помилок (ненавмисних), які можуть виявитися страшнішими за пожежу. Тому авіапідприємству з розгалуженою корпоративною інформаційною системою ми б рекомендували до використання автоматизовану систему управління і адміністрування прав користувачів, над створенням якої наразі працюють автори статті.

Надійшла 24.05.2007 р.

УДК 004.415 **Готун А.М.**

ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ В ПОЛІТИЧНІЙ КОМУНІКАЦІЇ: ПРОБЛЕМИ КОНТРОЛЮ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Щорічно у світі втрати від несанкціонованого втручання у роботу мереж, крадіжок і витоку інформації подвоюються. У 2004 році вони становили 10,2 млрд. доларів, у 2005-му – біля 20 млрд [1]. Але багато компаній відмовляються розголошувати збитки, пов'язані з втратою або витоком інформації, боячись зіпсувати свій імідж. Насамперед, це стосується соціально-економічної сфери. Не піддаються підрахункам, на жаль, втрати пов'язані з підготовкою і проведенням політичних кампаній. Адже до останнього часу хакерські атаки за замовленням з метою викрадення стратегічно важливої інформації із комп'ютерних мереж конкурентів ставили собі за мету переважно політики. Вони періодично замовляють зламування сайтів один одного, а найбільш гучний випадок – атака на сервер Центрвиборчкому у 2004 році (хоча слідство до цього часу не доказало, що мова йде про хакерів, а не про банальний підкуп адміністратора).

Безперечно, що все більш вагомим фактором розвитку сучасної політики стають нові інформаційно-комунікаційні технології. Глобальний віртуальний простір, а саме мережа Інтернет, є своєрідним викликом традиційним інститутам і механізмам політичного процесу. Глобальність й інтерактивність – найважливіші якісні ознаки нової віртуальної реальності, що не визнає умовностей державного суверенітету, форм політичної участі, ієрархічних структур політичних партій та інших інституціональних суб'єктів політики. Політичні наслідки нових технологій неоднозначні.

З розширенням масового доступу до мережі Інтернет вона почала відігравати все більш помітну роль не тільки у повсякденному житті людей, а й у сучасному політичному процесі. Інтернет сприяє більшій відкритості і транспарентності політичних інститутів і політики в цілому. В мережі з'являється все більша кількість сайтів різних державних органів, партійних структур, чисельних міжнародних неурядових організацій, які містять різноманітну інформацію, що суттєво збільшує політичну поінформованість широких мас. Різноманітні урядові публікації, які раніше були доступними лише небагатьом і тільки номінально подавали суспільну інформацію, з'являючись сьогодні в онлайновому режимі, стають у повному розумінні слова суспільно доступними. Завдяки Інтернету виникають нові, досить ефективні механізми політичної мобілізації громадян. Він виступає, зокрема, як засіб досить оперативної організації і координації дій політичних однодумців, які є прихильниками нетрадиційних соціальних рухів.

Інтернет являє собою надзвичайно потужний глобальний інструмент комунікації, освіти, розваг і інформованості. Але це – всього лише інструмент, значення якого не варто ані недооцінювати, ні ідеалізувати. Сила і характер його впливу залежать від того, ким і заради чого він використовується. Подібно будь-якому іншому інструменту або технологічному засобу, він може бути застосований як для блага так і для шкоди. Він може бути засобом освіти для людини у тій же мірі, що і засобом його розтління.

Величезні інформаційні ресурси Інтернету можуть бути використані і для творення, і для розрухи. З його допомогою можуть розповсюджуватись благородні, високі ідеї і транслюватися суспільно небезпечні ідеологічні погляди.

Вище вже зазначалося, що Всесвітня Мережа перетворюється сьогодні у важливий інструмент політичної мобілізації, яка може спрямовувати політичну активність мас у конструктивне русло, орієнтувати на зміцнення і розвиток демократії. Але вона й може бути підпорядкована екстремістським цілям, збуджуючи національну, релігійну, соціальну ворожнечу. Екстремісти різних видів (нацисти, скінхеди, расисти, релігійні фанатики тощо) вбачають у становленні мережі Інтернет надзвичайно ефективний засіб активізації своєї діяльності, розповсюдження своїх поглядів і залучення до орбіти свого впливу нових прибічників.

З одного боку, якісно нові інтерактивні можливості знімають географічні й структурні обмеження прямої політичної участі, колективної дії, усувають дистанцію між громадянами й особами, що приймають рішення. З іншого –глобальна віртуальна реальність робить виклик інтересам суспільної й державної безпеки. Багатогранна проблема регулювання Інтернет має технічні, політичні, моральні, економічні й правові (у т.ч. міжнародно-правові) аспекти. Нерегульованість Інтернету – багато в чому ілюзія; політичні заходи контролю можуть значною мірою доповнити й компенсувати обмеженість технічних можливостей. Більше того, розвиток нових інформаційних і комунікаційних технологій робить індивіда й суспільство більше уразливим перед політичним контролем, сприяє нарощенню й удосконаленню інструментарію політичного панування і маніпулювання свідомістю. Інтернет вже досить довгий час є засобом поширення завідомо неправдивої інформації, що використовується під час політичних кампаній і в повсякденній політичній активності суб'єктів політичної комунікації [2].

Основна перевага мережі Інтернет як засобу брудної політичної боротьби полягає в його анонімності й віртуальності. Існуючі технології Інтернет дозволяють з одного боку безперешкодно поширювати небажану або недостовірну інформацію, а з іншого не дозволяють однозначно встановити авторство цієї інформації. Така відносна безкарність при здійсненні цілком реальних злочинів проти особистості сприяє формуванню широкого спектру варіантів застосування мережі Інтернет з метою дискримінації тієї чи іншої політичної сили або політичного діяча. Саме тому проблема дослідження інформаційної безпеки в мережі Інтернет є досить актуальною.

Інформаційна безпека розглядається дослідниками, в тому числі і вітчизняними, з різних точок зору [3]. Як зазначає професор Зернецька О.В.: „Інформаційна безпека може розглядатися в різних аспектах: і як фактор соціально-економічного розвитку, і як відстеження і класифікація комп'ютерних і мережевих загроз, і як збереження і захист технічної і мовної інформації, і як новий вид озброєння, і як запобігання інформаційній війні тощо" [3]. Всебічно і ґрунтовно нею проаналізовано проблеми інформаційної безпеки в масово-комунікаційній сфері [4].

У даній статті зосереджено увагу головним чином на методах і прийомах поширення завідомо неправдивої інформації в мережі Інтернет, які використовуються під час проведення політичних кампаній, зроблено спробу проаналізувати їх еволюцію і наведено приклади успішного протистояння подібним заходам.

Одним із перших способів використання Інтернету в політиці з метою поширення недостовірної інформації було розміщення в мережі компромату. Для цього орендується дисковий простір на якому-небудь веб-сервері через який потім на сайті розміщується необхідна компрометуюча інформація. Після цього залишається тільки розрекламувати адресу сайту в політичних форумах або поштою. Цей засіб є досить популярним, адже він дуже ефективний. Ефективність досягається за рахунок стрімкого поширення цікавої інформації в Інтернеті. Навіть якщо губиться сам доступ до джерела інформації, залишається безліч доступних незалежних копій по всій мережі. Потім інформація попадає в традиційні

ЗМК через журналістів, що користуються Інтернетом. Природа поширення такого компромату подібна до поширенням звичайних слухів.

Слідом за разовим анонімним компроматом з'явилася ціла когорта сайтів, які регулярно збирають і публікують слухи й компромат, знайдені в Інтернеті. Ще одним засобом поширення недостовірної інформації, введення в оману користувачів Інтернету, є створення сайту з доменним ім'ям, схожим на назву особи, яку хочу скомпрометувати, або схожим на доменне ім'я, реально існуючого сайту цієї особи. Основною метою такого засобу є залучення користувача Інтернету на свій сайт для повідомлення свідомо помилкової або неперевіреної інформації. Причому можливий відвідувач може навіть не здогадуватися про те, що він потрапив не на «той сайт». Для цього навіть можуть застосовуватися аналогічний дизайн і аналогічна структура сайту. Оскільки доменні імена не закріплені за якоюсь конкретною особою, протидіяти такій активності дуже складно. При бажанні будь-хто може зареєструвати на себе доменне ім'я одного з відомих політиків або політичних партій і подавати інформацію від його імені. Таких осіб називають кіберсквоттерами. Вони реєструють на своє ім'я різноманітні доменні імена, а потім намагаються їх продати справжнім власникам. А якщо власники відмовляються викупити таке доменне ім'я, його може купити хто завгодно – у тому числі й конкуренти.

Одним з найбільш поширених способів розповсюдження інформації, як негативної так і будь-якої іншої, в тому числі і політичної, є спам (від. англ. spam) - це небажана електронна пошта, що приходить на особисту адресу одержувача без його згоди, причому адресована не йому, а величезній групі осіб, особисто невідомих відправникові. За даними інформаційного агентства Washington ProFile, збиток від дій осіб, що розсилають спам у світовому масштабі перевищує сотні мільярдів доларів. Найбільш активне несанкціоноване розсилання по електронній пошті відбувається у США, Росії, Україні й Китаї [5].

Спам дозволив створити цілу галузь економіки. Тільки в США діє кілька десятків компаній, що створюють програмне забезпечення для боротьби зі спамом. Одночасно діє безліч фірм, які обслуговують інтереси спамерів. За повідомленнями Washington ProFile, якщо вивчити статистику листів, що розсилаються, то близько 14% несанкціонованих листів по електронній пошті складають послання шахраїв, 14,5% - порнографія, 21% - реклама товарів, 16% - пропозиції фінансових послуг [5].

Приклади політичного спама в Інтернеті зустрічаються не так часто, як, наприклад, комерційний спам, однак електронна пошта все-таки використовується в політичних цілях. Так, наприклад, у січні 2003 року США здійснили в мережі Інтернет кампанію, у рамках якої всім тим, хто знає що-небудь про виробництво в Іраку зброї масової поразки, пропонувалось повідомити про це за допомогою електронної пошти. Відповідний електронний лист було розіслано за всіма доступними іракськими електронними адресами [6].

Окрім використання політичного спама під час виборчих кампаній все більшого поширення набирає кіберзлочинність. Одним із останніх прикладів цього явища можна назвати події, пов'язані з парламентськими виборами в Естонії, під час проведення яких хакери здійснили масовані атаки на Інтернет-сайти політичних партій і Центральної виборчої комісії і заблокували їх роботу [7].

Одним з останніх оприлюднених прикладів появи і використання політичного спама в США під час виборів 2006 року є поява розсилки, що нібито інформує користувачів про атаку на онлайнові банківські сервіси, а насправді перенаправляє користувачів на сайт, що критикує політичну ситуацію в США. Наприклад, представники відомої в індустрії інформаційної безпеки іспанської компанії PandaLabs виявили появу безлічі електронних листів, що інформують користувачів про атаку на онлайнові банківські сервіси, що нібито трапилася 9 листопада 2006 року. В листах рекомендується відвідати веб-сторінку для забезпечення власної безпеки. Однак зміст цієї сторінки – критика політичної ситуації в США. Заголовок повідомлення орієнтований на користувачів Інтернет-банків, у той час як саме повідомлення носило політичний характер з посиланням на веб-сторінку [8].

Атака збігається із проміжними виборами в США і є спробою вплинути на результати.

Втім, за словами директора PandaLabs Луїса Корронса, "у дійсності ця атака не тільки слабка з технічної точки зору, вона навіть проведена не вчасно. Перші виявлені повідомлення практично збіглися із закриттям виборчих дільниць. Але тривожним є те, що це – політично мотивована спроба маніпуляції свідомістю користувачів. Ми не знаємо, які можуть бути наслідки такої атаки, якщо вона буде виконана в потрібний час із застосуванням більш витонченої тактики. До неї явно не можна ставитися зі зневагою."

"Спам швидко еволюціонує відповідно до запитів кібер-злочинців. Ще кілька років тому небажана пошта використовувалася, в основному, для того, щоб переповнити ящики користувачів рекламою, нині ж вона все більше використовується для отримання „прямої" вигоди – або для одержання легких грошей, або, як у цьому випадку, для політичної маніпуляції користувачами. У будь-якому випадку, найбільш зваженою порадою буде ігнорувати подібні повідомлення," – пояснює Луїс Корронс [8].

Досвід розвинених країн свідчить, що єдиним ефективним способом боротьби зі спамом є його заборона на законодавчому рівні, тому що інші методи боротьби виявляються малоефективними. Так, у США в 2003 році було прийнято закон "CAN-SPAM Act of 2003, який забороняє використання багатьох стандартних спамерських технологій: фальсифікації зворотної адреси, маскування поля "Тема", автоматичного перебору комбінацій букв з метою виявлення діючих адрес, різних засобів подолання антиспамерських фільтрів.

Згідно з цим законом передбачається, що порушників закону будуть карати тюремним ув'язненням на строк до одного року й штрафами на суму до мільйона доларів. В Євросоюзі також діє заборона надсилати електронні листи без дозволу. У Великобританії з грудня 2003 року спамерам привласнюється статус кіберзлочинців. В грудні 2003 року австралійський уряд прийняв закон, згідно якого фірми, які займаються розсилкою спама, можуть бути оштрафовані на суму до 1,1 мільйона австралійських доларів [6].

Представники більшості розвинених країн вже давно дійшли висновку, що дана проблема не може бути вирішена самостійно. Про це свідчать результати зустрічі на найвищому рівні з питань інформаційного суспільства, яка відбувалась поетапно: в Женеві з 10 по 12 грудня 2003 року та в Тунісі з 16 по 18 листопада 2005 року і отримала назву Всесвітній Самміт з питань Інформаційного Суспільства. В результаті проведених зустрічей було підготовлено документ, що отримав назву „Туніське зобов'язання", в якому всі представники самміту наголосили, що проблему забезпечення безпеки в мережі Інтернет можна вирішити лише завдяки згуртуванню спільних зусиль [9]. Одним з основних факторів вирішення даної проблеми є прийняття, втілення в життя і забезпечення виконання міжнародно–правових механізмів регулювання політичної діяльності в мережі Інтернет. Насамперед це стосується проблеми розповсюдження заздалегідь недостовірної інформації.

Таким чином, можна виділити наступні напрямки міжнародного співробітництва із проблем безпеки політичної комунікації в інформаційній сфері:

1.Необхідно розпочати підготовку міжнародних угод про контроль над виробництвом і впровадженням у комп'ютерні мережі й системи інформаційних технологій, які реально або потенційно можуть використовуватися з метою розповсюдження недостовірної політичної інформації.

2.Треба сприяти активізації переговорів стосовно міжнародно-правового захисту мережевих інформаційних ресурсів, у тому числі даних персонального характеру окремих суб'єктів політичної діяльності, що розповсюджуються в Інтернеті й інших відкритих мережах.

3.Необхідно на міжнародному рівні розглянути можливості контролю й обмеження поширення по мережі недостовірної інформації політичного характеру, а також інших матеріалів, що здійснюють негативний вплив на процес забезпечення політичної комунікації в мережі Інтернет.

Проблема боротьби з комп'ютерною злочинністю для України є новою і тому в системі державного управління нашої країни ще не створено інститут, який би збирав, узагальнював і аналізував інформацію про здійснені комп'ютерні злочини. Окрім того, подібний центр зміг

би робити оцінки і прогнози, відпрацьовувати методику, перш за все, по попередженню кібезлочинності. Однак на даний час органи, які займаються питаннями попередження комп'ютерних злочинів, володіють розрізненими і несистематизованими даними про комп'ютерну злочинність, а законодавча і виконавча влади не мають реального уявлення про масштаби розповсюдження цього виду злочинності в країні, внаслідок чого держава втрачає можливість адекватного реагування на її динаміку. Ці функції зміг би вирішувати, наприклад, вже існуючий при Раді національної безпеки і оборони України Міжвідомчий науково-дослідний центр.

Список літератури

1. *Плещивцева Т.* Червяк в паутине // "Эксперт" Украинский деловой журнал, № 12 (110), 26.03.2007. – с 21.

2. *James N. Rosenau and J.P. Singh.* Information Technologies and Global Politics: the changing scope of power and governance. Published by State University of New York Press, 2002, p.265.

3. *Аспекти інформаційної безпеки аналізуються, зокрема, в працях:* Білорус. О.Г., Скаленко О.К. Інформаційна безпека як фактор соціально-економічного розвитку: Глобальні трансформації і стратегії розвитку. – К., 1998. – С. 361-373; Зубок Микола Іванович. Інформаційна безпека. — К. : КНТЕУ, 2005. — 133 с; Карпенко В. О. Інформаційна політика та безпека: Підручник. — К. : Нора-Друк, 2006. — 320 с. та ін.

4. *Зернецька О.В.* Проблеми інформаційної безпеки в масово-комунікаційній сфері // Колективна монографія „Глобалізація і безпека розвитку", за ред. Білоруса О.В – К.: КНЕУ, 2001. – С. 675-684.

5. *http://www.washprofile.org* - Інформаційне агентство Washington ProFile.

6. *Луков В.В.* Интернет как инструмент политических технологий в США // США v Канада: экономика, политика, культура. 2005. - № 5 (425). – С 91-107.

7. *http://www.cybersecurity.ru/net/23759.html* - сайт новин високих технологій "Cyber Security".

8. *http://www.pandasoftware.es/virus_info/pandalabs* - сайт компанії Panda Software.

9. http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0 - Tunis Commitment, Second Phase of the WSIS (16-18 November 2005, Tunis) // „Туніське зобов'язання" Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства (16-18 листопада 2005 року, Туніс).

Надійшла 17.05.2007 р.

УДК 621.391: 519.2

Алексейчук А. Н.

АНАЛИТИЧЕСКИЕ ОЦЕНКИ ТЕОРЕТИЧЕСКОЙ СТОЙКОСТИ РАНДОМИЗИРОВАННЫХ БЛОЧНЫХ СИСТЕМ ШИФРОВАНИЯ ОТНОСИТЕЛЬНО МЕТОДА РАЗНОСТНОГО КРИПТОАНАЛИЗА

Одним из общих подходов к повышению стойкости криптографических систем является применение рандомизации или случайного кодирования источника сообщений, при котором каждому фиксированному открытому сообщению отвечают различные кодовые слова, выбираемые в соответствии с некоторыми распределениями вероятностей из заданных попарно непересекающихся множеств шифруемых слов [1, 2]. В настоящее время известно немало работ, посвященных исследованию теоретической стойкости так называемых