УДК 347.731:681.3

О. В. Бойченко

ПИТАННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Наведено аналіз нормативно-правового забезпечення інформаційної безпеки як системи заходів запобігання шкоді національним інтересам України в інформаційній сфері. Визначено коло загальнодержавних заходів щодо підвищення рівня нормативно-правового забезпечення інформаційної безпеки держави.

Постановка проблеми. Наразі становлення інформаційного суспільства в Україні є доволі складним процесом. Ця складність визначається політико-економічними обставинами, характерними для сьогодення України, які не тільки стримують становлення демократичного суспільства, ринкових економічних відносин у державі, але й уповільнюють створення сучасних інформаційних відносин. Особлива проблема становлення інформаційного суспільства – створення дієвої системи заходів інформаційної безпеки, яка є складовою частиною національної безпеки держави. Тому наукові розробки стосовно вивчення проблем інформаційної безпеки та пропозицій щодо їх вирішення, особливо в частині нормативно-правового забезпечення, є необхідними та нагальними.

Аналіз останніх досліджень і публікацій. Узагальнюючи наукові здобутки, погляди та висновки провідних фахівців у сфері забезпечення інформаційної безпеки (О. Н. Бандурки, І. В. Арістової, О. Г. Фролова, Р. А. Калюжного, А. О. Письменицького, Б. А. Кормича, В. М. Брижка, І. Л. Бачила, В. П. Захарова, С. А. Дзіса, М. М. Дутова, М. В. Карчевського, Л. П. Паламарчука, Д. Я. Семир'янова та інших науковців), можна дійти висновку, що наявність досконалого нормативно-правового регулювання є одним із базових інструментів захисту національної безпеки в інформаційній сфері. Стрімкий і постійний розвиток інформаційно-телекомунікаційних технологій обумовлює необхідність безперервного відстеження рівня відповідності нормативно-правової бази тим загрозам, що існують в інформаційній сфері, і тому ця сфера діяльності людини потребує всебічного вивчення та подальших наукових досліджень.

Мета роботи – аналіз наявної нормативно-правової бази щодо забезпечення інформаційної безпеки у контексті загальної системи заходів забезпечення національної безпеки України та окреслення можливих напрямків удосконалювання цієї бази.

Виклад основного матеріалу. Законодавство України надає великого значення інформаційному складнику національної безпеки. Так, у ч. 1 ст. 17 Конституції України зазначається: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу" [1].

У цьому контексті інформаційна безпека розглядається на одному рівні з такими невід'ємними атрибутами державності, як суверенітет і територіальна цілісність. Проте необхідно зауважити, що ці категорії не є одного порядку. Усі аспекти національної безпеки, у тому числі й інформаційний, ґрунтуються на такому складнику, як державний суверенітет.

Оскільки мова йде про інформаційну безпеку як складник національної безпеки, то її джерелом необхідно вважати не лише суверенітет держави, а й суверенітет народу та нації як суб'єктів інформаційних відносин.

У Законі України "Про інформацію" така дефініція наводиться, але чіткого тлумачення її змісту немає. Так, у ст. 53 цього Закону ("Інформаційний суверенітет") хоч і вказується, що "основою інформаційного суверенітету України є національні інформаційні ресурси", проте зміст самого поняття інформаційного суверенітету не розкривається. До інформаційних ресурсів України згідно з нормами ст. 53 Закону України [2] входить уся належна їй інформація, незалежно від змісту, форм, часу і місця створення.

Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Таким чином, у рамках Закону України "Про інформацію" інформаційний суверенітет здебільшого розглядається як невід'ємне право держави формувати та розпоряджатися інформаційними ресурсами, які знаходяться в її власності відповідно до національного та

міжнародного законодавства [2]. Однак варто зауважити, що в такому випадку йдеться не про суверенітет, а про реалізацію права власності держави на певні види майна (майнові права).

У п. 3 розділу IV Національної програми інформатизації зазначається: "Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни" [3].

Крім того, передбачено, що результатом виконання Програми будуть:

– комплект нормативних документів з усіх аспектів використання засобів обчислювальної техніки для обробки та зберігання інформації обмеженого доступу;

– комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації;

– банк засобів діагностики, локалізації і профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо.

Як бачимо, у цьому випадку йдеться про відповідну інформаційну інфраструктуру та інформаційні ресурси, що покликані створювати безпечні і сприятливі умови життєдіяльності окремих осіб, усього суспільства та держави в цілому.

Інформаційна безпека – це стан захищеності національних інтересів в інформаційній сфері від внутрішніх та зовнішніх загроз. У свою чергу, забезпечення інформаційної безпеки – це система заходів запобігання шкоді національним інтересам в інформаційній сфері.

Необхідно навести деякі основні характеристики інформаційної безпеки, що зумовлюються специфікою її об'єкта.

1. Насамперед це зона інформаційної безпеки, яка розташована на пересіченні функції забезпечення національної безпеки та інформаційної функції держави. Це є дуже важливий момент у сукупності заходів збереження національного суверенітету України, тому що небажаний витік інформації при функціонуванні будь-якої сфери життєдіяльності суспільства спричиняє негативні наслідки стосовно національної безпеки держави.

2. Питання інформаційної безпеки держави має екстериторіальний характер, тобто такий, який визначається вагомими аспектами взаємодії України з іншими державами світу з приводу високоінтегрованої системи економічних, господарських та інших зв'язків, що, у свою чергу, потребує проведення нагальних заходів протидії витоку інформації конфіденційного характеру.

3. Суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними та різноплановими. Зазначене зумовлене стрімкими процесами інтеграції, насамперед української економіки в європейське та світове економічне товариство.

4. Компетенція державних органів у сфері інформаційної безпеки органів держави з регулювання інформаційних процесів. Одним із складників механізму інформаційної безпеки є Міністерство внутрішніх справ України, оскільки у його розпорядженні перебувають найбільш вагомі й ефективні засоби застосування державного примусу в інформаційній сфері. Виходячи з викладеного підрозділи МВС України вирішують низку завдань щодо забезпечення інформаційної безпеки.

5. У демократичному суспільстві державне регулювання інформаційної сфери можливе лише у визначених правом межах. Законодавство України в інформаційній сфері доволі розвинене, що забезпечує відповідний рівень нормативно-правового регулювання заходами забезпечення інформаційної безпеки. Однак недосконалість (або навіть відсутність) відповідних правових норм породжує низку проблем, що утруднюють застосування системи заходів захисту конфіденційної інформації. Зокрема, Верховною Радою України досі не прийнято Закон України "Про інформаційну безпеку України", який має стати базовим законодавчим актом побудови системи узгоджених правових інститутів цієї сфери.

6. Однією з, можливо, найважливіших характеристик інформаційної безпеки є політика інформаційної безпеки. Вона має багатовекторний характер, головним складником якого є регулювання інформаційних відносин.

Політика інформаційної безпеки здійснюється з метою:

– забезпечення свободи слова та доступу громадян до інформації відповідно до вимог Конституції України та Закону України "Про інформацію";

– протидії поширенню у засобах масової інформації культу насильства, жорстокості, порнографії відповідно до наведених вище

нормативних актів, а також згідно з нормами Кримінального та Кримінально-процесуального кодексів України. Зрозуміло, що виконання завдань зазначеного напрямку безпосередньо покладено на правоохоронні органи, у тому числі й органи внутрішніх справ (ОВС) України, що, у свою чергу, також визначає важливу роль та функцію ОВС у вирішенні питань забезпечення інформаційної безпеки держави;

– боротьби з комп'ютерною злочинністю та комп'ютерним тероризмом, що теж є прерогативою діяльності ОВС України. Тому широке запровадження сучасних інформаційно-пошукових систем, новітніх технічних систем захисту інформації, суттєве технічне переоснащення оперативних підрозділів ОВС може забезпечити достатній рівень протидії комп'ютерній злочинності, яка в наш час набуває найбільш глобальних масштабів. Проблема загострюється у зв'язку з тим, що комп'ютерні злочини зрощуються зі злочинами загальнокримінального напрямку, тобто є інструментом для їх підготовки, вчинення або навіть маскування фактів підготовки або вчинення злочину;

– недопущення розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– протидії намаганням маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

Однією із загроз суспільству є комп'ютерна злочинність. Протидія їй – одне із завдань правоохоронних органів України [4, 5].

Останнім часом комп'ютерна злочинність має транснаціональний та організований характер. Так, якщо у 2003 – 2004 рр. слідчими підрозділами СБУ було порушено лише 7 кримінальних справ у сфері протиправного застосування інформаційно-телекомунікаційних технологій, то за 2005 р. їх кількість зросла до 40. І найхарактернішими для цього періоду протиправними діяннями є несанкціоноване втручання в роботу автоматизованих систем, створення та розповсюдження комп'ютерних вірусів, несанкціонований збут інформації з обмеженим доступом тощо.

Це свідчить про підвищення рівня криміналізації інформаційно-телекомунікаційної сфери з одночасною активізацією діяльності органів внутрішніх справ щодо виявлення, попередження та припинення комп'ютерних злочинів як адекватне реагування на посилення згаданої загрози інформаційній безпеці держави з метою її мінімізації. Водночас на підставі аналізу сучасної ситуації у сфері забезпечення інформаційної безпеки можна зробити висновок про суттєве відставання України від системних заходів, насамперед правового характеру, що вживаються провідними державами світу.

Так, на ефективність діяльності правоохоронних органів щодо забезпечення інформаційної безпеки держави негативно впливає недосконала нормативно-правова база у сфері протидії комп'ютерній злочинності.

Незважаючи на те, що Верховною Радою України ратифіковано міжнародну Конвенцію про кіберзлочинність, є низка проблемних правових питань, нез'ясованість яких стримує ефективну реалізацію правозастосовчої функції правоохоронних органів, що протидіють комп'ютерній злочинності та комп'ютерному тероризму.

На сьогодні не вирішено проблему законодавчого регулювання правових відносин між суб'єктами ринку Інтернет-послуг, зокрема немає відповідного нормативно-правового регулювання підприємницької діяльності з надання послуг доступу до мережі Інтернет.

У січні 2005 р. з метою посилення відповідальності за комп'ютерні злочини набрали чинності зміни до Кримінального та Кримінально-процесуального кодексів України.

Однак, незважаючи на те, що нові статті Кримінального кодексу України конкретизують види комп'ютерних злочинів і з першого погляду є позитивним зрушенням у справі боротьби з комп'ютерними злочинами, вони все ж таки потребують поглибленого науково-практичного опрацювання для чіткого встановлення кваліфікуючих ознак складу злочинів.

Крім того, у зв'язку з ратифікацією Конвенції про кіберзлочинність уже зараз потрібно вносити до розділу певні зміни відповідно до вимог міжнародного законодавства, адже у наявному змісті розділу XVI Кримінального кодексу України не враховано міжнародний підхід до визначення кола суспільно небезпечних діянь, які визнаються комп'ютерними правопорушеннями щодо інформації, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями; підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення,

пов'язані з порушенням авторських та суміжних прав.

Взагалі у чинному Кримінальному кодексі зазначено низку злочинів, що можуть бути віднесені до категорії інформаційних, але містяться вони в різних розділах кодексу, що зумовлює визначення родових об'єктів цих злочинів різними.

Ураховуючи сучасний рівень розвитку інформаційних відносин та зростаючу значущість інформаційних ресурсів, доцільно погодитися з деякими поглядами науковців-правників щодо виділення в окрему групу інформаційних злочинів, родовим об'єктом яких є суспільні відносини у сфері інформаційної безпеки в Україні (забезпечення безпеки інформації, безпеки від впливу інформацією та захисту прав суб'єктів інформаційних відносин), тобто створити окремий розділ Кримінального кодексу України "Злочини у сфері інформаційної безпеки".

З огляду на необхідність суворого дотримання прав і свобод людини та громадянина під час виконання правоохоронних функцій, безумовного забезпечення конституційних та міжнародних правових засад у цій сфері як головної ознаки демократичної держави викликає занепокоєння неврегульованість ситуації із приведенням норм чинного законодавства України у відповідність до загальносвітових вимог.

Сьогодні насамперед опрацьовуються законодавчі акти, які безпосередньо регулюють основи оперативно-розшукової та контррозвідувальної діяльності.

У 2005 р. Україна підписала Конвенцію про захист осіб стосовно автоматизованої обробки персональних даних та додатковий протокол до неї. Важливість законодавчого врегулювання питань захисту персональних даних обумовлена тим, що незаконне поширення електронної інформації, яка містить персональні дані, вже набуло масового характеру і безпосередньо стосується питання інформаційної безпеки. Тому вдосконалення чинного законодавства в частині захисту персональних даних (Закон України "Про захист персональних даних") є питанням, що потребує нагального вирішення для підвищення рівня стану забезпечення інформаційної безпеки держави.

Висновки

Підсумовуючи викладене, можна окреслити коло загальнодержавних заходів, які сприятимуть підвищенню рівня нормативно-правового забезпечення інформаційної безпеки держави, а саме:

– прискорення ратифікації Верховною Радою України Конвенції про захист осіб стосовно автоматизованої обробки персональних даних;

– внесення доповнення до законів України "Про основи інформаційної безпеки", "Про захист персональних даних", "Про перехоплення телекомунікацій", "Про засоби масової інформації" в частині віднесення до ЗМІ електронних видань, які розміщуються в мережі Інтернет, та встановлення відповідальності власників цих видань за зміст і характер відомостей, що у них містяться;

– посилення кримінальної відповідальності за незаконне збирання, зберігання, поширення інформації про особу, введення кримінальної відповідальності за незабезпечення умов щодо захисту персональних даних в автоматизованих системах;

– запровадження ліцензування господарської діяльності у сфері надання доступу до мережі Інтернет провайдерами таких послуг та утримувачами пунктів колективного доступу до Інтернет з визначенням умов організації цього доступу відповідно до вимог Конвенції про кіберзлочинність;

– відновлення роботи міжвідомчої робочої групи з розроблення Державної програми з протидії комп'ютерній злочинності;

– активізація роботи з приведення чинного законодавства України у відповідність до встановлених в Європі стандартів та норм.

Список використаних джерел

1. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Про інформацію : закон України від 02.02.1992 р. // Голос України. – 1992. – 21 трав.

3. Про Національну програму інформатизації: закон України від 04.02.1998 р. // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181.

4. 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 : указ Президента України // Офіц. вісн. України. – 2001. – № 50. – Ст. 28.

5. Про основи національної безпеки України: закон України від 19.06.2003 р. № 964-IV // Офіц. вісн. України. – № 29. – С. 38. – Ст. 1433.

Стаття надійшла до редакції 12.11.2008 р.