МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ГОЛОВНЕ УПРАВЛІННЯ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ В ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ

Практичні аспекти організації припинення роботи інтернет-ресурсів національного та закордонного сегментів, що використовуються для вчинення злочинів

Методичні рекомендації

Дніпропетровськ
2015

Рекомендовано науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 3 від 12.11.2015 р.)

РЕЦЕНЗЕНТИ

М.О. Алексєєв – доктор технічних наук, професор, декан факультету інформаційних технологій Державного ВНЗ «НГУ»
В.Б. Вишня - доктор технічних наук, професор, професор кафедри інформатики та інформаційних технологій в діяльності ОВС

Практичні аспекти організації припинення роботи інтернет-ресурсів національного та закордонного сегментів, що використовуються для вчинення злочинів: методичні рекомендації / [В.О. Мирошниченко, І.В. Краснобрижий, В.Д. Поливанюк, С.В. Бабанін, І.О. Кисельов, Д.Ю. Чередниченко, Ю.В. Заскока]. – Дніпропетровськ: Дніпроп. Держ. Ун-т. внутр.. справ, 2015.. – 50 с.

З урахуванням сучасних потреб правоохоронної практики, стану розвитку інформаційних технологій та кримінально-правової науки розглянуті сучасні тенденції боротьби з поширенням інтернет-ресурсів національного та закордонного сегментів, що використовуються для вчинення злочинів. У методичних рекомендаціях розглянуто міжнародний досвід регулювання всесвітньої мережі Інтернет, моделі та методи цензури контенту в Інтернеті, пошук інформації, пов’язаної з роботою ресурсів, що використовуються для вчинення злочинів та правові аспекти боротьби з комп’ютерними злочинами.
Методичні рекомендації розраховані на працівників органів внутрішніх справ, які працюють над розкриттям та розслідуванням злочинів у сфері комп’ютерних технологій.

ЗМІСТ

Вступ

Стрімкий та динамічний розвиток інформаційних технологій кожен день все більше змінює аспекти економічного, політичного і соціального життя у всіх країнах світу. Але розширення інформаційного обміну супроводжується не тільки процесами, які збільшують культурно-комунікативні можливості людини, але й такими, що створюють підґрунтя для виникнення нових форм злочинності у сфері високих технологій.

Злочини у сфері сучасних інформаційних технологій приймають міжнародний та транснаціональний характер, у зв’язку з чим потерпілі від таких злочинів можуть знаходитись в різних країнах світу. Тому для протидії таким видам злочинів особливе значення має посилення і удосконалення міжнародного співробітництва в даній сфері, підвищення його ефективності.

На теперішній час вказані проблеми мають тенденцію до того, що міжнародні організації та органи влади багатьох країн вживають організаційні та правові заходи щодо запобігання та протидії злочинам у сфері сучасних інформаційних технологій. Для підтримки такої позиції, на базі використання системи криміналістичної класифікації способів вчинення правопорушень у сфері інформаційних технологій був розроблений кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачені комп'ютерні .злочини. З метою запобігання злочинам вчиненим у сфері інформаційних технологій, 23 листопада 2001 року в Будапешті була підписана Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, більш відома в Україні під назвою «Конвенція про кіберзлочинність». Вона відкрита для підписання як державами - членами Ради Європи, так і тими державами, які не є її членами та брали участь у її розробці. Зокрема, її підтримали США і Японія. Крім того, Європейським комітетом з проблем злочинності Ради Європи в 1990 році, з метою підвищення ефективності протидії таким видам злочинів та правового визначення в Європі такої групи злочинів, пов'язаних з комп’ютерами і інформаційними

технологіями, були підготовлені рекомендації про включення в законодавство європейських країн кримінальних норм «Мінімального списку» і «необов’язкового списку» комп’ютерних злочинів.

Міжнародний досвід регулювання всесвітньої мережі Інтернет

Регулювання Інтернету в Великобританії:

Підхід до фільтрації контенту у Великобританії являє собою особливий інтерес у зв'язку з тим, що саме британська система регулювання Мережі була взята за зразок при створенні Ліги безпечного Інтернету й ініціюванні закону № 139-ФЗ, у рамках якого з'явився «реєстр заборонених сайтів».

Уряд Великобританії в середині 2000-х років позначив два ключових завдання, які повинні переслідувати фільтрацію інтернет-контенту: боротьба з тероризмом і запобігання поширення дитячої порнографії. Пізніше до цього переліку додалася боротьба із систематичним порушенням авторських прав.

Ключову роль у питаннях регулювання контенту в Мережі грають не державні органи, а благодійний Фонд спостереження за Інтернетом (Internet Watch Foundation), заснований в 1996 році. Фінансування фонду частково забезпечують британські оператори зв'язку, інтернет-компанії й виробники програмного забезпечення, а частково - уряд Великобританії й структури Євросоюзу.

Офіційно задачею, що декларується IWF, є «мінімізація доступності потенційно незаконного інтернет-контенту, особливо дитячої порнографії, поза залежністю від того, де він розміщений, а також видалення незаконного порнографічного контенту, розміщеного на території Великобританії». Раніше організація ставила своєю метою також боротьбу з розпаленням расової ненависті, однак в 2011 році ця функція була передана поліцейському проекту True Vision, що покликаний акумулювати скарги на злочини, пов'язані з

розпаленням ненависті відносно різних груп населення, і закривати дані ресурси, якщо вони розташовані на британських серверах.

Функція IWF зводиться до ведення реєстру заборонених сайтів, що являє собою набір посилань, переважно пов'язаних з дитячою порнографією. Безпосереднім веденням даного реєстру займаються декілька фахівців, навчених поліцією. За різними оцінками, усього в списку IWF одночасно утримується приблизно 1000 функціонуючих сайтів.

У свою чергу, у інтернет-провайдерів встановлене спеціальне програмне забезпечення Cleanfeed, яке покликане блокувати доступ до заборонених сайтів. Дана система була розроблена державною корпорацією British Telecom в 2004 році й у цей час її використання є обов'язковим для всіх провайдерів Великобританії, поза залежністю від того, державні вони або недержавні. У результаті, дія системи Cleanfeed поширюється практично на всіх британських інтернет-користувачів.

Провайдери самі визначають, повідомляти чи ні своїм користувачам про те, що сайт, на який вони хотіли перейти, заблокований Cleanfeed. Деякі виводять відповідне повідомлення, однак більша частина повідомляє про те, що дана сторінка відсутня на сервері (page not found). Таким чином, користувачі не знають про те, що той або інший контент був заблокований. Тому що блокування здійснюється не за рішенням суду а сам оператор реєстру не є державним, процедура апеляції блокування здійснюється за внутрішніми правилами IWF.

З 2011 року система Cleanfeed використовується операторами зв'язку не тільки для боротьби з дитячою порнографією. Британська асоціація кінематографістів через суд змусила провайдерів використовувати систему фільтрації контенту для блокування сервісів обміну неліцензійним контентом, що порушує авторські права. Зокрема, у травні 2012 року серед інших блокуванню піддався найбільший торрент-трекер The Pirate Bay.

Технічна реалізація системи виглядає наступним чином. Існує конфіденційний список заборонених інтернет-сторінок (не сайтів), доступ до якого є тільки у фахівців IWF. Він не доступний ні провайдерам, ні рядовим

користувачам. Провайдерам надається список IP-адрес сайтів, на яких розміщені дані сторінки, для того, щоб саме до цих адрес застосовувалися правила фільтрації.

Провайдери перенаправляють трафік, що йде на ці адреси, на спеціальні проксі-сервери, які порівнюють HTTP-запити з адресами сторінок, що містяться в реєстрі заборонених адрес. Якщо вони не збігаються - трафік проходить фільтр і користувач потрапляє на запитувану сторінку.

Робота Cleanfeed здійснюється у два етапи:

1. Перевірка IP-Адреси, до якого звернений запит.

2. Порівняння сторінки, до якої звертається користувач, зі списком адрес у реєстрі заборонених ресурсів.

Пізніше система Cleanfeed була експортована в деякі країни британської співдружності. У Канаді в цей час вона використовується на добровільній основі найбільшими провайдерами країни, що обслуговують приблизно 80% інтернет-користувачів. В Австралії впровадження даної системи зіткнулося з політичною протидією, і її реалізація в масштабах країни була відкладена на невизначений термін.

У серпні 2011 року після масових безладь у найбільших британських містах, прем'єр-міністр Великобританії Девід Кемерон зустрівся з керівництвом найбільших інтернет-компаній з метою обговорення можливих заходів, які дозволили б запобігти використанню соціальних мереж погромниками. Із цього приводу Кемерон зробив наступну заяву в парламенті:

«Всі ми уражені тим, що жахливі події, які відбулися в нашій країні, організовані за допомогою соціальних медіа. Вільний потік інформації може використовуватися в благо. Але також він може використовуватися й зі злим наміром. Коли люди використовують соціальні медіа для провокування насильства, наше завдання - зупинити їх. Тому ми працюємо разом з поліцією, розвідувальними службами й інтернет-індустрією над питанням: чи правильно буде призупинити інтернет-комунікацію через певні сайти й сервіси, якщо нам

відомо, що за допомогою їх плануються дії, пов'язані зі злочинністю й насильством».

Регулювання Інтернету в США

На практику регулювання Інтернету в США великий вплив зробили відразу декілька факторів, зробивши її унікальною серед інших країн. По-перше, США - історична батьківщина Інтернету, а багато американських IT-компаній, такі як Google, Facebook і Twitter, займають лідируючі позиції в мережі. По-друге, перше виправлення Конституції США прямо забороняють приймати закони, що обмежують свободу слова. Отже багато методів регулювання Інтернету американським законодавцям недоступні. У третіх, провідна роль США у світовій політиці й економіці дозволяє добиватися від іноземних країн і компаній виконання вимог американської влади.

Спроби поставити за обов'язок інтернет-провайдерів і реєстраторів доменів блокувати доступ до сайтів за рішенням суду неодноразово здійснювались правовласниками й прихильниками боротьби з дитячою порнографією. Але щораз такі закони не приймалися Конгресом, а рішення судів відмінялися. Так, в 2004 році штат Пенсільванія прийняв закон, що наказує інтернет-провайдерам фільтрувати сайти з дитячою порнографією. Механізм блокування не був добре відпрацьований, і в результаті крім нелегального контенту недоступними виявилися більше мільйона інших сайтів. Незабаром федеральний суддя виніс рішення про невідповідність даного закону першому виправленню.

В 2012 році Конгрес розглядав проекти законів SOPA і PIPA, які зобов'язували провайдерів і хостерів блокувати доступ до сайтів з матеріалами, що порушують авторські права, по вимозі правовласників. У знак протесту тисячі сайтів, включаючи Вікіпедию й Craigslist, на день перестали працювати. Петиція проти законів, розміщена на сайті Google, зібрала більше 4,5 мільйонів підписів. У результаті, Конгрес відклав їхній розгляд.

В 2000-х роках Мін'юст США застосовував тактику по конфіскації доменів сайтів, що порушують закон, трактуючи їх як майно, використовуване для кримінальної діяльності. Цей захід також зазнав критики активістів по захисту свободи слова в Інтернеті. Крім цього, її ефективність була сумнівною - найчастіше сайти ставали доступні по новій адресі. Інший випадок блокування DNS-записів державою - застосування Акту про торгівлю з ворогом, що забороняє ведення бізнесу з рядом держав. Відповідно до його положень компанія-реєстратор доменів була змушена блокувати DNS-запис туристичного агентства, що рекламував тури у Кубу.

У цілому, на сьогоднішній день Інтернет у США залишається вільним від технічних методів цензури з боку держави. Замість цього фільтрація контенту добровільно здійснюється приватними компаніями за підтримкою державних структур. Наприклад, у випадку з дитячою порнографією, ряд великих інтернет-провайдерів підписали угоду з окружним прокурором Нью-Йорка, погодившись добровільно блокувати доступ до таких ресурсів.

Іншим важливим інструментом США по регулюванню Інтернету залишається тиск на іноземні компанії. Оскільки в США нелегальна більшість видів азартних онлайн-ігор, а держава не має можливості блокувати доступ до іноземних сайтів, влада пішла на ряд жорстких заходів відносно порушників. Конгрес прийняв закон, що передбачає заборону онлайн-казино й букмекерським конторам приймати платежі від американських громадян. Google і Yahoo відмовилися від розміщення рекламних банерів таких сайтів, після того як Мін'юст США заявив, що реклама може бути розцінена як сприяння злочину. Ряд власників букмекерських контор, що працюють онлайн, були піддані карному переслідуванню. Такий тиск дозволяє добиватися від компаній, що перебувають поза юрисдикцією США, виконання вимог американських законів.

США одними з перших прийняли закони, що регулюють інтелектуальну власність в Інтернеті. Відповідно до законодавства, інтернет-провайдери й хостингові компанії звільняються від судової відповідальності за передачу й зберігання інформації, що порушує авторські права, якщо вони видаляють її

після звертання правовласника. Закон привів до того, що, побоюючись позовів, сайти найчастіше видаляють контент на першу вимогу, не вникаючи чи дійсно він порушує авторські права. Наприклад, Google одержує кілька мільйонів запитів на місяць на видалення посилань із результатів пошуку.

Справжнім тестом для дії першого виправлення Конституції США в Інтернеті став скандал навколо сайту Вікілікс. Неприємності з американським правосуддям у нього почалися ще в 2008 році - по позову швейцарського банку суд наказав заблокувати доменне ім'я сайту. Рішення викликало протести з боку активістських груп і незабаром було скасовано. Справжні проблеми ж викликала публікація в 2010 році засекречених документів і матеріалів, зокрема відеозапису розстрілу американськими військовими цивільних осіб в Іраку й дипломатичній переписці посольств. Їхнє оприлюднення завдало істотної шкоди національним інтересам США.

Незважаючи на те, що формально, публікація третьою стороною незаконно отриманої інформації не суперечить законодавству країни, Міністерство юстиції розглянуло можливість карного переслідування творця сайту Джуліана Ассанджа за обвинуваченням в «крадіжці державної власності» і порушенні Акту про шпигунство від 1917 року. Влада США заблокувала доступ до сайту з комп'ютерів федерального уряду й зробила безпрецедентний тиск на компанії, що працюють із Вікілікс. Зокрема, Amazon відмовився від надання послуг хостингу сайту, а платіжні системи Visa, Mastercard і Paypal перестали приймати платежі на його адресу. Проте, переважна більшість інтернет-користувачів США як і раніше можуть безперешкодно відвідувати сайт Вікілікс.

Інтернет-Цензура в Ірані

По долі населення, що користується Інтернетом, Іран посідає друге місце на Близькому Сході, уступаючи тільки Ізраїлю. У країні особливо розвинена блогосфера - по оцінках експертів, число регулярно обновлюваних блогів перевищує 60000. Зусилля уряду Ірану, з одного боку, спрямовані на розвиток

інфраструктури Інтернету, з іншого боку - на повний контроль того, що публікується користувачами в мережі.

В умовах жорстких законів, що регулюють пресу, Інтернет до 2004 року залишався однією з деяких місць, де можна було вільно виражати свою думку. Але поступово таке джерело вільнодумства привернуло увагу влади Ірану, і вона почала реалізацію послідовної політики по боротьбі з небажаним контентом. Дія положень закону про пресу було розширено на електронні публікації. Додатковим стимулом для посилення контролю над Інтернетом стали масові протести після президентських виборів 2009 року, коли опозиція використовувала соціальні мережі для координації акцій і зв'язку із західними агентствами новин.

Обмеження свободи слова прямо передбачені іранською конституцією, у якій сказане, що «засоби масової інформації повинні втримуватися від руйнівних і анти-ісламських практик». Закон про пресу також обмежує неприпустиму інформацію, зокрема «висвітлення тематик, які шкідливі для основ Ісламської республіки», «образа Лідера Революції», «підбурювання громадян до дій проти безпеки, гідності й інтересів Ісламської республіки». Також заборонені будь-які публікації, що ображають іслам. Такі розпливчасті категорії дозволяють владі блокувати практично будь-яку інформацію зі свого розсуду.

Фільтрація контенту в Інтернеті донедавна здійснювалося на підставі серії постанов Верховної Ради Культурної революції, а визначення критеріїв для блокування було довірено міжвідомчому комітету, у який входять представники міністерств культури, безпеки й Генеральної прокуратури. Практичною реалізацією політики фільтрації займається підрозділ головної державної телекомунікаційної компанії й агентство Міністерства по комунікаціях. В 2012 році лідер Ірану Хаменеі оголосив про створення Верховної ради по кіберпростору, що із цього моменту займається створенням єдиної політики у відношенні Інтернету.

Всі провайдери країни повинні одержувати ліцензію від державних органів, а користувачі підписують зобов'язання не відвідувати « анти-ісламські

сайти». Для домогосподарств діє ліміт на швидкість в 128 Кбіт/с, що полегшує навантаження на систему фільтрації, а також обмежує доступ користувачів до небажаних західних фільмів і музики. На організації й університети він не поширюється. На даний момент Іран залишається єдиною країною, де діє законодавче обмеження на швидкість доступу в Інтернет для користувачів.

Однією з умов надання провайдерам ліцензії є застосування системи фільтрації, що блокує список веб-сторінок, наданого державою. Спочатку вся цензура здійснювалася саме на рівні провайдерів, але в останні роки влада Ірану розробила й впровадила централізовану систему, що працює у зв'язці із фільтрами провайдерів. Цей крок забезпечив більшу однаковість у політиці цезури, тому що раніше вона сильно варіювалася від провайдера до провайдера. Технічна фільтрація в Ірані прозора - при спробі звертання до сайту, занесеному в державний список, видається блок-сторінка з роз'ясненням, що ресурс недоступний, і контактами адміністратора, якому можна направити запит.

Фільтри, застосовувані в Ірані, являють собою проксі-сервери, на які перенаправляється трафік користувачів. Кожний запит звіряється зі списком заблокованих сайтів і сторінок, а також аналізується на предмет наявності певних ключових слів. У випадку збігу користувач перенаправляється на блок-сторінку.

Ранні дослідження Open Net Initiative показали, що технічним рішенням, що використовували інтернет-провайдери, був SmartFilter американської фірми Secure Computing. Сама компанія-виробник відхиляла продаж програмного забезпечення, стверджуючи, що Іран використовує його незаконно. Співробітництво з Іраном у цій сфері могло стати не тільки серйозним ударом по репутації Secure Computing, але й можливим порушенням економічних санкцій США.

Влада Ірану була незадоволена залежністю своєї системи фільтрації від західних технологій, побоюючись убудованих уразливостей, які можуть порушити її роботу. Тому їхні зусилля були спрямовані на перехід до інформаційних рішень, розроблених місцевими компаніями. На сьогоднішній

день технічна система фільтрації Ірану використовує власні розробки не тільки для блокування сайтів, але й для автоматичного пошуку забороненого контенту в мережі.

В Ірані діє тверда система контролю за користувачами. Інтернет-провайдери зобов'язані зберігати протягом 3 місяців не тільки логи, але й саму інформацію, що передається користувачами. Коли один з іранських дисидентів був арештований за висловлення в системі миттєвого обміну повідомленнями, доказом його провини виступала роздруківка його переписки. Користувачі інтернет-кафе повинні надавати свою ідентифікаційну інформацію, а власники зобов'язані встановлювати в приміщенні камери й зберігати записи про відвідувачів.

Думки фахівців розходяться в оцінці здатності Ірану застосовувати технологію глибокого аналізу пакетів. В 2008 році компанію Nokia Siemens Systems обвинуватили в поставках головному телекомунікаційному операторові країни встаткування, яке здатне масово перехоплювати повідомлення користувачів. Однак представник NSS заявив, що його можливості обмежені тільки законним відстеженням комунікацій окремих користувачів у рамках діяльності правоохоронних органів. Розслідування Reuters і Wall Street Journal показало, що дві китайські корпорації Huawei і ZTE співробітничали із владою Ірану в створенні системи інтернет-стеження. Їхні представники також відкинули ці обвинувачення. Проте, є ряд свідчень того, що Іран має подібну технологію. Так, в 2012 році під час виборів влади блокували весь зашифрований трафік.

Виправлення до закону про пресу Ірану, прийняті в 2009 році, зобов'язують власників сайтів проходити процедуру реєстрації в Міністерстві культури, що має право відзивати ліцензію й забороняти окремі публікації. З положень іншого закону, інтернет-сервіси відповідають за матеріал, розташований у них іншими користувачами. За таких умов, широке поширення одержала самоцензура, коли користувачі побоюються висловлювати свою думку онлайн, а власники сайтів зі своєї ініціативи видаляють будь-який спірний контент.

Влада Ірану активно застосовує карне переслідування відносно користувачів Інтернету, у тому числі страту. За інформацією Human Rights Watch, в 2011 Іран встановив рекорд по кількості арештованих блогерів і журналістів. За кримінальним кодексом Ірану покарання аж до страти передбачено за «пропаганду проти держави», «образу релігії», «хвилювання громадськості» і «поширення неправдивих чуток». Так, в 2004 році блогер був арештований за повідомлення про арешт трьох інших користувачів. В 2012 році за обвинуваченням у поширення дезінформації був арештований адміністратор сайту, що повідомляв про курс національної валюти стосовно долара.

За заявою представника офіційної влади, в 2006 році в Ірані були блоковані більше 10 мільйонів сайтів, 90% з яких належали до «аморального контенту». Порнографія залишається одним з головних пріоритетів для блокування. При цьому до неї Іран відносить навіть зображення провокаційного одягу. Пошукові запити, що містять слова «секс», «жінка» і «фотографія» на фарсі або англійському також блокуються. Фільтруються й багато інших сайтів, близькі до цієї тематики, зокрема сайти знайомств, матеріали по статевій освіті й ресурси Лгбт-співтовариства.

Іншою широкою категорією контентів, доступ до яких в Ірані обмежується, є сайти, що порушують норми ісламу. Блокуються ресурси, пов'язані із уживанням наркотиків і алкоголю, а також азартними іграми. За критику державної релігії передбачене суворе покарання, а подібні сайти, розташовані за кордоном, ретельно блокуються.

Відповідно до результатів тестування Open Net Initiative, Іран посідає перше місце у світі по частці блокованих ресурсів політичного характеру. Основні зусилля цензорів зосереджені на матеріалах на фарсі; із сайтів на іноземних мовах блокуються тільки самі великі новинні портали, такі як The Huffington Post, Al-Arabiya і Global Voices.

Серед політичного контенту, що фільтрується, перебувають сайти політичної опозиції, правозахисних організацій, що зокрема виступають за права жінок, етнічних і релігійних меншостей, активістів і журналістів, що критикують

режим. Якщо після виборів 2009 року активно блокувалися ресурси кандидатів, що виступають проти діючого президента Ахмадінежада, то в 2011 році недоступною виявився й сайт групи його прихильників.

За станом на 2012 рік, в Ірані блоковані найбільші міжнародні інтернет-сервіси, такі як Facebook, YouTube, Twitter і Flicker. Доступ до сервісів Google періодично пропадає, що утруднює їхнє використання. Заблоковано більшість платформ для ведення блогів, у тому числі Livejournal і Xanga.

В 2011 році Іранська влада оголосила про плани по створенню Національного Інтернету, що передбачають захист країни від кіберпогроз, обмеження доступу користувачів до контенту за кордоном, а також більш суворий контроль за їхніми діями. Ініціатива припускає створення національних аналогів пошукових систем, поштових сервісів і платформ для ведення блогів. Недолік офіційної інформації привів до появи різних версій того, які цілі переслідує Іран. По одній з них, під Національним Інтернетом мається на увазі мережа, повністю ізольована від глобальної, на зразок діючої в Північній Кореї. У той же час, представники влади заявили, що як базова модель обрана регулювання Інтернету в Китаї, коли весь зовнішній трафік строго контролюється, але доступ до нього зберігається.

Інтернет-цензура в Китаї

Коли мова заходить про систематичне цензурування інтернет-контенту на державному рівні, майже завжди наводиться приклад Китаю - країни, де нібито заборонено практично все. Однак, як це часто буває, реальність виявляється набагато складніше, ніж створений міф.

Насамперед, для аналізу китайської моделі блокування контенту в Мережі необхідно зупинитися на тому, що взагалі являє собою китайський сегмент Інтернету. На сьогоднішній день Китай з 564 мільйонами інтернет-користувачів посідає перше місце у світі по даному показнику, а рівень їхньої активності в Мережі не тільки не поступається, але й у деяких сегментах значно перевершує

активність громадян інших держав, незважаючи на відсутність доступу до популярних міжнародних комунікаційних сервісів. Аналогічна ситуація й у комерційної складової Мережі - Китай не поступається країнам Європи в частині розвитку розважального й комерційного сегментів: існують великі торговельні площадки, розвинена система мікроплатежів, а ринок онлайн-ігор посідає перше місце по своєму обсязі у світі з величезною кількістю локальних продуктів.

У той же час, гігантський з погляду аудиторних і фінансових параметрів інтернет-сектор Китаю уживається зі складною системою цензури, що складається із трьох базових елементів:

1. Система фільтрації трафіка «Золотий щит» (вона ж «Великий китайський фаєрвол»);

2. Система блокування пошуку небажаної інформації;

3. Ручна система фільтрації контенту, що публікується в соціальних мережах і блогосфері.

«Золотий щит»

«Золотий щит», він же «Великий китайський фаєрвол» - це система фільтрації інтернет-контенту, розробка якої почалася в 1998 році, а офіційний запуск відбувся в 2003. По оцінках експертів, вартість її створення могла скласти до $800 млн., а в її розробці брали участь великі американські корпорації, зокрема IBM. Завданням «Золотого щита» є блокування доступу користувачів з материкового Китаю до деяким інтернет-ресурсам, розташованим на серверах за межами країни. Список заборонених ресурсів формується безпосередньо в Пекіні й у нього входять як сайти політичної спрямованості, так і світові соціальні сервіси, непідконтрольні пекінській владі.

На початок минулого року було відомо про приблизно 2600 сайтів, доступ до яких заблокований за допомогою системи «Золотий щит». Серед цих сайтів 45 ресурсів, що входять у список 1000 самих відвідуваних у світі інтернет-сайтів за версією сервісу статистики Alexa. Так, у списку заблокованих перебувають Facebook.com, Youtube.com, Twitter.com, Blogspot.com, Blogger.com, Vimeo.com,

Nytimes.com, WordPress.com, а також найбільші порнографічні ресурси Мережі. Найкрупніші російські соціальні мережі «В контакте» і «Однокласники» доступні китайським користувачам, однак лише тому, що місцеві жителі ними практично не користуються.

Доступ до деяких сайтів обмежений лише частково. Так, китайським користувачам доступний сайт Вікіпедії, однак відсутній доступ до статей, що зачіпають питання китайської політики. Аналогічна ситуація спостерігалася з пошукачем Google, функції якого були доступні лише частково, перше ніж компанія вирішила припинити свою роботу в материковому Китаї.

Технологічно «Золотий щит» передбачає наступні методи фільтрації:

1. Блокування IP-Адреси;
2. Фільтрація DNS-Запитів і їхня переадресація;
3. Блокування інтернет-адреси (URL);
4. Фільтрація на етапі пересилання пакетів;
5. Блокування з'єднань, здійснюваних через VPN.

Таким чином, «Золотий щит» сполучає у собі практично всі можливі на сьогоднішній день технічні методи фільтрації, використовуючи їх вибірково стосовно тих або інших ресурсів. Це підвищує гнучкість і точність інтернет-цензури: одні ресурси можуть блокуватися повністю, а інші лише частково. Аналіз пакетів і блокування VPN і TOR-з'єднань, у свою чергу, ускладнюють обхід державних фільтрів для рядових користувачів.

Втім, незважаючи на розхоже представлення, китайські інтернет-користувачі зовсім не страждають від недостачі сервісів комунікації. З моменту запуску системи «Золотий щит» найкрупніші локальні компанії безупинно копіюють найбільш успішні західні інтернет-продукти. Так, у Китаї існують практично повні (а найчастіше навіть удосконалені) аналоги сервісів Google (Baidu), Facebook (RenRen), Twitter (Sina Weibo), YouTube (Tudou, YouKu), Wikipedia (Baike). Аналогами комерційних сервісів Amazon і eBay є, відповідно, портали Dangdang і Taobao.

Масштаби використання даних сервісів колосальні, так, сервісом мікроблогів Sina Weibo регулярно користуються приблизно 300 млн. чоловік, що перевищує аналогічний показник усього світового Twitter. Більшість суспільно-політичних дискусій, що відбуваються в китайському сегменті Інтернету, зосереджені переважно в цьому сервісі, причиною чого частково є особливості китайської мови (1 китайський твіт з 140 символів дорівнює по кількості інформації приблизно 4 англійським), а також реалізована система коментарів до твітів, що більше нагадує Facebook. Таким чином, з погляду змістовної насиченості китайські мікроблоги скоріше ближче до «великого» блогосферу, ніж до «твіттеру» у російському й американському його розумінні.

Незважаючи на те, що основний вантаж цензури лежить на другому й третьому рівнях системи, вони були б неможливі без існування «Золотого щита». Ключове завдання цього державного «фаєрвола» - це не блокування доступу китайських користувачів до політичної інформації, розміщеної на закордонних сайтах, а створення умов для державного контролю над ключовими учасниками китайського інтернет-ринку. Саме тому блокуванню піддаються, насамперед, глобальні соціальні сервіси, призначені для обміну інформацією між людьми, а аж ніяк не політичні ресурси.

Завданням китайського уряду є максимізація можливостей по керуванню тим, що і як публікується в національному сегменті Інтернету без тотального обмеження громадян на самовираження у Мережі. «Золотий щит» вирішує це завдання, створюючи ситуацію, при якій найбільші пошукові системи й соціальні сервіси належать китайським компаніям (переважно приватним) і розташовані на китайських серверах. Тим самим, головний «важіль» завжди перебуває в руках держави.

Блокування пошуку небажаної інформації

На всі пошукові системи, що працюють у китайському сегменті Інтернету, поширюються правила фільтрації пошукової видачі по ряду ключових запитів.

Можливо розділити всі заблоковані ключові фрази на дві групи: постійні й тимчасові. Постійне блокування стосується найбільш чутливих тим, пов'язаних із критикою Комуністичної партії Китаю й питанням прав людини. Приклади постійно заблокованих ключових слів: «демократія», «права людини», «диктатура», «мітинг», «червоний терор», «репресії», «незалежність Тибету» і ін. Також у списку заблокованих пошукових запитів більшість імен китайських дисидентів і лідерів забороненого релігійного культу Фалуньгун. Примітно, що серед заблокованих пошукових запитів є й словосполучення «китайсько-російська границя», що пов'язане з поширеною критикою на адресу уряду з боку користувачів, що врахували демаркацію границі між двома країнами зрадництвом національних інтересів.

Тимчасовому блокуванню піддаються слова й фрази, пов'язані з обмеженими в часі кризовими ситуаціями, поза залежністю від їхнього характеру. Мова може йти про політичні виступи, екологічні нещастя або корупційні скандали.

Пошукові обмеження поширюються не тільки на спеціалізовані пошукові системи. Аналогічні правила діють і в найкрупніших китайських соціальних сервісах, зокрема, у сервісі мікроблогів Sina Weibo.

Фільтрація контенту в соціальних медіа

Незважаючи на те, що в публічному полі переважно обговорюється «Великий китайський фаєрволл», ключову роль у фільтрації контенту грає зовсім не він, а десятки тисяч інтернет-цензорів, які вручну переглядають і фільтрують повідомлення, що публікуються сотнями мільйонів китайських інтернет-користувачів у блогах і соціальних мережах.

За останні роки було опубліковано два ключових дослідження, що дозволяють зрозуміти, як працює ця система: «How Censorship in China Allows Government Criticism but Silences Collective Expression», опублікований в American Political Science Review гарвардськими професорами Гаррі Кінгом, Дженніфером Пеном, Маргарет Робертс, і «Tracking and Quantifying Censorship

on a Chinese Microblogging Site», підготовлений групою американських дослідників під керівництвом китайського незалежного експерта Тао Жу. В обох випадках аналіз проводився переважно на основі сервісу мікроблогів Sina Weibo, як найбільш значимий інтернет-сервіс для суспільно-політичних дискусій у Сінетє (самоназва китайського сегмента Мережі).

В обох випадках дослідники прийшли до висновку про те, що принципи функціонування й завдання китайської інтернет-цензури не так прості, як це прийнято вважати. Аналіз фільтрованих повідомлень показав, що метою китайської інтернет-цензури не є тотальне викорінювання якої-небудь політичної або громадської критики в соціальних мережах. Китайські користувачі не менше інших, у тому числі й російських, залишають критичні повідомлення на адресу уряду й чиновників, і ці повідомлення не цензоруються.

Цензори починають діяти, коли негативний для китайської влади інформаційний привід здобуває «вірусні» риси, загрожуючи перерости в масові політичні виступи, паніку або політичний рух, у тому числі, віртуальний. Завданням є «зрізати» інформаційну хвилю, знизивши масштаб і гарячковість обговорення. І, у цілому, китайським «інтернет-поліцейським» це найчастіше вдається.

Ця система складається з декількох рівнів:

1. Урядові інтернет-цензори;
2. Регіональні інтернет-цензори;
3. Цензори усередині великих інтернет-компаній

Китайський уряд не розкриває дані про чисельність підрозділів «інтернет-поліції», але за різними даними на рівні уряду й регіональних центрів чисельність цензорів становить від 20 000 до 50 000 чоловік. У той же час, основну роботу виконують не вони, а цензори, що працюють усередині інтернет-компаній. У найбільших компаніях, таких як Sina і Tencent, чисельність співробітників, у чиї обов'язки входить фільтрація контенту, досягає тисячі чоловік.

За допомогою масштабного аналізу й залучення складного технічного інструментарію американськими дослідниками був виявлений як перелік тем, що підлягають цензуруванню, так і різні параметри, пов'язані з фільтрацією контенту.

Логіка втручання наступна: як тільки кількість повідомлень по якійсь темі починає різко зростати, а сама тема здобуває характер «інформаційної хвилі», цензори вживають заходів для руйнування комунікативних зв'язків між користувачами й перешкоджають подальшому обговоренню теми. Через нетривалий час, користувачі, що позбулися можливості публікувати й/або одержувати відгук аудиторії на свої повідомлення з боку інших користувачів, починають втрачати інтерес до теми.

У той же час, у спокійній інформаційній ситуації, що не передвіщає масових політичних виступів і інформаційних скандалів, критика уряду, регіональних чиновників і різних явищ суспільно-політичного життя не забороняється. Більше того, на думку ряду дослідників, китайський уряд з більшою увагою ставиться до критичних публікацій блогерів, особливо в частині критики регіональних чиновників, сприймаючи це як один із ключових елементів необхідного «зворотного зв'язку» для керування країною.

Інструменти фільтрації контенту в рамках Sina Weibo можна розділити на три категорії: проактивні, реактивні та інші.

- До проактивних інструментів фільтрації належать:

Запобігання відправлення повідомлень. У цьому випадку при відправленні повідомлення Weibo інформує користувача, що в повідомленні міститься контент, що порушує правила сервісу й не може бути опублікований.

Премодерація повідомлень. У цьому випадку Weibo приймає до відправлення повідомлення, однак інформує користувача, що воно буде опубліковано протягом декількох хвилин. Цей час потрібно для ручної перевірки контенту цензорами.

Приховання повідомлень від інших користувачів при публікації. Weibo публікує повідомлення, однак робить його невидимим для інших користувачів. У

цьому випадку автор повідомлення ніяк не інформується про подібний статус його публікації.

- Реактивні інструменти:

Видалення раніше опублікованих повідомлень. Разом з оригінальним повідомленням віддаляються протягом декількох хвилин і всі «репости» і коментарі до нього.

Закриття аккаунтів найбільше «шкідливих» користувачів.

- Інше:

Обмеження пошуку по сервісу мікроблогів.

При «реактивному» видаленні повідомлень по темі, велика їхня кількість видаляється протягом години після публікації. Приблизно 90% повідомлень, що цензоруються, включаючи репости й коментарі, видаляються протягом доби після їхньої публікації.

Втім, китайські користувачі соціальних сервісів швидко навчилися обходити обмеження блокування тих або інших слів і виразів за допомогою особливостей китайської мови. Так, ієрогліф «цензура» у Мережі заміняють ієрогліфом «річковий краб», що при різному написанні однаково вимовляється. Аналогічна ситуація й з іншими формально забороненими словами. Втім, подібні виверти можуть утруднити роботу цензорів, але не роблять її неможливою. При виникненні кризової інформаційної ситуації замаскований контент також піддається видаленню.

При виникненні потенційно небезпечної «інформаційної хвилі» уживають заходи не тільки спрямовані на фільтрацію окремих повідомлень, але й на ліквідацію ключових джерел негативної інформації. Акаунти найбільш активних блогерів видаляються, а самі вони можуть піддатися переслідуванню з боку правоохоронних органів. Втім, строки арешту для блогерів, як правило, невеликі - від декількох днів до місяця.

Зрозуміло, цензори не в змозі вручну відслідковувати абсолютно всі повідомлення, що публікуються в системі мікроблогів. Моніторинг здійснюється двома шляхами. По-перше, за допомогою пошуку ключових слів, що належать

до фільтрованої теми, включаючи слова-замінники, використовувані користувачами для обходу системи фільтрації контенту. Другий спосіб - це персональний моніторинг найбільше «неблагонадійних» користувачів, раніше помічених в обговоренні чутливих для китайської влади тем. Їхній поведінці приділяється найбільш пильна увага.

Американським дослідникам удалося виділити теми, повідомлення з яких піддавалися цензурі в період з липня по серпень 2012 року:

Антиросійські й антикитайські заяви сірійських бойовиків;

Екологічні протести в східному Китаї із приводу будівництва трубопроводу;

Повторний арешт Чі правозахисника Гуіжі;

Фотографії групового сексу за участю регіональних чиновників;

Побиття японського кореспондента, що брав інтерв'ю в учасників політичних протестів;

Слух про обвалення однієї зі станцій метро в Пекіні;

Обговорення висловлень колишнього прем'єр-міністра Китаю Вена Дзябао про політичні реформи в Китаї в ефірі телеканалу CNN;

Протести в Гонконгу проти введеного в школах курсу «національної освіти»;

Смерть матері й дитини в результаті примусового аборту, зробленого в рамках політики «одна родина - одна дитина».

Як уже було сказано вище, повідомлення з вищевказаних тем цензоруються рівно в той момент, коли вони набули характер «інформаційної хвилі» і могли привести до масових виступів. Після того як розпалювання теми спадає, активність цензорів поступово припиняється. Простежити це дозволяють дані з роботи How Censorship in China Allows Government Criticism but Silences Collective Expression, зібрані в 2011 році:

Варто відзначити, що подібна система цензури існує не тільки в Sina Weibo і інших великих загальнонаціональних інтернет-сервісах. Цензоруються й повідомлення, що залишаються на численних й популярних в Китаї регіональних

і муніципальних інтернет-форумах. У цьому випадку процес видалення небажаних записів займає трохи більше часу, але однаково переважна більшість небажаного контенту віддаляється протягом доби.

Втім, незважаючи на наявність настільки масштабної й багаторівневої системи контролю за контентом у Мережі, китайські влади регулярно виступають із ініціативами по введенню нових елементів, покликаних відгородити громадян від небажаної інформації. Найцікавішою ініціативою подібного роду можна назвати програмний комплекс «Зелена дамба», запущений в 2009 році.

Передбачалося, що встановлення даної програми буде обов'язкове на всіх персональних комп'ютерах, які були у продажу в Китаї з 1 липня 2009 року. Однак спершу уряд КНР вирішив відкласти дату запуску системи через численні технічні проблеми і той факт, що виробники комп'ютерів не встигали встановити програму на свою продукцію. Втім, уже в серпні 2009 року було ухвалене рішення зробити встановлення «Зеленої дамби» необов'язковим, а до кінця 2010 року уряд відмовився від даного проекту зовсім, пообіцявши, однак, що в майбутньому повернеться до цього питання.

Наприкінці 2012 року була почата ще одна спроба посилення державного контролю над інтернет-простором. Влади Китаю вирішили скористатися досвідом сусідньої Південної Кореї й провести масштабну деанонімізацію китайської блогосфери. Був прийнятий закон, що зобов'язує користувачів реєструватися в соціальних сервісах, таких як Sina Weibo, під своїми справжніми іменами. Ті користувачі, які зареєструвалися раніше, також повинні були повідомити свої паспортні дані операторам сервісів. Втім, через деякий час з'ясувалося, що недотримання даної норми не приводить до яких-небудь санкцій, тому значна частина блогерів зволіла зберегти свій анонімний статус.

Моделі цензури в Інтернеті

Закони, що регулюють Інтернет, застосовувані методи фільтрації і контент, що блокується, специфічні для кожної держави. Проте, існують групи країн, які переслідують схожі цілі в питаннях інтернет-цензури. На підставі спільності завдань і доводів, що використовують ці країни для обґрунтування втручання в Інтернет, а також схожості інструментів, які вирішують дане завдання, можливо виділити 5 моделей цензури. При цьому окремі держави можуть демонструвати характерні ознаки відразу двох моделей.

Азіатська модель

Характерна риса: розпливчасте визначення категорій контенту, що блокується, який надає уряду широкі можливості в галузі цензури.

Приклади країн: Китай, В'єтнам, Південна Корея, Сінгапур.

Мета і завдання фільтрації Інтернету: Незважаючи на істотні розходження в політичному устрої зазначених держав, загальною рисою цих країн є переважна точка зору на головну роль держави, що повинна обмежувати доступ своїх громадян до небажаної інформації. Закони, що регулюють Інтернет, прямо вказують на головну роль держави в охороні суспільних відносин і національної безпеки. У Китаї визначені 9 категорій інформації, що розглядається як шкідлива, у тому числі для «національної єдності». В'єтнам забороняє «зловживання демократичними свободами на шкоду інтересам держави». Південна Корея - інформацію, що порушує «громадський спокій і порядок, мораль і гарні традиції». У Сінгапурі завданням агентства, що регулює пресу, є запобігання появи матеріалів «проти суспільних інтересів, порядку й національної гармонії».

Категорії контенту, що блокується: Розпливчасте визначення матеріалу, який вважається забороненим, дає урядам країн широкі повноваження в трактуванні законів. Пріоритет віддається політичному контенту й інформації, що блокується по міркуванням безпеки. Китай фільтрує самий широкий спектр чутливих тем - починаючи від незалежності Тайваню й закінчуючи духовним рухом Фалуньгун. Особливо ретельно блокуються міжнародні сайти, що містять

критику Комуністичної партії Китаю, і популярні соціальні сервіси. Схожа картина спостерігається й у В'єтнамі, де головним об'єктом цензури виступають сайти, що піддають сумніву керівну роль його влади. Південна Корея блокує вузьку категорію контенту, але робить це з високою ефективністю - під забороною все, що пов'язано з північним сусідом, а також окремі антидержавні матеріали.

Крім боротьби із сайтами в Інтернеті, карному переслідуванню піддаються користувачі, що залишають повідомлення з похвалою Північної Кореї в соціальних мережах. У Південній Кореї також активно борються з порушеннями авторських прав - з 2009 року там діє закон «про три попередження». Він передбачає відключення від Інтернету користувачів, систематично завантажуючих нелегальну продукцію. Влади Сінгапуру бачать одну з основних погроз у расизмі - населення острова багатонаціональне й там проживає значна кількість іноземців. В 2005 році троє користувачів були заарештовані відповідно до «Акту про підбурювання» за расистських повідомлень в Інтернеті.

Незважаючи на те, що формально порнографія належить до контенту, який фільтрується у всіх країнах цієї групи, дослідження OpenNet показало, що там недоступна незначна частина таких сайтів. Лише Китай провів в 2010 році широку кампанію по блокуванню порнографічних матеріалів і онлайн-казіно. У Сінгапурі символічно заблоковані лише кілька сайтів з порнографією.

Використовувані методи фільтрації: Основні методи, на які покладаються влади даної групи країн - самоцензура й збір інформації в Інтернеті. Всі користувачі Південної Кореї, що використовують великі сайти, донедавна повинні були реєструватися під своїм справжнім ім'ям. Сінгапур зобов'язує проходити процедуру реєстрації не тільки інтернет-провайдерів, але й користувачів, «що поширюють або обговорюють політичну або релігійну інформацію, пов'язану із Сінгапуром». І в Китаї, і у В'єтнамі урядові агентства здійснюють активне стеження в Інтернеті й регулюють роботу інтернет-провайдерів.

З огляду на те, що в цих державах користувачі неодноразово піддавалися карному переслідуванню за висловлення в Інтернеті, такі заходи дозволяють жорстко контролювати хід онлайн-дискусій. Крім цього, країни застосовують системи технічної фільтрації різної складності. Якщо Китай володіє самою сучасною на сьогоднішній день системою «Золотий щит», яка використовує всі методи фільтрації, то В'єтнам і Південна Корея покладаються на більш прості способи. Так, В'єтнам застосовує перекручування DNS-записів, а влади Південної Кореї делегують видалення небажаного контенту провайдерам.

Характерна риса систем фільтрації даної групи країн - застосування комерційного програмного забезпечення західних IT-Компаній. Саудівська Аравія й Оман використовують SmartFilter від McAfee, Катар - Netsweeper однойменної компанії. Інтернет-провайдери Індонезії блокують порнографію за допомогою HTTP проксі-серверів різних виробників. Перевагою такого підходу є те, що складання й відновлення блок-аркушів бере на себе постачальник програмного забезпечення. Як результат, Саудівській Аравії вдається блокувати значну частку порнографічних сайтів - вражаюче досягнення, якщо врахувати їхню кількість в Інтернеті. Його зворотною стороною є те, що блокується переважно англомовний контент, у той час як ресурси арабською мовою зазнають обмежень в останню чергу. Крім технічних методів, країни активно переслідують порушників законів у Мережі. Комітет із захисту журналістів визнав Саудівську Аравію однієї із самих гірших країн для блогерів - за виступи із критикою держави користувачі регулярно піддаються карному переслідуванню. Катар і Оман прибігають до арештів користувачів у менших масштабах. В Індонезії випадків карного переслідування блогерів мало - зокрема, один користувач був арештований за розміщення карикатури на пророка Мухаммеда на своїй сторінці в Facebook.

Контент, що блокується з міркувань безпеки:

- Сайти екстремістських, сепаратистських і терористичних рухів. Блокування застосовується як демократичними, так і авторитарними державами.

- Інтернет-ресурси військових супротивників. Південна Корея ретельно блокує сайти Північної Кореї. У Грузії під час і якийсь час після війни з Росією в 2008 році діяли обмеження на доступ до російських сайтів.

- Ресурси з конфіденційними даними. У США сайт Wikileaks недоступний з комп'ютерів федеральних установ. Влади Франції у квітні 2013 року зажадали від Wikipedia видалення однієї зі статей, тому що в ній містилася секретна інформація.

- Сайти онлайн-шахраїв і фінансових пірамід.

- Масове розсилання небажаної пошти (спам) і шкідливе програмне забезпечення (malware). Блокується більшістю інтернет-провайдерів, а також антивірусами й фаєрволами, установленими на комп'ютерах користувачів.

Грань між блокуванням сайтів з міркувань національної безпеки й політичною цензурою не завжди чітка. Уряд США неодноразово обвинувачували в політичному переслідуванні проекту Wikileaks і його засновника Джуліана Ассанжа. Інші країни блокують ресурси прихильників сепаратизму, навіть якщо вони перебувають винятково в політичній площині й не є екстремістськими. З іншого боку, боротьба із шахрайством, спамом і шкідливими програмами є рутинною технічною роботою із забезпечення нормального функціонування Інтернету.

- Сайти й сервіси, що порушують економічні інтереси

- Сайти, що порушують інтелектуальну власність. Особливо жорстке законодавство в цій сфері діє в США. Великі пошукові системи, зокрема Google, фільтрують результати пошуку з урахуванням скарг правовласників.

- Файлообмінні сайти, програми й торрент-трекери. В 2012 році під тиском американської влади був заблокований на той момент один із самих відвідуваних сайтів Інтернету - файлообмінний сервіс MegaUpload, а його творці були арештовані. Широко висвітлюється боротьба з торрент-трекерами (The Pirate Bay, Demonoid, IsoHunt), які формально не порушують закон, але сприяють нелегальному поширенню інтелектуальної власності.

- VoIP (Voice-over-IP) програми й сервіси, що дозволяють передавати голос по Інтернету, такі як Skype і «Mail.Ru Агент». В Об'єднаних Арабських Еміратах і Омані використання таких програм нелегальне й карається великим штрафом або тюремним ув'язненням. Причина блокування VoIP програм двояка - з однієї сторони дзвінки по них складніше відстежити й прослухати, з іншого боку, їхнє використання веде до збитків компаній стаціонарного й стільникового зв'язку, які найчастіше пов'язані із правлячими колами.

- Інтернет-інструменти й соціальні сервіси. Інструменти, що дозволяють обходити інтернет-цензуру. У цю категорію потрапляють анонімайзери й сайти зі списками проксі-серверів, тому що вони можуть бути використані для обходу державних фільтрів.

- Хакерські сайти й ресурси з інформацією про обхід інтернет-цензури.

- Соціальні мережі, площадки для блогів і мікроблогів, хостинги відео й зображень. У Китаї заблокований Twitter, Facebook, YouTube, WordPress і ряд інших подібних ресурсів, сервери яких розташовані за кордоном. У такий спосіб китайський уряд примушує своїх користувачів використовувати місцеві сервіси, які легше контролювати й фільтрувати інформацію у контенті.

- Пошукові системи. Так, у Китаї й на Кубі блокуються американські пошукові системи Google і Bing.

- Безкоштовні поштові сервіси.

- Онлайн-перекладачі. Вони можуть бути використані як проксі-сервери для обходу цензури. Крім цього, з їхньою допомогою користувачі можуть одержати доступ до небажаної інформації на іноземних мовах, яку складно відстежити.

Класифікація систем фільтрації Інтернету

Дослідження Дерека Бамбаура з Університету Арізони, проведене в 2008 році, пропонує класифікацію інтернет-фільтрів, що абстрагується від характеру блокованого контенту. Замість цього системи оцінюються з чотирьох параметрів - відкритість, прозорість, точність і підзвітність. Такий підхід дозволяє найбільш

повно оцінити, наскільки практика держави відповідає заявленим цілям фільтрації, і чи порушується право громадян на інформацію.

Відкритість. Цей параметр оцінює те, наскільки явно держава визнає фільтрацію Інтернету й пояснює свою мотивацію. Так, на сайті підрозділу уряду Саудівської Аравії, що займається Інтернетом, описана діюча система фільтрації. В якості пояснення, чому уряд вважає за необхідне блокувати певний матеріал, приводяться цитати з Корану й посилання на статті. При спробі відвідати небажаний ресурс, користувачеві видається сторінка із вказівкою того, що даний матеріал заблокований. У Китаї, навпроти, значна частина фільтрації здійснюється непомітно, а її застосування маскується під технічні помилки. У результаті цього, користувач може в принципі не усвідомлювати, який матеріал блокується й чому, тому що китайські влади офіційно не визнають окремі епізоди цензури. Таким чином, незважаючи на всю свою жорсткість, система Саудівської Аравії набагато більш відкрита, чим китайська - користувачів повідомляють, що держава втручається в Інтернет, і пояснюють чому.

Прозорість. Параметр прозорості оцінює, наскільки чітко прописані критерії, за яких матеріал підлягає фільтрації. У законах Китаю для цього використовуються розпливчасті формулювання начебто «чутки, що поширюються» і «порушення національної єдності», які дозволяють блокувати будь-який матеріал, що не влаштовує цензорів. Франція блокує доступ до сайтів, що розпалюють міжнаціональну й релігійну ворожнечу. Критерії для визначення такого роду матеріалу є частиною карного законодавства країни, тому можливості для зловживання обмежені. Разом, критерії відкритості й прозорості дозволяють визначити, на який рівень контролю інформації претендують влади країни.

Точність. Параметр точності дозволяє оцінити наскільки успішно втілюється заявлена державою політика в галузі інтернет-цензури. Невід'ємною проблемою більшості методів інтернет-фільтрації є надмірне й недостатнє блокування. При надмірному блокуванні разом з небажаним матеріалом недоступним виявляється й цілком нейтральний. Подібне можливо було

спостерігати в Росії, коли разом із заблокованими ресурсами недоступними ставали й сторонні сайти, що розташовуються на одній групі серверів. Зворотний ефект спостерігається при недостатньому блокуванні - користувачі можуть бачити той контент, що держава розглядає як шкідливий. І надмірне, і недостатнє блокування може бути випадковим і навмисним. Приміром, мав місце випадок, коли провайдер у Пенсільванії помилково заблокував більше мільйона сайтів, виконуючи розпорядження суду про обмеження доступу до 400 сайтів, що містять дитячу порнографію. У Сінгапурі, навпроти, незважаючи на заявлену державою боротьбу з онлайн-порнографією, символічно заблоковані тільки кілька сайтів.

Підзвітність. Даний параметр оцінює рівень участі громадян у політику інтернет-фільтрації, що здійснюється державою. Чи пройшов закон, що регулює Інтернет, належний суспільний контроль і обговорення? Чи можуть користувачі оспорити те або інше рішення цензорів або, навпроти, внести на розгляд сайт, що порушує закон? Закон США про авторське право в цифрову епоху (Digital Millennium Copyright Act), що регулює захист авторських прав в Інтернеті, був прийнятий після серії публічних слухань і розгляду в Конгресі. З іншого боку, політика регулювання Інтернету в Саудівській Аравії була прийнята без демократичної участі її громадян, що взагалі характерно для цієї країни. Але при цьому жителі Саудівської Аравії можуть внести на розгляд сайти для фільтрації або оспорити рішення блокувати певний ресурс. Таким чином, участь громадян можлива й при авторитарних політичних режимах.

Методи цензури контенту в Інтернеті

Збір інформації в Інтернеті

Хоча сам по собі збір інформації в Інтернеті не належить до фільтрації контенту, отримані таким методом дані можуть бути використані для виявлення користувачів, що одержують доступ до забороненого матеріалу, сайтів, що містять такі матеріали, і способів обходу інтернет-фільтрів.

Зберігання логів і іншої технічної інформації. У більшості країн уведені закони, що зобов'язують інтернет-провайдерів зберігати інформацію про користувачів і відвіданих ними ресурсів. Поліція й спецслужби можуть використовувати цю інформацію для встановлення особистості порушників в Інтернеті.

Спостереження за інтернет-кафе. З метою запобігання використання інтернет-кафе для нелегальної діяльності в ряді країн до їхніх власників пред'являються жорсткі вимоги по забезпеченню безпеки. Так, у Китаї й Італії користуватися інтернет-кафе можна тільки при пред'явленні паспорта, а власники зобов'язані зберігати записи про користувачів. У В'єтнамі й Бірмі в кожному інтернет-кафе повинна бути встановлена відеокамера.

Системи інтернет-стеження. Можливості з відстеження інтернет-трафіка передбачені законодавством практично всіх країн світу. У Росії діє СОРМ-2, що зобов'язує провайдерів установлювати спеціальний пристрій, що дозволяє спецслужбам відслідковувати трафік окремих користувачів. Аналогічна система за назвою CALEA діє й у США. Особливий інтерес представляють системи, здатні вивчати трафік цілої країни, використовуючи технологію глибокого аналізу пакетів (Deep Packet Inspection). За допомогою подібних систем можливо здійснювати спостереження за активністю користувачів, наприклад, визначаючи які додатки й сервіси вони використовують і яку інформацію пересилають. Застосування таких систем суперечить праву громадян на приватне життя й заборонене в ЄС і Росії. Проте, у цей час на міждержавному рівні ведуться дебати про допустимість їхнього застосування з метою боротьби з тероризмом і порушенням авторських прав. Оскільки вивчення трафіка цілої країни вимагає значних обчислювальних потужностей, дозволити собі системи масового спостереження за Інтернетом можуть не всі держави. У США Агентство національної безпеки в рамках «Патріотичного акту» відслідковує активність у Мережі за допомогою суперкомп'ютерів NarusInsight. Китай використовує глибокий аналіз пакетів з метою інтернет-цензури; серед інших країн, помічених у такому застосуванні технології - Іран і Туніс.

Технічні методи

Блокування за IP-адресою. При застосуванні даного методу сервер, на якому перебуває небажаний матеріал, стає повністю недоступним для користувача. Головною перевагою цього методу є його простота - він може бути реалізований за допомогою базового мережевого обладнання, що використовується інтернет-провайдерами. Однак з урахуванням сучасних технологій за однією IP-адресою можуть знаходитися тисячі сайтів, а також інших сервісів, таких як FTP або електронна пошта, тому його блокування приведе до того, що всі вони стануть недоступними. Через низьку точність даного методу країни застосовують його з обережністю. Блокування за IP-адресою легко обходиться за допомогою різних технічних рішень, зокрема, проксі-серверів і VPN.

Перекручування DNS-Записів. При звертанні користувача до будь-якого сайту, комп'ютер надсилає запит до DNS-серверу для того, щоб перетворити доменне ім'я в IP-адресу. У випадку застосування даного методу, DNS-сервер повертає невірну адресу, і сайт виявляється недоступним. Перекручування DNS-Запису також може бути реалізоване без застосування додаткового встаткування. Її перевагою перед блокуванням за IP-адресою є більш висока точність - недоступним стає тільки один сайт на сервері. При цьому все рівно відбувається надмірне блокування. Наприклад, Китай періодично позбавляє своїх користувачів доступу до CNN International через небажані новини, які там з'являються. Хоча ставиться ціль фільтрації тільки однієї сторінки новини, інші сторінки сайту також стають недоступними. Перекручування DNS-записів легко обходиться користувачами - у настроюваннях браузера досить указати альтернативний DNS-сервер або вручну прописати IP-адресу заблокованого сайту.

Блокування за URL-адресою. В HTTP-протоколі URL-адреса містить доменне ім'я сайту, а також параметри запиту. Вони можуть бути звірені зі списком заблокованих ключових слів, і у випадку відповідності, зв'язок

користувача із запитаним ресурсом розривається, або він перенаправляється на блок-сторінку. Даний метод є більш ефективним у порівнянні із блокуванням за IP-адресою й перекручуванням DNS-запису, але вимагає додаткового устаткування, тому що він використовує поверхневий аналіз пакетів. Його додатковою перевагою є те, що він здатний динамічно блокувати нові сторінки, якщо в їхній адресі містяться заборонені слова. Наприклад, у Китаї блокуються всі запити, що містять слова “falun” і “gong”. Однак при неправильному настроюванні ключових слів точність методу різко погіршується - він може пропускати небажаний матеріал або, навпаки, допускати надмірне блокування. Блокування по URL-адресі не можна обійти за допомогою звичайних проксі-серверів - необхідні інструменти, які шифрують трафік, такі як VPN або TOR.

Пакетна фільтрація. Найбільш складний і дорогий метод, тому що він вимагає застосування глибокого аналізу пакетів. На даний момент повноцінно реалізований тільки в Китаї. При використанні пакетної фільтрації, вивчаються не тільки заголовки пакетів, що містять URL-адресу, але й весь їхній зміст. У випадку наявності заборонених слів, зв'язок між користувачем і сервером розривається. Метод дозволяє фільтрувати небажаний контент не тільки у веб-сторінках, але й у всіх протоколах - електронній пошті, сервісах миттєвих повідомленнях та ін. Істотним недоліком даного методу є те, що застосування глибокого аналізу пакетів може привести до зниження швидкості інтернет-з'єднання, що спостерігається при доступі з Китаю до закордонних інтернет-серверам. В цілому, пакетна фільтрація має ті ж достоїнства й недоліки, що й блокування за URL-адресою.

Фільтрація через HTTP проксі-сервер. Даний метод найчастіше використовується організаціями для підключення корпоративних мереж до Інтернету, але його можна використовувати для фільтрації інтернету в рамках всієї країни. Гібридний варіант за назвою Cleanfeed ефективно застосовується у Великобританії й Канаді для боротьби з дитячою порнографією. Кожний запит користувача звіряється зі списком IP-адрес, що містять заборонені матеріали. Якщо збігів немає, то запит користувача відсилається прямо. У противному

випадку, він перенаправляється на проксі-сервер громадської організації Internet Watch Foundation. Проксі-сервер одержує запитувану сторінку й аналізує її на наявність дитячої порнографії. Якщо сторінка не містить заборонених матеріалів, то користувач одержує до неї доступ, інакше - створюється видимість, що ресурс недоступний. Гібридні варіанти фільтрації через HTTP проксі-сервер дозволяють при низькій вартості точно блокувати вузькі категорії контенту. При цьому, вони настільки ж легко обходяться, як і фільтрація за IP-адресою.

Порушення роботи мережі. В екстрених випадках, таких як масові безладдя, влади країни можуть піти на повне або часткове відключення Інтернету. Досягається це шляхом фізичного відключення роутерів з Мережі або ж зміни їхніх настроювань, через що більша частина з'єднань скидається. Даний метод застосовувався в Єгипті в ході безладь 2011 року, Лівії, Сирії й Бірмі. Проте, досвід використання даного методу в ряді країн показує, що повне блокування доступу в Мережу найчастіше провокує додатковий ріст масових безладь.

Фільтрація результатів пошуку. У ряді країн, таких як Китай, Франція й Німеччина, працюючи там пошукові системи зобов'язані виключати з результатів пошуку посилання на заборонені матеріали. Так, у французьких і німецьких версіях Google з пошукових результатів виключаються посилання на неонацистські групи й інші матеріали, заборонені законом. Таким чином, користувачі не можуть знайти небажаний контент. Фільтрація результатів пошуку - один з основних методів боротьби з порушеннями авторських прав в Інтернеті. Метод обходиться використанням інших пошукових систем - наприклад, міжнародна версія Google не виключає з результатів сайти неонацистських угруповань і при цьому доступна із Франції й Німеччини.

Варіанти розміщення систем технічної фільтрації

Обов'язковою умовою установки інтернет-фільтрів є їхнє розміщення на ключових ділянках мережі, через які проходить весь трафік. Тому можливі наступні рівні установки інтернет-фільтрів:

Міжнародний шлюз. Цей варіант припускає централізований підхід до фільтрації контенту. Програмне й апаратне забезпечення встановлюється на ділянці, що з'єднує національну мережу з міжнародними магістралями. Перевагою даного методу є більш повний контроль і єдиноподібність підходу до цензури - політика фільтрації може оперативно коректуватися, а її зміни будуть торкатися відразу всіх користувачів. Однак, створення централізованої системи фільтрації Інтернету, здатної точно блокувати небажаний контент, вимагає істотних витрат, пропорційних обсягу зовнішнього трафіка. Даний метод використовуються більшістю мусульманських країн Близького сходу. У Китаї, Пакистані, Узбекистані й Ірані він застосовується разом з фільтрацією на рівні інтернет-провайдерів.

Інтернет-Провайдери. Іншим підходом до цензури в Інтернеті є установка систем фільтрації всіма провайдерами країни. З питання, які ресурси підлягають блокуванню, вони орієнтуються на рішення судів, або на реєстр, що ведуть державні або недержавні органи. У випадку якщо методи фільтрації не регламентуються, їхня реалізація залишається на розсуд кожної компанії. У результаті, практика фільтрації може істотно варіюватися від провайдера до провайдера, як убік надлишкового, так і недостатнього блокування. Зокрема, у Росії через некоректну реалізацію вимог закону 139-ФЗ окремими компаніями, для їхніх користувачів виявилися недоступні всі блоги на платформі WordPress. Фільтрація на рівні інтернет-провайдерів застосовується більшістю європейських країн, а також В'єтнамом, Бірмою й Південною Кореєю й рядом інших держав.

Інтернет-Сайти й мережі організацій. Фільтрація на рівні мереж організацій найчастіше застосовується приватними компаніями для контролю використання Інтернету своїми співробітниками, але також використовується державами для регулювання роботи шкіл, бібліотек і урядових закладів. Так, у США відповідно до Акту про захист дітей в Інтернеті умовою одержання державних субсидій для шкіл і бібліотек є встановлення фільтрів, що обмежує доступ неповнолітніх до порнографії. Оскільки вимога не є обов'язковою для

всіх установ, а закон передбачає відключення фільтрів на прохання дорослих користувачів, Акт не обмежує свободу слова, закріплену в Конституції США.

У державах, де за законом інтернет-сайти й сервіси відповідають за контент, розташований за їх користувачами, їхні власники наймають співробітників, відповідальних за цензуру, і встановлюють спеціальне програмне забезпечення, що відслідковує заборонений контент. Наприклад, в Китаї блог-платформа компанії Microsoft MSN Spaces не допускала назви блогів, що містять слова «демократія» і «свобода», автоматично відхиляючи такі варіанти. Сервіс мікроблогів Sina Weibo блокує записи з великого набору ключових слів, а в його штаті значаться сотні співробітників, що здійснюють цензуру вручну.

Індивідуальні комп'ютери. Даний підхід передбачає встановлення програмного забезпечення для фільтрації безпосередньо на комп'ютери користувачів. Головною проблемою тут є труднощі відстеження того, щоб користувач не видалив або відключив фільтр. З урахуванням цього, найчастіше індивідуальні фільтри використовуються на комп'ютерах приватних компаній, які можуть технічно обмежити права своїх співробітників вносити зміни в настроювання, а також батьками для захисту дітей від небажаного контенту у Мережі. Спроби застосовувати даний підхід для державної цензури робив Китай. У планах його влади було встановлення програмного забезпечення «Зелена дамба»на всі комп'ютери країни, що блокує доступ до віддалено обновлюваного списку сайтів і здатного розпізнавати порнографічні зображення. Але через численні технічні труднощі державні органи відмовилися від цієї ініціативи.

Пошук інформації у мережі Інтернет, пов’язаної з роботою ресурсів, що використовуються для вчинення злочинів

Інтернет, як специфічне соціальне середовище, має низку особливостей, які значно ускладнюють контроль з боку правоохоронних структур. До таких особливостей можна віднести відсутність географічних обмежень, відсутність системи автентифікації користувачів, що надає змогу в більшості випадків діяти

анонімно. Такі особливості все частіше спокушають зловмисників до опанування можливостей мережі Інтернет з метою вчинення злочинів.

Стратегія протидії злочинам, як правило, полягає у необхідності попереднього проведення комп'ютерної розвідки з метою виявлення і встановлення осіб, які причетні до їх вчинення, з подальшою їх оперативною розробкою традиційними методами.

Виявлення інтернет-ресурсів, що використовуються для вчинення злочинів, здійснюється, окрім застосування класичних оперативно-розшукових методів (надання завдань особам, які конфіденційно співробітничають з ОВС, на виявлення осіб, що організовують роботу таких ресурсів), також шляхом самостійного пошуку оголошень або інформаційних повідомлень в мережі Інтернет від осіб, які можуть бути причетні до злочинної діяльності.

З метою пошуку інформації кримінального характеру в мережі Інтернет, найдоцільнішим є використання пошукових систем. Це можуть бути як повідомлення на публічних он-лайн ресурсах (форуми, дошки оголошень, соціальні мережі, блоги), так і сайти, спеціально створені зловмисниками з метою створення умов для вчинення злочину.

На даний час, найпотужнішими пошуковими системами в українському та російському секторах Інтернету є Google та Yandex. Механізми індексації та ранжування результатів пошуку цих пошукових систем дозволяють в найкоротший час обробляти мільйони електронних документів у різних форматах з метою пошуку інформації, що цікавить суб'єкта пошуку. В залежності від виду злочинної діяльності, яку має на меті виявити оперативний працівник, в пошуковий запит необхідно включати ключові слова, характерні для даного виду діяльності.

Працівники відповідних органів повинні мати уяву про той чи інший вид злочинної діяльності і вміти складати перелік ключових слів та фраз, найбільш характерних для того чи іншого виду злочинного промислу. Оскільки переважна більшість Інтернет спільноти на території України спілкується російською мовою, доцільним буде здійснювати пошук по ключовим словам або фразам не

тільки українською, а ще також російською мовами. Наприклад, для пошуку повідомлень кримінального характеру, опублікованих потенційними особами, які вчиняють злочини у сфері незаконного обігу наркотичних засобів, характерними ключовими словами та фразами можуть бути: «трава», «баян», «колеса», «драп», «план», «дур», «трамал», «ширка», «приход», «винт», «джеф», «гера», «кокс», «белый», «полные дрова», «полный улёт» та інші їх варіації.

Крім об'яв, опублікованих у коментарях сайтів різних тематик, існує низка он-лайн ресурсів, присвячених конкретній тематиці протизаконних дій в Інтернет. Наприклад, існує чимала кількість російськомовних форумів, присвячених різновидам незаконного обігу наркотичних засобів, серед активних учасників яких, окрім осіб зі здоровим інтересом, є ряд активних зловмисників, які використовують такі форуми для підвищення кваліфікації, пошуку або подачі об'яв, пов'язаних із злочинною діяльністю по їх профілю, знайомства і пошуку потенційних співучасників злочинної діяльності, інше.

Серед таких форумів можна назвати:

1. forum.antichat.ru
2. forum.xakep.ru
3. forum.hackersoft.ru
4. http://high.ru
5. http://mjk.msk.ru/~max/greenbreath/index2.html
6. http://www.drugon.cjb.net
7. http://drugon.home.ml.org
8. http://www.narcko.newmail.ru
9. http://narckota.cjb.net
10. http://www.cannabis-sativa.i.am
11. http://www.legalize.spb.ru
12. http://www.chat.ru/~drgs
13. http://www.radicalparty.org
14. http://www.icelord.net/legalize
15. http://www.guelman.ru/pg

16. http://www.halyava.ru/zx/start/htm
17. http://www.caribase.da.ru
18. http://www.rastaman.tales.ru
19. http://www.utopia.pl.ru
20. http://www.zhurnal.ru/music/rasta
21. http://www.marihuana.da.ru
22. http://www.poets.spb.ru/ie/index.html
23. http://www.legalize.spb.ru/mountainhigh_nl
24. http://www.high.ru/cgi-bin/chat.pl
25. http://www.here.ru
26. http://imperium.lenin.ru/EOWN/eown7
27. http://www.ptuch.ru

Як правило, при перегляді повідомлень на таких форумах, можна знайти ряд повідомлень кримінального характеру, які надають можливість зв'язатися із автором у той чи інший спосіб зв'язку в мережі Інтернет.

Іншим способом пошуку осіб, які можуть бути причетними до злочинної діяльності через мережу Інтернет, є умисна публікація повідомлень про купівлю або продаж протизаконних товарів або послуг. Наприклад, працівник оперативного підрозділу, з цією метою, може створити свій власний веб-сайт, опублікувати ряд повідомлень на безкоштовних онлайн-дошках повідомлень, в коментарях до повідомлень на певних веб-сайтах, або на тематичних форумах. Для реалізації таких дій необхідно попередньо зареєструвати нову поштову скриньку на одному з безкоштовних поштових онлайн-сервісів, бажано використовувати сервіс http://mail.google.com, оскільки він більш стійкий до зламу з боку хакерів.

Під час Інтернет активності, з метою пошуку й встановлення контактів із особами, які можуть бути причетними до злочинної діяльності через мережу Інтернет, необхідно дотримуватись базових принципів конспірації. Не рекомендується використовувати службові комп'ютери та Інтернет з'єднання, оскільки, такі особи, як правило, при перших контактах, намагаються провести

додаткові контрзаходи, спрямовані на перевірку нового клієнта на причетність до правоохоронних структур. Оскільки рівень технічної підготовки таких осіб, як правило, досить високий, вони з легкістю можуть використати помилки у конспірації на свою користь. Отже, рекомендується використовувати нові комп'ютери, з новою операційною системою, не зберігати на них будь-які документи, причетні до службової діяльності та використовувати бездротовий доступ до мережі Інтернет, під час реєстрації якого не використовувалися паспортні дані, наприклад новий пакет мобільного Інтернету (модем та SIM-карта) одного з операторів мобільного зв'язку, що надають послуги мобільного Інтернету та працюють без контракту.

У такий спосіб можливий пошук та встановлення контакту з особами будь-якого злочинного профілю, починаючи від хакерів та закінчуючи торговцями людьми, які використовують мережу Інтернет в своїх злочинних цілях.

Створення інформаційних повідомлень в комп'ютерній мережі не вимагає зазвичай надання з боку користувача його дійсних установчих даних. Крім того, особи які вчиняють злочини в кіберсередовищі, зазвичай застосовують додаткові заходи своєї „анонімізації" в мережі Інтернет.

Очевидно, що головною умовою припинення злочинів, що вчинюються із використанням мережі Інтернет, є встановлення особи злочинця. Встановлення злочинця за допомогою технічних можливостей мережі, безпосередньо пов'язане із встановленням місця перебування комп'ютера або комп'ютерів, які використовує зловмисник під час сеансів виходу до мережі Інтернет. Отже, задача встановлення особи зловмисника напряму пов'язана із встановленням IP-адрес, під якими його комп'ютер працював в Інтернеті.

Зважаючи на викладене, та відповідно до описаного в даній роботі алгоритму дій, процес встановлення особи, яка розповсюджує інформацію в мережі Інтернет можна умовно поділити на такі етапи:

- пошук інформації в мережі Інтернет щодо фактів злочинної діяльності;
- встановлення провайдера Інтернет послуг, до мережі якого належить IP-адреса;

- встановлення місця знаходження комп'ютера, який мав доступ до Інтернет у вказаний час під встановленою IP-адресою.

Рекомендації щодо блокування забороненого контенту в Інтернеті

На сьогоднішній день проблеми протидії, виявлення та розслідування злочинів у сфері інформаційних технологій має глобальний, міжнародний та міжнаціональний характер. За даними Nua Internet Surveys кількість користувачів глобальної мережі Інтернет з 80 тисяч у 1988; році зросла до 2,4 мільярдів на кінець 2013 року. Зростання кількості користувачів мережі Інтернет не може не відобразитись на кількості злочинів, вчинених у сфері інформаційних технологій. Слід також зазначити, що у зв'язку з існуванням у світі значної загрози з боку комп'ютерного тероризму, дане питання актуальне на сьогодні і для України. Задачі протидії цьому закріплено в Законі України «Про основи національної безпеки України», в статті 7 якого «комп'ютерний тероризм» та «комп'ютерна злочинність» визначені серед основних потенційних та реальних загроз національній безпеці України в інформаційній сфері.

За дослідженням в Україні, на сьогоднішній день, методики виявлення і розслідування злочинів у сфері новітніх інформаційних технологій потребують подальших досліджень та наукових вивчень, а також напрацювання нових методик їх викриття та, зокрема, розслідування.

Слід надати визначення цій категорії злочинів. На нашу думку, визначення поняття цієї категорії злочинів може бути наступним: злочини у сфері інформаційних технологій – це злочини корисливої направленості, що здійснюються особами з використанням сучасних інформаційних технологій, та, зокрема, Інтернету для досягнення злочинних цілей.

На даний момент однією з найбільш нагальних проблем України є протидія поширенню в мережі Інтернет різних видів інформації расистського, ксенофобного та іншого характеру, що підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, і ґрунтується на расовій, національній, релігійній або

етнічній приналежності (в законодавстві України відповідальність за такі дії передбачена в ч.2 та ч.3 ст.109, ст.258-2, ст.295, ст.300, ст.436, ч.2 ст.442 КК України), а також дитячої порнографії та матеріалів порнографічного характеру (в законодавстві України відповідальність за такі дії передбачена в ст. 300 КК України). Проблема полягає в тому, що будь який користувач мережі Інтернет в Україні має змогу отримати доступ до електронного ресурсу, на якому розміщена зазначена вище інформація, навіть якщо він не знає назви даного Інтернет сайту. Достатньо лише ввести пошуковий запит «дивитись порнографію», чи «дивитись порно», чи «відео про вбивство» до пошукової системи, наприклад, до такої як «Google», і користувач отримає відповідь на свій запит у вигляді посилань на Інтернет ресурси, на яких і розміщена інформація, щодо якої у користувача виник інтерес. Навіть якщо батьки на домашніх комп'ютерах своїх дітей поставлять спеціальні програмні фільтри для того, щоб діти не мали змоги отримати режим доступу до заборонених батьками Інтернет ресурсів, ніщо не заважатиме дітям отримати режим доступу до цих Інтернет ресурсів з інших комп'ютерів. І це є великою проблемою для будь-якої країни, адже за таких умов в мережі Інтернет можливо розмішувати аудіо, відео, текстові та графічні матеріали будь-якого змісту, і кожен пересічний громадянин матиме змогу ознайомитись з інформацією, яка містить в собі, наприклад, заклики до повалення конституційного ладу в країні, чи відеофільм дитячої порнографії.

Якщо Інтернет сайти розміщені на комп'ютерах, які фізично перебувають на території України, та на яких розміщена інформація, розміщення та розповсюдження якої підпадає під склад певного злочину Кримінального кодексу України, то це ще невелика проблема для правоохоронних підрозділів. Але часто буває так, що такі Інтернет сайти розміщені на комп'ютерах, що фізично перебувають, наприклад, на Філіппінських островах, і тоді припинити режим доступу до таких сайтів становить проблему для українських правоохоронців.

Фізично, будь-які Інтернет ресурси розміщені на певних комп'ютерах, що розміщені по всьому світу. Для того, щоб будь-який користувач міг отримати доступ до певного ресурсу, данні про те, на якому саме комп'ютері розміщений той чи інший Інтернет сайт заносяться до спеціальних цифрових таблиць DNS серверів, які фізично

розміщені на території США. Проміжною ланкою між користувачем і DNS сервером є Інтернет провайдер, тобто юридична особа, яка платно чи безоплатно забезпечує зв'язок між користувачем, DNS сервером та Інтернет сайтом, режим доступу до якого хоче отримати користувач. На території України існує безліч Інтернет провайдерів, але їхня діяльність ґрунтується лише на законах та підзаконних актах України. А оскільки будь-який Інтернет провайдер може налаштувати програмні фільтри так, щоб користувачі підключені до нього не мали доступу до певного Інтернет сайту чи ресурсу, ми пропонуємо:

1) створити відповідний підрозділ в системі Міністерства внутрішніх справ України, на який би покладалось завдання з пошуку та виявленню Інтернет ресурсів, де розміщена інформація расистського, ксенофобного та іншого характеру, яка підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовій, національній, релігійній або етнічній приналежності, а також різних видів дитячої порнографії та матеріалів порнографічного характеру;

2) на законодавчому рівні створити Єдиний державний реєстр заборонених Інтернет ресурсів, до якого вносити Інтернет ресурси виявлені зазначеним вище підрозділом;

3) законодавчо закріпити зобов'язання Інтернет провайдерів вносити Інтернет ресурси, що потрапили до зазначеного вище Єдиного державного реєстру заборонених Інтернет ресурсів до своїх програмних фільтрів, з метою блокування режиму доступу до них користувачами мережі Інтернет;

4) зважаючи на те, що кожен день в мережі Інтернет з'являється багато нових Інтернет ресурсів, а вже існуючі можуть змінювати характер та склад інформації, яка розміщується на них - регулярно проводити обновлення Єдиного державного реєстру заборонених Інтернет ресурсів, тобто включати до нього нові Інтернет ресурси, та виключати ті, які зі свої сторінок видалили інформацію забороненого характеру.

Можна зробити висновок, що для реалізації зазначених пропозицій щодо протидії розповсюдженню забороненої законодавством інформації в мережі Інтернет і впровадження вищезазначеного, необхідно створити відповідну законодавчу і нормативно-правову базу.

Юридичні аспекти припинення роботи інтернет-ресурсів що використовуються для вчинення злочинів

Протягом останніх років Україна знаходиться у достатньо важких соціально-економічних й політичних умовах, що не в останню чергу відображається на стані злочинності. Разом із цим, в останнє десятиліття при загальному збільшенні рівня злочинності в державі, спостерігається різкий приріст злочинів, що пов'язані з використанням електронно-обчислювальної техніки (далі – ЕОМ).

Найбільш поширеними діяннями, що зустрічаються у кіберпросторі є різноманітні види втручань у роботу ЕОМ та автоматизованих систем, мереж електрозв'язку, а також використання різноманітного шкідливого контенту з метою шахрайських або інших протиправних дій.

Діючий Кримінальний кодекс України (далі – КК) передбачає ряд кримінально караних діянь, які вчинюються у сфері використання ЕОМ. Зокрема, КК містить Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», у якому законодавцем розміщено ряд складів злочинів, що безпосередньо вчинюються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Водночас, відсутність правозастосовної практики, а також належного досвіду та професіоналізму працівників правоохоронних органів, нажаль, часто дозволяють зловмисникам уникнути не лише кримінальної, але й фактично будь-якої іншої відповідальності.

Особливу проблему наразі становить використання зловмисниками окремих Інтернет-ресурсів національного та закордонного сегментів для вчинення злочинів. Таке використання може проявлятись у найрізноманітнішій формі. Основна проблема при цьому, полягає в тому, що діюче законодавство України не передбачає конкретного (та й в загалі хоча б якого-небудь) порядку припинення роботи таких ресурсів. З точки зору адміністративної діяльності,

жоден з державних суб’єктів, що діє в полі використання ЕОМ та діяльності пов’язаної з використанням мережі Інтернет, наразі немає ніяких повноважень для обмеження доступу до окремих Інтернет-ресурсів що використовуються для вчинення злочинів. У січні 2014 року законодавцем було прийнято спробу встановити повноваження Національній комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі – НКРЗІ), обмежувати доступ користувачів до ресурсів мережі інтернет на підставі висновків експертів, однак прийняті зміни втратили чинність і станом на сьогодні не діють. Відповідно, наразі існує ситуація, коли зацікавлені особи можуть безперешкодно використовувати ресурси мережі Інтернет для вчинення протиправних дій на території України, і правоохоронні органи, нажаль, не в змозі цьому запобігти.

Чинний КК, поміж іншим, не передбачає також і такого виду санкцій як «обмеження доступу або припинення роботи» Інтернет-ресурсів які використовуються для вчинення злочинів, або навіть були для цього використані в минулому. Дана особливість вкрай ускладнює ефективну роботу підрозділів правоохоронних органів у сфері телекомунікації не лише з точки зору запобігання численним порушенням та відверто злочинній діяльності, але й навіть у випадках вчинення злочинів та затримання злочинців.

Водночас, незважаючи на зазначені вище особливості, у працівників правоохоронних органів залишається можливість у певний спосіб припиняти на цілком законних підставах роботу окремих Інтернет-ресурсів українсього сегменту. При цьому, можливість легального припинення роботи Інтернет-ресурсів українсього сегменту прямо залежить від виду та способу діяльності зловмисників.

У діючому КК передбачено ряд злочинів, для яких характерним є наявність спеціального предмету. До таких складів можна віднести ст.ст.176, 301 КК в санкціях яких, окрім основного виду покарання передбачається також і «конфіскація та знищення всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм

мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення» та «конфіскація порнографічних предметів та засобів їх виготовлення і розповсюдження».

Зазначені у санкціях статей спеціальні види конфіскації, окрім додаткового покарання для зловмисників, передбачають одночасно, на етапі документування протиправних дій також й діяльність щодо забезпечення справи доказами та можливістю привести у виконання вирок. Інакше кажучи, у випадках (і це, до речі, доволі часті випадки) коли зловмисники використовують роботу Інтернет-ресурсів національного сегменту для здійснення злочинних дій, існує законна можливість припинення роботи таких ресурсів, яка повинна бути аргументована з позиції необхідності вилучення відповідних предметів злочинів, передбачених ст.176 та 301 КК України.

У всіх інших випадках, національне законодавство та повноваження державних органів у сфері телекомунікації на сьогоднішній день не дозволяють припинити роботу Інтернет-ресурсів як національного так і закордонного сегментів, навіть у випадках, якщо вони використовуються для здійснення відкрито злочинних дій.

ПЕРЕЛІК ДЖЕРЕЛ:

1. Класифікація комп’ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. – Режим доступу: http://www.cyberpol.ru/cybercrime.shtml
2. Конвенція Ради Європи про злочинність у сфорі комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5*6, ст. 71.
3. Кримінальний кодекс України за станом на 05.07.2012 року // Відомості Верховної Ради України. - 2001.
4. 15-й, 17-й, 18-й, 42-й, 47-й зводи законів США // Современное право средств массовой информации в США. - М. - 2000, С. 205-223.
5. Закон України «Про основи національної безпеки України» зі змінами та доповненнями - Відомості Верховної Ради України (ВВР), 2003, N 39, ст. 351.
6. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія *І* Д. М. Цехан ; за науковою редакцією О. О. Подобного. - Одеса: Юридична література, 2011.-216 с.
7. Офіційний сайт «Internet Assigned Numbers Authority» (IANA) [Електронний ресурс]. - Режим доступу: http://www.iana.org
8. Сервіс ідентифікації користувача за IP адресою «WHOIS» Інтернет-ресурсу «2IP.RU» [Електронний ресурс]. - Режим доступу: http://2ip.ru/whois
9. Зацеркляний М.М. Інформаційні системи і технології в діяльності правоохоронних органів: навч.посіб. / Зацеркляний М.М., Наумов В.В. - Харків: Тимченко, 2010. - 382 с. з іл.
10. Горбачов А. Електронна інформація як доказ при розслідуванні злочинів у сфері комп'ютерних технологій / А. Горбачев // Компьютерная

преступность и кибертерроризм : сб. науч. ст. — Запорожье, 2005. - Вып. 3. — С. 157.

11. Ищенко Е. П., Новые информационные технологии обеспечения раскрытия и расследования преступлений / Е. П. Ищенко // Вісник ЛДУВС. 2010. - № 1, спец. вип. № 2. - С. 3-14.
12. Захарченко В.Ю., Лазуренко В. И., Олифиров А. В., Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: Учебное пособие / Под общ. редакцией В. И. Лазуренко. - К: Центр учебной литературы, 2007. - 170 с.
13. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс]. / Комітет протидії корупції та організованої злочинності. - Режим доступу: http://kpk.org.ua/2007/02/05/ kberzlochinnst_v_ukran_perspektivi_protid.html.
14. Голубев В. А., Головин А. Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий. [Электронный ресурс]. - Режим доступа: www.crime-research.ru.
15. Голубєв В. О. Розслідування комп'ютерних злочинів: Монографія. - Запоріжжя, 2003. - С. 82-92.
16. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов международного сообщества и частного сектора // Группа экспертов для проведения всестороннего исследования киберпреступности / Вена, 25-28 февраля 2013 года: [Электронный ресурс] / UNODC/CCPCJ/EG.4 - 2013. - 21 с. - Режим доступа: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf
17. Конвенція про кіберзлочинність від 23 листоп. 2001 р. [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.
18. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю / А.В. Войціховський / Науковий журнал «Право і Безпека». - 2011. - №4. [Електронний ресурс]. - Режим доступу:

http://archive.nbuv.gov.ua/portal/soc_gum/pib/2011_4PB–4/PB–4_26.pdf

19. Про ратифікацію Конвенції про кіберзлочинність : закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. - 2006. - №5-6. - Ст. 71.
20. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. - Режим доступу: http://www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?=nreg=994_687.
21. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій: навч. посіб./ Д.О. Максимус, О.О. Юхно. – Харків: НікаНова, 2013. – 102с.