматриваются основные виды компьютерных преступлений. Характеризуются некоторые технические меры ограничения доступа к нежелательной информации.

In the article main forms of computer crimes are viewed. Some technical measures of limitation access to prohibited information are characterized.