

Секція 1. Економічна та інформаційна безпека

УДК 621.3.037.3:[347.21:65.012.8](477)

І.О. Громико¹, Т.І. Саханчук²

¹Харківський національний університет внутрішніх справ, Харків

²Військовий інститут інформатизації та телекомунікацій НТУУ «КПІ», Київ

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Всі уряди розвинутих країн світу визнають важливу значущість інформаційної компоненти в державній політиці безпеки своїх держав. Це у повному обсязі відноситься до України, на території якої к моменту отримання незалежності накопичено наймогутніший науковий потенціал.

У зв'язку з наявністю загроз інформації кожна держава відстоює свій інформаційний суверенітет, основою якого є національні інформаційні ресурси. Тому Конституція України визначає захист суверенітету і територіальної цілісності, забезпечення економічної та інформаційної безпеки найважливішими функціями держави, справою всього українського народу.

Добра атмосфера законотворчої змагальності дозволяє урядам колишнього СРСР розробляти пакети міждержавних законодавчих актів і створювати сучасні національні законодавчі бази незалежних держав у тісному міжнародному спілкуванні.

Разом з тим не можна не зауважити, що при розробці інформаційно-правових баз незалежних держав має місце процес накопичення помилок. Вони стають занадто помітними у тих випадках, коли науковці мають діаметрально протилежні погляди на вирішення тих чи інших проблем. Так склалося з сучасним визначенням терміну «інформаційна безпека держави», котре зараз або існує у проектах, або дублює варіанти закордонного тлумачення.

Назріла необхідність коректного формулювання саме визначення інформаційної безпеки України, що усуне помилки трактувань даного терміну, і сприятиме розвитку держави.

Принципове значення має обов'язкова підпорядкованість визначення «інформаційної безпеки України» наступним домінуючим у процесі безпечного розвитку держави ідеям:

1) орієнтованість на інформаційний стан розвитку держави та ведучих країн світу;

2) сприяння інтеграції держави у прогресивне світове товариство;

3) повне врахування внутрішніх та зовнішніх загроз національним інформаційним ресурсам та системам інформації;

4) створення правового підґрунтя для застосування попереджальних заходів у боротьбі з загрозами.

Кожна країна відстоює свій інформаційний суверенітет, основою якого є національні інформаційні ресурси. Тому Конституція України визначає захист суверенітету і територіальної цілісності, за-

безпечення економічної та інформаційної безпеки найважливішими функціями держави, справою всього українського народу [1]. У свою чергу, Закон України «Про інформацію», виділяє основні елементи забезпечення інформаційного суверенітету України [2], захист яких диктує, що в першу чергу необхідно протидіяти: порушенню права власності України на свої інформаційні ресурси; спробам завадити створенню (та функціонуванню, - автори) національних систем інформації; несанкціонованій зміні, тобто порушенню режиму доступу інших держав до інформаційних ресурсів України; порушенню принципу рівноправного співробітництва з іншими державами.

Традиційно, загрози поділяють на дві великі групи – внутрішні та зовнішні. Однак, загрози інформаційній безпеці України є складними інформаційними процесами, які не припускають спрощеного вивчення джерел загроз, атак та наслідків.

Розгляд змісту тільки однієї з загроз інформаційному суверенітету України показує (див. таблицю), що у внутрішніх загрозах є така важлива риса, як здатність створювати джерела зовнішніх загроз.

Ретельний розгляд складових терміну «Інформаційна безпека» показує, що відсутність підпорядкованості державним домінантам приводить авторів або до надмірної конкретизації визначень, або до втрати суттєво важливих елементів безпеки і державності. І на цей час в інформаційно-правових джерелах приведено істотно відмінні варіанти визначень термінів.

Слід констатувати, що державна домінантність інформаційної безпеки України вимагає наявності у визначенні цього терміну інформації про запобігання та протидію всім різновидам загроз. Тому авторами враховано наступне: 1) поняття протидії інформаційним будь-яким загрозам як правило об'єднують перераховуючи по тексту; 2) процес створення інформаційних загроз системою (державою) для елементів самої системи можна віднести до різновиду внутрішніх загроз; 3) забезпечення інформаційного суверенітету України в його розумінні як «здатності держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» дозволяє стверджувати [2], що застосування в визначенні терміну «інформаційний суверенітет» це не тільки протидія загрозам державі ззовні. Цей

термін є інтегральним і охоплює як протидію загрозам, що створюють джерела зовнішніх загроз. зам ззовні держави, так і протидію внутрішнім за-

Таблиця

Зміст загрози інформаційному суверенітету України

Загроза	Деякі варіанти змісту загрози	Тип загрози
Порушення права власності України на свої інформаційні ресурси	Крадіжка промислових технологій з державних підприємств оборонного комплексу іноземними бізнес-структурами, які працюють у правовому полі України на її території. Мета: особисте збагачення та ін.	Внутрішня
	Крадіжка промислових технологій з державних підприємств України розвідниками іноземних держав. Мета: – економія іноземними державами ресурсів, що витрачаються на наукові дослідження (час, кошти, люди) й ін.; – озброєння військових підрозділів вдосконаленою та більш ефективною зброєю й т. ін.	Зовнішня.
	Модифікація та несанкціонована зміна вмісту інформаційних ресурсів вітчизняними хакерами (по замовленню правопорушників), яка може привести до розповсюдження за кордоном неправдивої інформації про Україну, дії керівництва держави. Мета: дискредитація України перед світовим співтовариством для: – отримання додаткових прибутків в економічному ракурсі; – політичної переваги у виборному процесі; – стимуляції небажаних дій з боку іноземних держав відносно України, керівництва, діяльності підприємств-конкурентів, установ та ін.	Внутрішня, що створює зовнішню
	Пошкодження, підробка вмісту інформаційних ресурсів (або таке інше діяння) та розповсюдження за кордоном неправдивої інформації про Україну, дії керівництва держави (й ін.) закордонними хакерами під керівництвом терористичних або розвідувальних і військових організацій Мета: дискредитація України перед світовим співтовариством для: – отримання переваг в економічному, політичному та військовому ракурсах; – виправдання незаконних дій (наприклад, - військового вторгнення) іноземних держав у будь-якому регіоні світу; – організації негативних дій іноземних держав відносно України, керівництва, діяльності підприємств, установ та ін.	Зовнішня

Крім того, спираючись на світовий досвід, доцільно підкреслити, що загрозою безпеці держав, що тільки отримали незалежність, може бути також їх надмірна ізольованість від інших країн [4]. Тому міжнародне інформаційне співробітництво має бути враховане як обов'язкова умова – одна з вагомих складових забезпечення інформаційної безпеки України.

Таким чином ретельний аналіз всіх складових дозволяє сформулювати визначення у наступному вигляді:

«Інформаційна безпека України – це захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний

розвиток міжнародного інформаційного співробітництва».

Список літератури

1. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – № 30 – С. 141.
2. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – С. 650.
3. Закон України «Про національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України, 1998. – № 27 – 28. – С. 181.
4. Пендюра М.М. Національні інтереси – фундаментальний елемент національної безпеки України в умовах євроінтеграції / М.М. Пендюра // Держава і право. – 2004. – № 26. – С. 48-52.