Координація діяльності правоохоронних органів та інформаційна безпека

Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід’ємною складовою яких є інтенсивне використання досягнень сучасних інформаційних технологій. Після вибору Україною шляху до інтеграції в Європу, яка сьогодні активно розбудовує інформаційне суспільство, гостро постала проблема ефективного забезпечення інформаційної безпеки молодої держави.

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп’ютерної злочинності і т. ін. Тому Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави [1].

Концепцією (основами державної політики) національної безпеки України визначено загрози національній безпеці України в інформаційній сфері:

невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері;

повільність входження України у світовий інформаційний простір;

інформаційна експансія з боку інших держав;

витік інформації, що становить державну та іншу передбачену законом таємницю.

Концепцією визначено основні напрями державної політики національної безпеки України в інформаційній сфері, зокрема:

вжиття комплексних заходів щодо захисту свого інформаційного простору та входження України до світового інформаційного простору;

усунення негативних чинників порушення інформаційного простору;

розробка і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значимої інформації, створення розвиненої інфраструктури в інформаційній сфері і т. ін. [2].

Як свідчать наукові дослідження, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в рамках адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки України та інші чинники зумовлюють ескалацію загроз, що може призвести (і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам України [3].

У цьому аспекті своєчасним та дійовим (важливим) нормативно-правовим документом став Указ Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України”» від 6 грудня 2001 р. № 1193/2001 [4].

Указом передбачено розробку Концепції національної інформаційної політики та інформаційної безпеки України, здійснення заходів щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації, створення організаційної структури системи забезпечення інформаційної безпеки, аналіз програм в інформаційній сфері, які фінансуються з Державного бюджету України, вжиття заходів стосовно першочергової реалізації та повноцінного фінансування найактуальніших з них та інші важливі заходи для забезпечення інформаційної безпеки.

З огляду на зазначене, варто зупинитися на одному з найважливіших аспектів забезпечення належного захисту інформаційної безпеки – на координації діяльності державних органів, приватного сектору, громадських організацій та окремих громадян. Згідно зі статтею 17 Конституції України забезпечення інформаційної безпеки – справа усього українського народу.

Проблема координації є важливою сама по собі та набуває значення у зв’язку з тим, що, на відміну від багатьох інших галузей, у сфері інформаційних технологій постійно змінюється термінологія, ламаються традиційні уявлення про методи та засоби передачі, отримання, обробки та зберігання інформації, хоча часом за зміною вже сталих термінів простежується тільки робота маркетологів з просування власних проектів. Це призводить до того, що одне й те саме поняття описується завдяки різним термінам, і, навпаки, один і той самий термін несе різне значеннєве навантаження.

Наприклад, під поняттям “інформаційні війни” фахівці технічних галузей знань розуміють порушення електронної інфраструктури суспільства (у розвинених країнах – мережі державних та фінансових установ, таких як управління транспортом, електроживлення, військові та космічні системи, що неодноразово піддавались атакам кібертерористів). У разі, коли здійснення терористичного акту буде поєднано з атакою на інформаційну систему рятувальних служб, медичних закладів чи правоохоронних органів, збитки від нього можуть виявитися колосальними. З остраху стосовно здійснення таких атак з боку країн “третього світу” призвело до появи спеціальних силових підрозділів, що володіють інформаційною зброєю та методами захисту від нього.

Інакше трактують це поняття фахівці гуманітарного профілю, працівники засобів масової інформації. Під “інформаційними війнами” вони розуміють нав’язування певних ідеологічних стереотипів, тієї чи іншої суспільної думки за допомогою засобів масової інформації, у тому числі через електронні видання.

Якщо на побутовому рівні різне тлумачення термінологічних понять можна зрозуміти з контексту повідомлення, то у правозастосуванні понятійна невизначеність призводить до знецінення самих законів.

Вагомим кроком на шляху до координації діяльності державних органів став Указ Президента України “Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України” від 22 січня 2002 р. № 63/2002, згідно з яким було створено відповідну Міжвідомчу комісію на чолі з Секретарем Ради національної безпеки і оборони України [5].

Основні завдання Комісії такі:

аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики;

аналіз здійснення галузевих програм і виконання заходів, пов’язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері;

розроблення і внесення Президентові України та Раді національної безпеки і оборони України пропозицій стосовно: визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення інформаційної безпеки держави; здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір; удосконалення системи правового та наукового забезпечення інформаційної безпеки України; розвитку інформаційної інфраструктури держави, зокрема з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення; організації та порядку міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;

удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі й альтернативною інформацією) у сфері національної безпеки і оборони.

Одну з найнебезпечніших загроз національній безпеці України в інформаційній сфері становить так звана “комп’ютерна злочинність” [6]. Як показують дослідження Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю, рівень загрози буде зростати пропорційно розширенню використання нових інформаційних технологій в управлінні, бізнесі, торгівлі. Загрози можуть бути як зовнішніми, так і внутрішніми. Слід зазначити, що у зв’язку із поширенням використання в Україні глобальної комп’ютерної мережі Інтернет та з приєднанням до міжнародних систем телекомунікацій нових країн, підвищенням інтелектуального рівня зловмисників зовнішня загроза постійно зростатиме. Через глобальну комп’ютерну мережу Інтернет, що не має державних кордонів, хакери мають несанкціонований доступ до комп’ютерної інформації, а для проведення безподаткових фінансових операцій, “відмивання брудних” коштів через електронні банківські системи глобальна мережа створює принципово нові умови, які у повному обсязі використовують кримінальні структури. Тому вже сьогодні необхідною є відповідна координація зусиль щодо забезпечення протидії цьому виду правопорушень.

На сьогодні найгострішою проблемою залишається створення Міжвідомчого центру боротьби з комп’ютерною злочинністю (МЦБКЗ), в якому необхідно організувати контактний пункт для отримання повідомлень про “кіберзлочини” та надання оперативної допомоги жертвам зловмисників, а також організувати лабораторію для проведення комп’ютерних експертиз. Центр може стати місцем для організації семінарів, практикумів у системі підготовки суддів, прокурорів, слідчих. Якщо сьогодні на створення та функціонування МЦБКЗ не буде виділено достатніх фінансово-матеріальних ресурсів, то у недалекому майбутньому втрати економіки держави від комп’ютерної злочинності виявляться набагато більшими.

Міжвідомчий центр боротьби з комп’ютерною злочинністю міг би стати практичним органом виконавчої влади щодо координації роботи правоохоронних органів у сфері інформаційних технологій, що дозволить підтримувати в Україні необхідний рівень інформаційної безпеки, сприятиме входженню нашої держави до світового інформаційного суспільства з усіма його перевагами.

Як показують наші дослідження, вирішення зазначеної проблеми неможливе без комплексу заходів, який передбачає широке залучення громадськості, міністерств та відомств, навчальних закладів, засобів масової інформації з формування у населення відповідного правового менталітету.

Вирішенню цього питання може сприяти громадська організація “Асоціація захисників інформації”.

Робота членів Асоціації може допомогти у формуванні державної політики стосовно інформаційної безпеки шляхом:

обговорення законопроектів з питань інформаційної безпеки з подальшим внесенням пропозицій до органів влади та управління;

координації і методичного забезпечення освіти населення щодо інформаційної безпеки;

організації презентацій розробок програмно-технічних систем захисту інформації;

популяризації літератури у сфері інформаційної безпеки;

координації зусиль фахівців з технічного захисту інформації у розробці та впровадженні технічних засобів захисту інформації;

міжнародного співробітництва з організаціями, науковими установами з питань інформаційної безпеки.

1. Конституція України: Прийнята на п’ятій сесії Верховної Ради України 28 черв. 1996 р. – К.: Україна, 1996. – 54 с.

2. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 р. // Відомості Верховної Ради. – 97. – № 3.

3. Жданов І. Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України // Матеріали до круглого столу “Безпека інформації в інформаційно-телекомунікаційних системах”. – К., 2001. – 28 трав.

4. Указ Президента України «“Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України”» від 6 грудня 2001 р. № 1193/2001.

5. Указ Президента України “Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України” від 22 січня 2002 р. № 63/2002.

6. Комп’ютерна злочинність: Навч. посіб. – К.: Атіка. – 240 с.