

ПРОБЛЕМНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Наукові праці МАУП, 2010, вип. 2(25), с. 194–198

Охарактеризовано деякі окремі проблемні аспекти інформаційної безпеки держави. Показано, що міжнародне співробітництво в галузі забезпечення інформаційної безпеки має будуватися на основі поєднання національних інтересів зацікавлених країн в інформаційній сфері.

В умовах глобалізації, стрімкого розвитку новітніх технологій та інформатизації зростають інформаційні потреби людини. Нині інформація є не лише джерелом знання, вона дає можливість стежити за подіями, які відбуваються в усьому світі, а також є засобом здобуття авторитету та влади. Завдяки достовірній та своєчасній поінформованості можна приймати зважені та правильні рішення.

Своєчасне донесення інформації завжди було важливим та складним завданням. Нині дуже актуальним є налагодження системи засекречення, отримання та донесення достовірної інформації. Для досягнення цієї мети необхідна наявність трьох основних елементів — новітні технології, кваліфіковані кадри, відповідне нормативно-правове закріплення.

Дослідженню проблем забезпечення інформаційної безпеки стосовно сучасних міжнародних концепцій безпеки, міжнародної безпеки через співробітництво, інформаційної безпеки в масово-комунікаційній сфері приділялася увага в роботах таких фахівців, як Е. І. Низенко, О. П. Дзьобань, А. М. Прохоров, В. Лисичкин, І. Г. Утюж [5; 6; 8; 9; 13].

Суспільству, незалежно від його політичних, економічних соціальних, культурних та інших характеристик, притаманний масовий характер, тому що в ньому принципово не буває суто індивідуальних подій. Кожний прояв суспільного життя — це масова подія. В неї втягується все більша кількість людей і все більшу роль у житті будь-якого суспільства, що прагне захистити і реалізувати власні національні інтереси, відіграватимуть

саме масові інформаційні процеси, розраховані на масове одночасне сприйняття великими і водночас розосередженими аудиторіями. Тому захист від інформаційно-психологічних агресій є одним із пріоритетних завдань при реалізації усього комплексу національних інтересів України, що, в свою чергу, дає всі підстави говорити про такий різновид національної інформаційної безпеки, як безпека інформаційно-психологічної сфери. Забезпечення її належного рівня неможливе без відповідного адекватного реальності менеджменту викликів, що існують у цій сфері, а також загроз:

- фактична приватизація національного інформаційного простору окремими фінансово-політичними угрупованнями;
- заміна колишньої тоталітарної цензури на сучасну “цензуру грошових мішків”;
- комерціалізація національного інформаційного простору, фінансова заангажованість багатьох ЗМІ;
- тотальна підміна об’єктивної інформації піаром, реальної дійсності — іміджами, соціальних та економічних зрушень до кращого — окремими національними спортивними успіхами;
- слабкість і вторинність національної системи контрпропаганди і нейтралізації недружніх інформаційних дій та інтервенцій. Відсутність системної, науково обгрунтованої, випереджаючої, оперативної та своєчасної системи протидії антиукраїнським інформаційно-психологічним маніпуляціям;
- тенденція до перетворення звичайної інформаційно-політичної боротьби на цивільну

інформаційно-психологічну війну із власним для неї залякуванням електорату і суспільства за допомогою підконтрольних ЗМІ, що призводить до появи масових катастрофічних, апокаліпсичних настроїв, паралізуючого песимізму, масового відчуття неминучості “надзвичайного стану”;

- зростання рівня й інтенсивності явної та прихованої експансії іноземних держав і транснаціональних корпорацій у масову сферу національного інформаційного простору;
- перманентне приховане і явне витіснення національних ЗМІ з внутрішнього інформаційного ринку;
- прицільно спрямована дискредитація і спроби девальвації національних і загальнолюдських духовних цінностей, агресивна пропаганда антихудожніх зразків масової культури, заснованих на аморалізмі й культурі насильства. Демонстрація насильства як єдина можливість найефективнішого засобу розв’язання особистих, суспільних, економічних і соціальних проблем. Показ зла, людських вад і пороків у привабливому вигляді. Надмірність і пряме зловживання багатьма ЗМІ сексуальною тематикою як інформаційною “приманкою”;
- невинуватена експлуатація страху як основного компонента інформаційних повідомлень ЗМІ;
- блокування (комунікативне, адміністративне, фінансове, технічне) діяльності вітчизняних засобів масової інформації з об’єктивного інформування вітчизняної і зарубіжної аудиторії;
- маніпулятивне надання (нав’язування) вітчизняним і зарубіжним ЗМІ брехливої або помилкової інформації про Україну;
- відсутність науково обґрунтованих критеріїв і методів оцінки стану й ефективності забезпечення інформаційно-психологічної безпеки України;
- діяльність, спрямована на протизаконну, насильницьку зміну основ конституційного ладу і порушення цілісності України, розпалювання мовної, соціальної, расової, національної, релігійної неприязні й ворожнечі, їх пропаганда в засобах масової інформації.

Потрібно зазначити, що загрози психологічній безпеці суспільства й держави містяться не лише в суто інформаційній сфері. Кожне покоління переконане, що саме йому випало жити в найбільш

важкий період всієї історії людства, і, все ж таки, саме наші співвітчизники повною мірою можуть претендувати на цю сумну “першість”.

Упродовж буквально кількох років жителям величезної держави довелося стати свідками, учасниками і жертвами двох катастроф планетарного масштабу — Чорнобильської аварії та геополітичної анігіляції своєї країни, яка ще “вчора” здавалася вічною, непорушною і могутньою.

Зникли колишні життєві орієнтири. Миттєво змінилися звичний устрій і повсякденний спосіб життя. Суспільство опинилося в стані глибокого, стійкого, системного соціально-психологічного неврозу. Якщо порівнювати пострадянське суспільство з організмом, то наслідки переходу до ринку і демократії цілком можна кваліфікувати як суспільну політичну травму.

Невпевненість, що виникає у зв’язку з цим, охоплює майже всі соціальні прошарки. У суспільстві все більше з’являється людей, для яких розмір прибутку набагато важливіший, ніж методи його отримання. У цих умовах найбільш поширеними й інтенсивними людськими відчуттями — і суспільними, й індивідуальними — стають тривога, неспокій, страх. І все інтенсивніше використовуються засновані на них політичні технології. Вибірчі кампанії все більше набувають рис справжніх битв.

Все більше з’являється свідчень і підтверджень тому, що нічим і ніким не обмежений і не обмежуваний так званий вільний ринок при всій його початковій (особливо після тотального панування насильницько-зрівняльного розподілу) привабливості не може забезпечити задоволення соціальних потреб основних верств суспільства.

Було б спрощенням бачити загрози інформаційній безпеці виключно у сфері інформаційно-масових процесів. Багато в чому вони породжуються і політичною нестабільністю, і економічними труднощами, і невирішеними соціальними проблемами українського суспільства.

Є підстави стверджувати, що основна проблема забезпечення інформаційної безпеки — це балансування між свободою доступу до інформації та необхідністю її обмеження в загальнодержавних інтересах. Досягнення такого балансу залежить від рівня культурного й економічного розвитку країни. Для цього необхідно застосовувати системний нормативно-правовий механізм, який забезпечить, з одного боку, захист інформаційних прав і свобод, а з другого — демократичний моніторинг і регулювання рівня інформаційної безпеки.

На верхньому рівні нормативно-правової ієрархії має бути документ доктринального характеру, який закріплює основи інформаційної безпеки, тобто визначає системно-концептуальний погляд на сутність, форми і способи вирішення проблеми захисту національних інтересів в інформаційній сфері. Наступним має бути рівень документів, які визначають принципи інформаційної політики при реалізації положень доктрини в усіх інформаційних складових кожної сфери національної безпеки. Таким чином, буде визначена єдина інформаційна політика щодо захисту суб'єктами інформаційної безпеки їхніх об'єктів в усіх сферах життєдіяльності. Далі мають розроблятися документи, які за змістом є конкретними цільовими програмами і планами дій з реалізації принципів єдиної інформаційної політики шляхом створення, використання і розвитку відповідних методів, засобів і технологій [3].

Сучасна Україна стрімко вбирає в себе інформаційну складову, що, з одного боку, відчутно підсилює її демократичний потенціал, а з другого — не менш відчутно створює ряд проблем і вразливих місць для цієї ж демократії. Знання точок інформаційно-психологічної вразливості, вміння захистити їх від недружніх дій, поза сумнівом, слугуватиме успішному виконанню завдань, що стоять перед Україною, зокрема й щодо поліпшення життя всього українського суспільства.

Україна завжди, а особливо впродовж другої половини ХХ ст., була могутньою частиною світового військово-промислового комплексу і сьогодні успадковує та зберігає ідеї та розробки у цій сфері знань [4].

Відповідно до Указу Президента України № 377/2008 від 23 квітня 2008 р. в Інституті проблем національної безпеки розроблено проект “Доктрини інформаційної безпеки України”, який уже оприлюднений на сайті Ради національної безпеки й оборони України. Правовою базою для її розробки і реалізації є Конституція України, Закон України “Про основи національної безпеки України”, Указ Президента України “Про стратегію національної безпеки України”, інші закони України, а також міжнародні угоди, ратифіковані Верховною Радою України, що визначають основи державної політики у сфері інформаційної безпеки.

Доктрина спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду і призначена для:

- формування ефективної державної політики у сфері забезпечення інформаційної безпеки України;
- підготовки вивірених пропозицій для подальшого системного вдосконалення правового, методичного, науково-технічного та організаційного забезпечення інформаційної безпеки України;
- розробки науково обґрунтованих цільових програм і планів дій із забезпечення інформаційної безпеки України, центрів влади й управління, державних і приватних підприємств.

Історичний досвід незалежної України свідчить, що каталізатором успішного практичного розв'язання проблеми національної інформаційної безпеки, врешті-решт, є політична воля — реальна здатність перших осіб до цілеспрямованої організації та об'єднання зусиль влади, бізнесу і громадян для побудови сучасного інформаційного суспільства. У зв'язку з цим нагадаємо вислів Уїнстона Черчілля: “Політичний діяч думає про майбутні вибори, а державний діяч — про майбутнє покоління”. Цей вислів набуває особливої актуальності в наших умовах.

На думку Е. І. Низенко, розвиток комп'ютерних технологій і їх використання в багатьох сферах економіки є на сьогодні одним з головних факторів її ефективності. Проте прогрес в інформаційній сфері створив і потенційні загрози у вигляді розроблення нових та вдосконалення вже відомих методів наукового шпигунства.

Збирання інформації про розробки високих технологій завжди було і залишається одним з пріоритетів у діяльності розвідок світу. Для отримання цінної інформації застосовуються всі доступні засоби і методи, серед них і різні типи аналізаторів [8, 9].

Захист інформації не обмежується технічними методами. Проблема є значно ширшою. Основний недолік захисту — люди, і тому надійність системи безпеки залежить в основному від ставлення до неї. Крім цього, захист повинен постійно вдосконалюватися разом з розвитком комп'ютерної мережі.

Нині узагальнену теорію безпеки інформації поки не створено. Застосовувані на практиці підходи й засоби нерідко страждають від істотних недоліків і не мають оголошену надійність. Тому необхідно володіти достатньою підготовкою й кваліфіковано орієнтуватися в усьому спектрі питань забезпечення інформаційної безпеки, розуміючи їх комплексний і взаємообумовлений характер.

Особливе місце в забезпеченні інформаційної безпеки держави займає національне співробітництво держав у даній сфері. Через ряд причин політичного й історичного характеру, через розбіжності у рівні розвитку національних економік і суспільства, національні інтереси окремих держав можуть не повністю збігатися між собою, що створює об'єктивні передумови для формування кожною державою своїх національних систем забезпечення інформаційної безпеки. Водночас глобальність процесів інформаційної взаємодії між громадянами різних держав, трансграничність комп'ютерної злочинності роблять необхідним об'єднання зусиль різних держав у боротьбі з тими загрозами, з якими вони не в змозі впоратися самостійно [5].

Це робить необхідним пошук “точок зближення” між державами в галузі забезпечення інформаційної безпеки, закріплення сукупних інтересів і спільне проведення заходів щодо їхнього захисту переважно на основі двосторонніх і багатосторонніх угод. На наш погляд, таке співробітництво могло б розвиватися у таких напрямках:

1. Прискорення розробки міжнародних принципів, які були б спрямовані на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем і сприяли б боротьбі з інформаційним тероризмом і криміналом.
2. Розробка узгоджених стратегій і державної політики в галузі забезпечення інформаційної безпеки, а також заходів і механізмів, пов'язаних з їх реалізацією, включаючи вдосконалювання форм, методів і засобів виявлення, оцінки й прогнозування загроз інформаційній безпеці, а також системи протидії цим загрозам.
3. Розвиток міжнародного співробітництва в галузі заборони розробки, поширення і застосування інформаційної зброї.
4. Удосконалення й уніфікація нормативної правової бази забезпечення інформаційної безпеки держав, включаючи механізми реалізації прав і свобод громадян в інформаційній сфері, форми і способи реалізації правових норм, що стосується взаємодії держави із засобами масової інформації.
5. Розширення взаємодії з міжнародними органами й організаціями при вирішенні науково-технічних і правових питань забезпечення безпеки інформації в міжнародних інформаційних і телекомунікаційних системах.

6. Забезпечення необхідного рівня технологічної незалежності держав у найважливіших сферах інформатизації і зв'язку, що визначають їх безпеку.
7. Розвиток науково-практичних основ забезпечення інформаційної безпеки з урахуванням сучасної геополітичної ситуації й існуючих загроз застосування інформаційної зброї.
8. Розробка критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки, уніфікація сертифікації цих систем і засобів.
9. Розвиток національних систем підготовки кадрів у галузі інформаційної безпеки й інформаційних технологій і надання взаємодопомоги в цих питаннях.
10. Зміцнення взаємодії правоохоронних органів держав щодо запобігання комп'ютерним (інформаційним) злочинам.

Забезпечення інформаційної безпеки — необхідна умова формування інформаційного суспільства. З огляду на це здатність держави, суспільства, особистості забезпечити з певною ймовірністю достатні й захищені інформаційні ресурси та інформаційні системи для підтримки своєї життєдіяльності й довіри до них характеризують їхню готовність до гідного й рівноправного партнерства в умовах нової суспільно-економічної формації — інформаційного суспільства.

Поширення й використання інформаційних технологій і засобів зачіпає інтереси усієї міжнародної спільноти, і тільки широке міжнародне співробітництво здатне забезпечити їх безпечне застосування в інтересах кожної держави. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки має будуватися на основі поєднання національних інтересів зацікавлених країн в інформаційній сфері, їхніх уявлень про загрози цим інтересам, методи і засоби протидії загрозам.

Отже, поки в країні не настане політична, економічна, а відповідно й соціальна та інформаційна стабільність, не вдосконалиться законодавство, безпека інформаційного простору України перебуватиме під масовими впливами як внутрішніх, так і зовнішніх сил.

Комплексний характер проблем інформаційної сфери потребує по-новому визначити загрози безпеці та оцінити їхню небезпеку, розробити теоретичні й методологічні основи напрямів протидії з огляду на національні інтереси кожної країни, з якою спілкуємось. Потрібна широка загальнона-

ціональна дискусія фахівців державних інституцій та громадських структур, що займаються питаннями інформатизації держави та підготовки кадрів з метою розробки концепції та стратегії розвитку інформаційного законодавства України. Вони мають віддзеркалити системне бачення нашого інформаційного простору в єдності всіх елементів його інфраструктури, ефективного використання потенціалу інформаційних ресурсів, форм та засобів інформаційно-комунікаційних технологій як складових інноваційних проєктів розвитку України в глобальному вимірі.



Література

1. Закон України "Про основи національної безпеки України" // ВВР України. — 2003. — № 39. — С. 351.
2. Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества: Материалы круглого стола, Москва, октябрь 2000 г. / Под ред. В. И. Добренкова. — М.: Изд-во МГУ. — 2001. — С. 34–41.
3. Горбулін В. П., Биченок М. М., Копка П. М. Актуальні проблеми системного забезпечення інформаційної безпеки України // Матеріали Міжнар. наук.-практ. конф. "Форми та методи забезпечення інформаційної безпеки держави". — К.: Нац. акад. СБ України. — 2008. — С. 79–85.

4. Держкомінформ започатковує державну програму "Журналіст" // Телекритика. Режим доступу: <http://www.telekritika.ua/media-rinok/regulyuvannya/verhovna-rada>

5. Дзьобань О. П. Національна безпека в умовах соціальних трансформацій (методологія дослідження та забезпечення): Моногр. / О. П. Дзьобань. — Х.: Константа. — 2006. — 440 с.

6. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К.: МАУП. — 2006. — 133 с.

7. Низенко Е. І. Загальнотеоретичні характеристики окремих напрямів захисту конфіденційної інформації від злочинних посягань // Наук. пр. МАУП. — К.: МАУП. — 2007. — Вип. 1 (15). — С. 127–132.

8. Лисичкин В., Шелепин Л. Третья мировая (информационно-психологическая) война. — М.: Ин-т соц.-полит. иссл. АСН. — 2000. — 304 с.

9. Прохоров А. М. Політичні технології як інформаційно-психологічне маніпулювання свідомістю / А. М. Прохоров // Політична культура: теорія, проблеми, перспективи. — К.: ПАРАПАН. — 2004. — С. 215–218.

10. Соболь О. Свобода особистості в інформаційному соціумі // Філософська думка. — 2002. — № 5. — С. 40–58.

11. Судоргин О. Новая роль информационного пространства в XXI веке // Власть. — 2009. — № 1.

12. Сухов А. Социальная психология безопасности. — М.: Академия. — 2002. — 256 с.

13. Утюж І. Г. Формування глобального інформаційного суспільства — виклик часу // Нова парадигма (Альманах наукових праць). — 2003. — Вип. 30. — С. 122–133.

Розглянуто деякі проблемні аспекти інформаційної безпеки, а також особливості інформаційної безпеки як однієї з головних складових національної безпеки України. Розкрито основні напрями національної політики України в галузі інформаційної безпеки.

Рассмотрены некоторые проблемные аспекты информационной безопасности, а также особенности информационной безопасности как одной из главных составляющих национальной безопасности Украины. Раскрыты основные направления национальной политики Украины в области информационной безопасности.

The article specifies some problematic aspects of informative security. Also features are examined informatively safety as one of main constituents of national safety of Ukraine. It is exposed basic directions of national policy of Ukraine concerning information security.

Надійшла 26 квітня 2010 р.