неправомірної вигоди службовою особою (ст. 368); незаконне збагачення (ст. 368^2); пропозиція, обіцянка або надання неправомірної вигоди службовій особі (ст. 369); зловживання впливом (ст. 369^2).

Найдюк Ю.М., *магістр Навчально-наукового інституту заочного та дистанційного навчання Національної академії внутрішніх справ*

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Найпоширенішим напрямком використання глобальної мережі в інтересах військово-політичного протиборства є заміна інформаційного змісту сайтів, що полягає в підміні сторінок або їхніх окремих елементів шляхом злому. Такі диверсійні дії, переважно, здійснюються з метою привернення уваги до атакуючої сторони, демонстрації її можливостей, зрештою, методом задекларувати певну політичну позицію. Крім прямої підміни сторінок, широко використовується реєстрація в пошукових системах сайтів протилежного змісту по однакових ключових словах, а також переспрямування (підміна) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених конфронтуючою стороною сторінок. Слід також виокремити так звані семантичні атаки, які полягають у зломі сторінок і наступному акуратному (без помітних слідів злому) розміщенні на них свідомо помилкової інформації. Подібним атакам, як правило, піддаються найбільш часто відвідувані інформаційні сторінки, змісту яких користувачі цілковито довіряють [1, с. 3].

Об’єктом інтернет-атак дедалі частіше стають інформаційні ресурси, вивід з ладу або ускладнення функціонування яких може завдати конфронтуючій

стороні значних економічних збитків або викликати великий суспільний резонанс.

Ще одним напрямком використання Інтернету в інтересах інформаційного протиборства є вивід з ладу або зниження ефективності функціонування структурних елементів мережі. Найпоширенішими методами диверсії в цьому аспекті постають: «бомбардування» мережі електронними листами; атаки, проведення яких по суті аналогічне технології масового розсилання електронних листів одному адресатові й полягає в генерації величезного числа звернень до обраного сайту, що уповільнює роботу обслуговуючого сервера або цілковито припиняє зовнішній доступ до нього; впровадження комп'ютерних вірусів.

Таким чином, розвиток глобальної мережі Інтернет супроводжується дедалі більшим використанням наданих нею можливостей для здійснення інформаційного протиборства; зростанням координації, масштабів і складності дій учасників цього протиборства, коло котрих включає як держави та їх коаліції, так й окремі організовані групи, в тому числі, терористичні [2, с. 87].

Нині Інтернет дедалі активніше й масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів. Він створює широкі можливості для формування суспільної думки; впливу на прийняття політичних, економічних і військових рішень; дії на інформаційні ресурси супротивника й поширення спеціально підготовленої інформації (дезінформації) [3].

Активне використання мережі Інтернет для ведення інформаційного протиборства обумовлено низкою її істотних переваг перед звичайними засобами й технологіями.

Розміщення й регулярне відновлення інформації на окремих сторінках, в інтернет-виданнях і різних розсиланнях новин, форумах та конференціях - не вимагають значного часу на підготовку матеріалів.

Економність є наслідком залучення невеликої кількості персоналу й матеріальних засобів для вирішення поставлених завдань. Зокрема, наявності мінімально підготовленого користувача персональної ЕОМ, підключеної до телефонної лінії, нерідко буває цілком достатньо.

Задля запобігання та нейтралізації наслідків застосування інформаційної зброї необхідно вжити таких заходів:

- захист матеріально-технічних об'єктів, що становлять основу інформаційних ресурсів;
- забезпечення нормального й безперебійного функціонування баз і банків даних;
- захист інформації від несанкціонованого доступу, її перекручування або знищення;
- збереження якості інформації (своєчасності, точності, повноти й необхідної доступності).

Нинішній стан української економіки, нерозвиненість інформаційної інфраструктури, непідготовленість більшості українських користувачів до ефективної роботи в мережах відкритого інформаційного обміну перешкоджають повноцінній участі країни в таких мережах, значно обмежуючи потенціал використання нових технологій у сфері інформації. Отже, необхідна активна участь України в проектах розвитку світових інформаційних мереж, у роботі міжнародних організацій, громадських комітетів і комісій цього напряму.

Крім того, входження України до міжнародної мережі має відбуватися поступово, відповідно до потреб, її економічних і технологічних можливостей. Заборонити розробку й використання інформаційної зброї, як це зроблено, наприклад, з хімічною або бактеріологічною зброєю, навряд чи вдасться. Обмежити зусилля багатьох країн з формування єдиного глобального інформаційного простору також неможливо. Проте, Україна може виступити ініціатором розробки угод, які опиратимуться

на міжнародне право й мінімізуватимуть небезпеку застосування інформаційної зброї [4].

Серед заходів програмного характеру, спрямованих на захист українського суспільства й держави від інформаційної зброї, пропонуються:

- організація моніторингу й прогнозування потреб економічних та інших організацій у різних видах інформаційного обміну через міжнародні мережі;
- заснування спеціалізованого державного органу по контролю за транскордонним інформаційним обміном;
- координація заходів державних і недержавних відомств з метою запобігання загрозам національній безпеці у відкритих мережах;
- організація міжнародного співробітництва в царині інформаційної безпеки;
- розробка державної програми вдосконалення інформаційних технологій, яка б забезпечила підключення національних і корпоративних мереж до світових відкритих мереж, за умови дотримання вимог безпеки інформаційних ресурсів;
- організація системи комплексної підготовки й підвищення кваліфікації масових користувачів і фахівців з інформаційної безпеки для роботи у світових інформаційних мережах;
- розробка національного законодавства в частині правил роботи з інформаційними ресурсами, регламенту прав, обов'язків і відповідальності користувачів відкритих світових мереж;
- визначення переліку інформації, що не підлягає передачі у відкритих мережах і забезпечення надійного контролю за дотриманням встановленого статусу інформації;
- активна участь в розробці міжнародного законодавства й нормативно-правового забезпечення функціонування світових відкритих мереж.

Список використаних джерел:

1. Петров В. В. Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн: автореф. дис. ... канд. політ. наук: спец. 21.01.01. Київ, 2010. 19 с.

2. Жарков Я. М., Петрик В. М., Присяжнюк М. М. Історія інформаційно-психологічного протиборства: підручник; заг. ред. Є. Д. Скулиша. Київ: Нац. акад. СБ України, 2012. 212 с.

3. Крутских А. О., Федоров А. К. О международной информационной безопасности. М.: Слово, 2008. 234 с.

4. Романчук О. Як перемогти в інформаційній війні? *Радіо Свобода.* 2017. Ц^: http://www.radiosvoboda.org/a/25364538.html

Танцюра О.С., *доцент кафедри цивільного права та процесу Юридичного інституту Національного авіаційного інституту, кандидат юридичних наук*

ДО ПИТАННЯ ІНТЕРНАЦІОНАЛІЗАЦІЇ ВІТЧИЗНЯНОЇ ОСВІТИ

Європейська спрямованість вітчизняної державної політики обумовила значний поштовх щодо внутрішніх структурних реформ, удосконалення університетського менеджменту, підвищення авторитету вищої освіти тощо.

Національна стратегія розвитку освіти в Україні на період до 2021 року (далі - Національна стратегія) стала одним із основоположних документів останніх років, прийняття якого не тільки дозволило закцентувати увагу на існуючих проблемах національної системи освіти. Він також визначив основні напрями розвитку, спрямовані на