УДК:323.21

Піщевська Е. В.
Одеський національний університет
імені І. І. Мечникова

ІНТЕРНЕТ У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У даній статті досліджується Інтернет з погляду ризиків для інформаційної безпеки. Розглядається вплив Інтернет-технологій на розширення можливостей тероризму, виявляються особливості комп'ютерного тероризму, аналізується досвід закордонних країн і практика України в регулюванні Інтернет-ресурсів.

Ключові слова: *Інтернет, тероризм, міжнародний тероризм, кибертерроризм, регулювання Інтернет ресурсів.*

Пищевская Э.В.

ИНТЕРНЕТ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной статье исследуется Интернет с точки зрения рисков для информационной безопасности. Рассматривается влияние Интернет-технологий на расширение возможностей терроризма, выявляются особенности компьютерного терроризма, анализируется опыт зарубежных стран и практика Украины в регулировании Интернет-ресурсов.

Ключевые слова: *Интернет, терроризм, международный терроризм, кибертерроризм, регулирование Интернет ресурсов.*

Picshevskaya E.

INTERNET IN CONTEXT OF INFORMATION SECURITY

This article explores the Internet in terms of risks to information security. The influence of Internet technologies to enhance the capacity of terrorism, identify the characteristics of computer terrorism, examines the experience of foreign countries and the practice of Ukraine in the regulation of Internet resources.

Key words: *Internet, terrorism, international terrorism, cyberterrorism, the regulation of Internet resources.*

Основними політичними чинниками забезпечення інформаційної безпеки сучасної української держави виступають: стан інформаційної політики держави; політична культура суспільства; рівень зрілості інститутів громадянського суспільства; політична і громадська соціалізація особи; міра розвиненості інформаційно-політичних, у тому числі вибіркових технологій; політична роль засобів масової інформації (ЗМІ).

Останніми роками в науковій літературі значно зріс інтерес до аналізу можливостей і перспектив використання новітніх інформаційних технологій і Інтернету в політичній сфері. У наукових працях російських дослідників М. Г. Анохіна, В. А. Ачкасова, Л. А. Василенко, А. В. Дмітрієва, Б. З. Докторова, А. І. Кулика, В. В. Латинова, Ю. А. Нісневича, Б. В. Овчинникова, М. Ю. Павлютенкової, Д. Н. Пескова, А. В. Чугунова та ін.; українських учених О. Дубаса, Е. Емельяненка, В. Коляденка, А. Маліса, В. Недбая та ін. проведені наукові дослідження з концептуальним

обґрунтуванням ролі глобальної мережі в сучасній політології. Дійсно, в літературі на теоретичному рівні ретельно вже проаналізована роль і функції Інтернет–технологій і політичних комунікацій в Мережі. В той же час проблеми інформаційної безпеки, що виникають з появою Інтернету, розглянуті не повною мірою.

Мета даної статті – розглянути Інтернет з точки зору ризиків інформаційної безпеки. Для досягнення даної мети поставлені такі *наукові завдання:* дослідити вплив інтернет-технологій на розширення можливостей тероризму, розглянути особливості комп'ютерного тероризму, досвід зарубіжних країн у регулюванні інтернет-ресурсів.

Всесвітня мережа – джерело і одночасний засіб здобуття стратегічно важливих державних секретів. Недавно в США в ЗМІ з'явилась інформація про комп'ютерну крадіжку секретних даних Пентагону, яку нібито здійснили російські спецслужби. Заяви спецслужб про те, що могли бути вкрадені відомості про системи наведення стратегічних ракет, викликали паніку серед населення. На користь національної безпеки керівництво Пентагону прийняло рішення про відключення від Інтернету 2 млн. комп'ютерів.

Ряд небезпек пов'язаний зі спробами певних політичних сил використовувати інформаційні можливості Мережі для формування громадської думки, з метою досягнення своїх інтересів. Безумовно, що до подібного інформаційного впливу вкрай схильна найбільш масова і активна частина аудиторії Інтернету – молодь. Вона привертає сьогодні особливу увагу політиків і лідерів громадської думки. Всі вони хочуть знати, яку роль здатна (або не здатна) грати молодь в розвитку демократії ринкової економіки, громадянського суспільства і правової держави. На молодих людей буквально обрушується потік інформації, значну частину якої вони не в змозі адекватно сприйняти [1, с. 37].

Не секрет, що традиційні кримінальні співтовариства використовують можливості Інтернету для координації своїх дій. Часто інтернет-форуми працюють як своєрідні біржі, де можна купити наркотики, найняти кілера або легалізувати засоби, отримані нелегально. Інтернет спричинив появу нових форм злочинності, серед яких найбільш масштабні – мережева порнографія, кардинг (злочини, пов'язані із зломом, підробкою і використанням кредитних карток) і фішинг (крадіжка конфіденційної інформації і грошей за допомогою їхньої переадресації на сфальсифіковані веб-сайти). Довкола цих явищ швидко склалися професійні кримінальні співтовариства з характерним сленгом і засобами комунікації. Вони майже повністю живуть в інформаційному суспільстві, оскільки Інтернет є для них єдиним джерелом і середовищем існування. Онлайнова злочинність широко використовує технічні новини і можливості, неактуальні для більшої частини користувачів.

Сучасні інтернет-технології сприяють розростанню міжнародного тероризму і виникненню принципово нового високотехнологічного кібертероризму. При цьому можуть застосовуватися як інформаційно-комп'ютерні, так і інформаційно-психологічні засоби. Інтернет все активніше використовується для поширення ідеології тероризму, залучення до протиправної діяльності нових членів, про що свідчить наявність великої кількості відповідних сайтів.

Навіть можна сказати, що кіберпростір став місцем існування деякого „електронного співтовариства" екстремістів. На сотнях, якщо не на тисячах веб-сторінок, далеко не всі з яких навіть утримаються в пошукових системах Інтернету, публікуються, наприклад, інструкції з виготовлення вибухових пристроїв. Інтернет виявився для членів екстремістських і терористичних організацій вельми зручним засобом подолання колишньої географічної роз'єднаності і пошуку однодумців. У системі електронної пошти, що дає можливість миттєвої доставки зашифрованих послань, які можна прочитати, лише володіючи спеціальними засобами декодування, вони знайшли надійний спосіб конспірації і безпечного для них обміну ідеями і планами.

Особливість комп'ютерного тероризму – в дешевизні здійснення і затратності виявлення. Анонімність, властива Інтернету, робить злочинця невразливим, а здатність безперешкодно входити в Мережу – всюдисущим.

Слід зазначити, що на території нашої країни давно вже проводяться інформаційні атаки, викликані протистоянням і змаганням еліт. У результаті цього на сторінках сучасних українських ЗМІ з'явилися і стали звичними терміни „інформаційна війна" або „інформаційно-психологічна війна".

У засобах масової інформації цей термін трактується в основному як „злив компромату", чому неабиякою мірою сприяє і поява нового засобу масової телекомунікації – комп'ютерної мережі Інтернет, яка ідеально сприяє не лише неконтрольованому поширенню компрометуючих матеріалів, але й вкиданню в суспільство потрібної і своєчасної інформації, яку друкарські і електронні ЗМІ зможуть потім тиражувати. Не випадково, Інтернет завдяки деяким скандальним сайтам заслужив на репутацію „вбивці авторитетів", „сміттєвої ями" і так далі.

Перетворення Інтернету на загальнодоступний глобальний інструмент суспільного розвитку робить управління його використанням одним із важливих питань порядку денного міжнародного співтовариства. Цим обумовлена актуальність проблем інтернаціоналізації управління використанням мережі, підтримка високого рівня довіри до цього унікального засобу міжлюдської взаємодії, участі в цьому процесі зацікавлених урядів, представників приватного сектора, громадянського суспільства і міжнародних організацій. Інтернаціоналізація повинна сприяти справедливому доступу до ресурсів Інтернет, полегшувати доступ для всіх, забезпечувати стабільне й безпечне його функціонування.

Важливим аспектом цього питання є вироблення міжнародних правових механізмів інтернаціоналізації управління Інтернетом, міжнародної співпраці в галузі забезпечення при його використанні інформаційної безпеки кожної національної держави і міжнародного співтовариства в цілому, стійкості функціонування глобальної інформаційної інфраструктури як критично важливої сфери життя громадян, бізнесу, організацій громадянського суспільства [2].

Як відомо, різні країни вирішують проблему регулювання інтернет-ресурсу по-різному. Так, наприклад, у Росії з боку МВС і Генпрокуратури пролунали пропозиції законодавчо ввести відповідальність власників інформаційних ресурсів за розміщувану на них інформацію. Є пропозиції прирівняти розміщення інформації в Мережі до публікацій у ЗМІ.

У Германії міністр з захисту прав споживачів Ільзе Айгнер запропонувала створити „кодекс честі" в Інтернеті. На думку І. Айгнер, кодекс, який повинен включити 10 „золотих правил", має бути вироблений самим Інтернет-співтовариством. Передбачається, що прийняття такого зведення правил повинне посприяти збереженню персональних даних. При цьому правила мають бути „короткими, чіткими і зрозумілими".

Німеччина є однією з країн, уряди яких приділяють значну увагу захисту персональних даних в Інтернеті. Так, саме в Германії було виявлено, що при складанні панорам вулиць різних міст для сервісу Street View Google незаконно збирає дані, що передаються потім по незахищених мережах Wi-Fi. Згодом Google визнав, що діяв, порушуючи закон, і припинив збір цих даних [3].

У Китаї офіційно заборонено доступ з території країни до найбільших пошукових систем Інтернету – Google і Alta Vista. Відмова в доступі до певних Інтернет-ресурсів широко практикується в країнах Азії і Африки. Проте обмеження, як правило, стосуються політичних і порнографічних сайтів, а не пошукових систем. В уряді КНР прийняте рішення пояснили тим, що в Інтернеті розміщена величезна кількість непотрібної і шкідливої інформації. Цікавим фактом є та обставина, що таке рішення було прийнято напередодні з'їзду Комуністичної партії Китаю, на якому відбулася зміна партійного керівництва [4, с. 17]. У рамках широкої програми з боротьби з мережевою порнографією, азартними іграми і шахрайством вже були закриті тисячі ресурсів в китайському сегменті Мережі. Пекін і далі має намір блокувати шкідливу інформацію з інших країн.

Крім того, фільтрація трафіку широко використовується в боротьбі з опозицією і критикою уряду. Так, пошукові системи, що знаходяться в материковому Китаї, зобов'язані піддавати цензурі свої результати. Через це з китайського ринку пішов Google, що відмовився від фільтрації своєї пошукової бази.

У китайському сегменті Інтернету налічується понад 400 мільйонів користувачів. В країні створено нове відомство з Інтернет-цензури. Воно стежить за повідомленнями в соціальних мережах.

Спеціальні фільтри, встановлені на вузлах обміну китайського трафіку із загальносвітовою Мережею, відсікають від місцевих користувачів тисячі сайтів, визнані політично невірними. Китайці не можуть зайти на сайти практично всіх західних ЗМІ, університетів, правозахисних організацій тощо. Найпотужніші суперсучасні програми фільтрують електронну пошту в автоматичному режимі, а також обчислюють відвідувачів неблагонадійних сайтів. Порушників чекає покарання аж до тюремного ув'язнення. Чиновники також хочуть зобов'язати авторів Інтернет-щоденників реєструвати їх із вказівкою паспортних даних [5].

В Узбекистані всі Інтернет-провайдери повинні проходити реєстрацію в Службі національної безпеки, де зобов'язуються повідомляти про своїх клієнтів, які відвідують заборонені сайти. Такими, зокрема, є більшість зарубіжних мережевих ЗМІ. Відправка всієї електронної пошти контролюється. В Інтернет-кафе існують штрафи за перегляд порнографічних сайтів (близько 4 доларів) і заборонених політичних (понад 8 доларів).

У Білорусі оголошена обов'язкова – до 1 липня 2010 р. – державна реєстрація всіх онлайн-ресурсів, а робота будь-якого сайту в країні, не здійсненого реєстрацію, вважатиметься незаконною, згідно з постановою білоруської Ради міністрів. Всі власники ресурсів, які хочуть пройти реєстрацію і працювати з 1 липня 2010 р. в рамках закону, повинні подати в Міністерство зв'язку і інформатизації Білорусі заяву, в якій вказати: найменування юридичної особи або ПІБ індивідуального підприємця, код країни, ПІБ керівника, місце знаходження юридичної особи, адресу індивідуального підприємця, контактний телефон, адресу електронної пошти, дані з Єдиного державного регістра юридичних осіб і індивідуальних підприємців (ЄДР), договір власника ресурсу з постачальником Інтернет-послуг, дані про права юридичної особи або індивідуального підприємця на вказані ресурси.

Для Інтернет-сайту вказуються: опис ресурсу, використовувані мережеві адреси, ім'я ресурсу, реєстраційний номер центру обробки даних, що здійснює цій ресурс, тощо.

Такого роду заяви на реєстрацію подаватимуть не лише власники сайтів, але і постачальники Інтернет-послуг, а також власники центрів обробки даних [6].

Ще однією новиною білоруських властей стало те, що з 1 липня 2010 р. власники комп'ютерних клубів і інтернет-кафе повинні збирати і зберігати дані про осіб відвідувачів. Згідно з урядовою постановою, користуватися послугами Інтернет-кафе буде дозволено лише тим, хто пред'явить документи. При цьому дані про особу відвідувача персонал закладу зобов'язаний фіксувати і зберігати. Крім того, персонал повинен вести електронний журнал, в якому мають відзначати відомості про „імена або IP-адреса Інтернет-ресурсів, з якими користувач здійснив з'єднання'. Дані про відвідувачів адміністрація інтернет-кафе зобов'язана зберігати протягом року з моменту надання послуги.

Постанова уряду була прийнята відповідно до президентського указу про регулювання білоруського Інтернету, який був підписаний на початку 2010 року. В указі також зазначалося про контроль за відвідувачами Інтернет-кафе, щоправда, вимоги до власників закладу були менш конкретні.

Положення указу стали об'єктом критики з боку журналістів і правозахисників. На їхню думку, власті, зокрема, створили умови для обмеження доступу громадян до опозиційних сайтів і блокування цих ресурсів [7].

8 липня 2010 р. з'явилася інформація про те, що в Білорусі вперше відключений сайт в рамках виконання указу про державне регулювання Інтернету. Сайт газети „Вітебський кур'єр" не пройшов офіційну реєстрацію відповідно до вимог, прописаних в указі. „Вітебський кур'єр" відмовився проходити цю процедуру і не подав відповідну заявку. На думку співробітників видання, указ є спробою цензури в ЗМІ. У результаті з 6 липня 2010 р. він припинив роботу. Сайт був відключений державним Інтернет-провайдером „Белтелеком". За словами представника видання, „Белтелеком" прийняв рішення відключити Інтернет-ресурс на підставі листа, що надійшов у компанію [8].

В Іспанії власники іспанських Інтернет-ресурсів повинні розміщувати на електронних сторінках своє ім.'я, адресу і персональний ідентифікаційний номер. Ухвалений у 2002 р. закон також вимагає від провайдерів блокувати доступ до зарубіжних сайтів, якщо на них міститься інформація, що загрожує національній безпеці Іспанії.

У США спеціального закону про Інтернет немає. Будь-які спроби обмежити свободу слова в Мережі розбиваються о першу поправку до конституції, що гарантує свободу слова і друку. Навіть ухвалений у 2001 році закон, що зобов'язав встановлювати в державних школах і бібліотеках систему Інтернет-фільтрів, що блокують доступ до забороненої інформації (наприклад, порнографічного змісту), був скасований Верховним судом США. Єдиний обмежувальний закон про захист дітей в Інтернеті забороняє власникам сайтів збирати інформацію про дітей молодше 13 років без згоди батьків [9].

Правові стосунки в Інтернеті пов'язані і з проблемою: юрисдикції стосунків між користувачами; відповідальності контент-провайдерів; саморегулювання стандартів і протоколів. Загальносвітова практика правового регулювання Інтернету зводиться на сьогодні до ряду суперечливих судових рішень, що визначають державну юрисдикцію. Це пов'язано з тим, що для нього відсутні так звані колізійні норми (наприклад, lex patrie – закон громадянства, lex loci actus – закон місця здійснення операції і так далі).

В Україні національні правові норми, що регулюють Інтернет-стосунки, існують з початку 90-х років XX століття. Вони закріплені в Законі України „Про телекомунікації" (Розділ „Державне управління у сфері телекомунікацій"; Законах України „Про захист інформації в автоматизованих системах» від 5 липня 1994 р., „Про науково-технічну інформацію" від 25 червня 1993 р., „Про основні принципи розвитку інформаційного суспільства в Україні на 2007-2015 рр." від 9 січня 2007 р., Указах Президента України „Про заходи по розвитку національної складової глобальної інформаційної мережі Інтернет і забезпеченні широкого доступу до цієї мережі в Україні" від 31 липня 2000 р. і „Про заходи по захисту інформаційних ресурсів держави" від 10 квітня 2000 р. та ін.

Недавно з'явилася інформація про те, що МВС України має намір влаштувати перевірку всіх сторінок „У Контакті" на наявність порнографії. Це пояснюється тим, що в міністерстві одним з головних розповсюджувачів подібних матеріалів вважають саме цю соціальну мережу. У першу чергу міліція шукатиме фотографії і відеозаписи з дитячою порнографією, сценами вбивств і насильства. А вже потім з їх поширенням боротиметься особливий департамент.

Такі плани МВС України стали об'єктом критики експертів, які вважають, що це перший крок до встановлення повного контролю над мережею. „Якщо вони отримають цей контроль, то дістануть і загальний доступ до мережі, який зможуть використовувати вже, як їм захочеться, навіть в політичних цілях", – вважає керівник компанії Prolject у складі групи компаній Advanter Group Антон Белецкий. На сьогодні близько 80 % Інтернет-користувачів є учасниками соціальних мереж. При цьому „У Контакті" прописалися 70 % від загального їх числа. Отже, отримавши контроль над одним сайтом, МВС візьме під свій контроль практично всіх українських Інтернет-користувачів. А це може викликати звинувачення в забороні свободи слова. Міліція перечитає сторінки користувачів „У Контакті" [10].

Все це дає підстави для стверджування, що Україна повинна чітко усвідомлювати і сприяти усуненню загроз, які несе Інтернет. У той же час неможна і не враховувати і

загрози для подальшої демократизації суспільних стосунків; нормального функціонування структур державної влади тощо. Таким чином, необхідно ефективно і розумно створювати і забезпечувати всебічний захист інформаційного політичного простору держави.

ЛІТЕРАТУРА

1. Гридчин М. Проблемы влияния информационных технологий на молодежь / М. Гридчин. – Власть. – 2007. – № 9. – С. 32−38.
2. Шерстюк В.П. Тезисы выступления [Електронний ресурс] / В.П. Шерстюк. – Режим доступу: http://www.iisi.msu.ru/news/news35/
3. В Германии предложили ввести „кодекс чести” в Сети [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/07/14/700664.html.
4. Нерсесян В. Национальная безопасность и формирование информационного общества в России / В. Нерсесян // Власть. – 2003. – № 9. – С. 14−20.
5. Китай начинает войну в Интернете [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/05/03/683579.html.
6. Белорусские сайты обязали пройти регистрацию [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/05/07/684195.html.
7. Белорусские Интернет-кафе обязали собирать данные о посетителях [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/05/05/683934.html
8. В Беларуси отключен первый сайт за отказ от регистрации [Електронний ресурс]ю – Режим доступу: http://podrobnosti.ua/internet/2010/07/08/699214.html
9. С каждым днем Интернет все более и более вклинивается во все сферы нашей деятельности, как личной, так и социальной. [Електронний ресурс] – Режим доступа: http://imho.net.ua/2007/02/26/demokratija_po_internetu__2.html.
1. Милиция перечитает страницы пользователей „Контакта” [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/07/07/698868.html