Зміцнення захищеності інформаційного простору України на основі досвіду Сполучених Штатів Америки

УДК 004.056

Валерія Гоц

Національний авіаційний університет, leragots@ukr.net

Захист та удосконалення інформаційних інфраструктури і простору України є невід'ємною частиною національної політики в сфері інформаційної безпеки (ІБ), що передбачає забезпечення суверенітету та національної цілісності нашої держави. Інформація та інформаційні засоби загалом на сьогодні стали потужними джерелами розвитку держав та міжнародних об'єднань, а також, на жаль, способом маніпулювання та наведення безладу в суспільстві.

Актуальність теми роботи пов'язана з небезпечним становищем у сучасному світі, де українсько-російська інформаційна війна та інші політичні конфлікти продемонстрували, що пропаганда - це масова зброя ураження, яка позбавляє можливості критично та об'єктивно мислити надзвичайно великі маси людей. Наразі є велика потреба у розробці нових принципів політики інформаційної безпеки з метою забезпечення інформаційної безпеки особі, суспільству та державі.

Мета роботи - проаналізувати стан розвитку та особливості функціонування системи кібер- та інформаційної безпеки України, порівнюючи її з досвідом США, ознайомитись із роллю різних американських структурних органів, що мають повноваження у цій сфері. Завдання - визначити недоліки у структурі забезпечення інформаційної безпеки України та запропонувати способи її покращення.

США на сучасному етапі виступають світовим лідером за рівнем розвитку, масштабами впровадження, розповсюдження і ефективністю використання сучасних інформаційних технологій як в державному управлінні, так і в усіх інших сферах суспільної діяльності. Структура забезпечення інформаційної безпеки США є дуже розгалуженою, і на кожен орган цієї системи покладені відповідні завдання. Всі структурні частини підпорядковуються Президентові США, який приймає основні рішення з питань національної безпеки.

Міністерство оборони є головним ідеологом забезпечення інформаційної безпеки не лише в частині функціонування технічних засобів розвідки, а й розвитку інформаційних і телекомунікаційних технологій у США. Завдання захисту національної інформаційної інфраструктури входить також до компетенції розвідувального співтовариства США, яке об'єднує низку самостійних спецслужб та підрозділів федеральних міністерств та відомств держави: Центральне розвідувальне управління (ЦРУ), Агентство національної безпеки (АНБ), Федеральне бюро розслідувань (ФБР), Міністерство внутрішньої безпеки (МВБ), Розвідувальне управління Міністерства оборони (РУМО) [1].

Загалом національна політика США в сфері захисту інформації формується АНБ, що є найбільш потужною у світі організацією, яка здобуває інформацію технічними засобами. Для вирішення найбільш складних завдань АНБ США

додатково залучає кращі науково-дослідницькі установи країни. За контрактами з АНБ співпрацює кілька десятків найвідоміших американських фірм, що займають передові позиції в галузі електроніки, фізики, комп'ютерної техніки. Важливою складовою підготовки фахівців ІБ у США є розвинена система курсової підготовки, в першу чергу комерційних курсів та навчальних центрів фірм-виробників ІТ-продукції. Комерційні компанії проводять масове навчання в галузі інформаційної безпеки: "Cisco Systeme", "Check Point Software Technologies", "Internet Security Systems", "Microsoft, Sun Microsystems", "DellComputer", "AlliedTelesyn", "Oracle Corp", "APC", "Symantec" та ін.

Висококваліфіковані фахівці ІБ, які пройшли навчання в навчальних центрах виробників і отримали відповідні сертифікати зазначених компаній, затребувані на ринках праці більше від тих, хто тільки закінчив навчальний заклад.

У період з 1967 року до сьогодні в США прийнято цілу низку законів: “Про свободу інформації” (1967 р.), “Про таємницю” (1974 р.), “Про право на фінансову таємницю” (1978 р.), “Про доступ до інформації, про діяльність ЦРУ” (1984 р.), “Про комп’ютерні зловживання та шахрайство” (1986 р.), “Про безпеку комп’ютерних систем “(1987 р.) та інші.

Можна зробити логічний висновок, що система забезпечення інформаційної безпеки США повністю сформована та продовжує невпинно розвиватись.

Відставання України від високорозвинених держав ще раз підкреслює надзвичайну актуальність дослідження проблем забезпечення ІБ. Досвід державної політики США у цій сфері є актуальним для багатьох питань української зовнішньої та внутрішньої політики.

До основних недоліків у структурі забезпечення інформаційної безпеки України можна віднести: 1) недостатній рівень фінансування та низьке стимулювання розвитку комп’ютерних технологій державою; 2) недостатній рівень взаємодії між міністерствами і відомствами з питань підготовки фахівців ІБ, обміну програмами підготовки; 3) інформаційна залежність України від запозичених інформаційних технологій, впроваджених у різні сфери державного і корпоративного управління країни; 4) недостатній рівень модернізації навчально-лабораторної бази навчальних закладів за відповідними напрямами і спеціальностями; 5) недостатня нормативно-правова база у сфері забезпечення інформаційної безпеки; 6) недостатня кількість державних органів та організацій, що відповідають за забезпечення ІБ України [2].

Зважаючи на досвід США у забезпеченні стабільності своєї інфраструктури та національної безпеки держави, а також на недоліки та слабкі ланки в системі забезпечення ІБ України, можна виділити шляхи зміцнення інформаційного простору України. Отже, в першу чергу необхідно чітко структурувати органи інформаційної безпеки та на законодавчому рівні затвердити їх основні завдання. Надзвичайно важливо звернути більше уваги та ресурсів на протидію іноземним розвідкам та створити окремий центр захисту інформації, що містить державну таємницю. Основна мета - детально

прорегламентувати процедуру взаємного обміну таємною інформації між Україною та іноземними державами, міжнародними організаціями і узаконити її; посилити контроль із боку міністерств та відомств за підпорядкованими установами щодо питання охорони державної таємниці. Також необхідно провести атестацію педагогічного складу навчальних закладів, інших закладів освіти;передбачити державне фінансування тих фахівців, які пропонують нові інформаційні, аналітичні, навчальні та просвітницькі програми; на законодавчому рівні передбачити функціонування незалежних аналітичних, дослідницьких, інформаційних організацій, наділивши їх відповідними правами в сфері забезпечення ІБ. Для подальшого розвитку інфраструктури необхідним є сприяння з боку держави розробленню національних програмних продуктів, створенню перспективних інформаційних технологій із метою зменшення залежності від програмного та апаратного забезпечення іноземного виробництва, що містить загрозу застосування недокументованих можливостей; працювати над збільшенням можливостей співпраці та обміну досвідом з іншими високорозвиненими державами світу [3].

Виконавши ці рекомендації та звернувши більше уваги на удосконалення інфраструктури України, уряд зможе стабілізувати становище в країні, покращить стан захищеності від внутрішніх і зовнішніх загроз та підвищити рівень життя населення. Адже національна безпека (і її складова - інформаційна безпека) є багатоплановим явищем, яке передбачає економічні, соціальні, політичні, воєнні, екологічні та інші характеристики.

Список використаних джерел

1. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу / А.М.Гуз. –К., КНТ,– 2007р . – 255 с.
2. Є. Скулиш. Організація захисту інформації з обмеженим доступом – перспективний напрям підготовки фахівців в Україні / Є. Скулиш, А. Марущак, А. Гуз. – Вища шк. -2012. – № 9. – 29 с.
3. Петрик В. М. Соціально-правові основи інформаційної безпеки : навч. посіб. / В. М.Петрик, А. М. Кузьменко, В. В. Остроухов, О. А. Штоквич, В. І. Полевий; Укр. акад.наук. – К. : Росава, 2007. – 496 с.

Науковий керівник – к.т.н., Гізун А.І.