УДК 343.1(477):65.012.8

В. В. МАРКОВ,
кандидат юридичних наук,
начальник факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В СИСТЕМІ МІЖНАРОДНОЇ КООРДИНАЦІЇ

Проаналізовано нормативно-правову базу у сфері боротьби з кіберзлочинністю. Визначено роль та компетенцію підрозділів боротьби з кіберзлочинністю. Розкрито проблеми міжнародного співробітництва правоохоронних органів з протидії кіберзлочинності.

Ключові слова: *інформаційна безпека, нормативно-правова база, світовий досвід, аналіз законодавства, міжнародне співробітництво, кіберзлочинність.*

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень та боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військових сил, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, а це передбачає:

– забезпечення інформаційного суверенітету України;

– удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у даній сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх

посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

У цьому аспекті своєчасним та дієвим (важливим) є акт прийняття Доктрини інформаційної безпеки України (Указ Президента України від 8 липня 2009 р. № 14/2009). Основною метою реалізації положень Доктрини інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету [1]. Доктрина спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду, яка є основою для:

– формування державної політики у сфері інформаційної безпеки України;

– розроблення проектів концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України;

– підготовки пропозицій щодо подальшого системного вдосконалення правового, методичного, науково-технічного і організаційного забезпечення інформаційної безпеки України.

Стратегія національної безпеки України «Україна у світі, що змінюється» (в редакції від 8 червня 2012 р. № 389/2012) відповідно до законодавства визначає загальні принципи, пріоритетні цілі, завдання і механізми захисту життєво важливих інтересів особистості, суспільства та держави від зовнішніх і внутрішніх загроз, у тому числі у сфері забезпечення інформаційної безпеки [2].

Ключовими завданнями політики національної безпеки у сфері забезпечення інформаційної безпеки є:

– стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

– забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

– розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність;

– створення національної системи кібербезпеки.

У стратегії зазначено, що формування гнучкої та ефективної системи публічних інститутів, спроможних адекватно та оперативно реагувати на зміни безпекової ситуації, передбачає здійснення адміністративної реформи держави. Слід зазначити, що питання, пов'язані з інформаційною безпекою, стосуються тільки загроз в інформаційній сфері, а роль правоохоронних органів як суб'єкта забезпечення інформаційної безпеки не висвітлюються.

Варто зауважити, що державні правоохоронні органи в різних країнах світу утворюють спеціалізовані підрозділи для збирання та аналізу «електронних» або «комп'ютерних» доказів. Таку функцію виконують спеціальні лабораторії судової експертизи. Досвід багатьох країн свідчить, що комп'ютерні злочини мають розслідуватися лише тими підрозділами або працівниками правоохоронних органів, які мають спеціальні знання для ведення таких справ та пройшли відповідну підготовку.

Органи внутрішніх справ України відіграють головну роль в аспекті боротьби із злочинністю та тероризмом. Фактично будь-яка інформація в цьому випадку є службовою або секретною, тому її збереження також виступає ключовим елементом діяльності всіх правоохоронних структур, а інформаційна координація правоохоронних структур – це процес управління інформаційними потоками щодо діяльності правоохоронних органів та ОВС України в межах виконуваних ними завдань і функцій у рамках законодавчих повноважень [2].

Одну з найнебезпечніших загроз національній безпеці України в інформаційній сфері становить кіберзлочинність та вирішення проблемних питань міжнародного співробітництва у сфері боротьби з указаним явищем сучасної дійсності.

У системі Міністерства внутрішніх справ (далі – МВС) України основні функції щодо боротьби з кіберзлочинністю покладено на підрозділи боротьби з кіберзлочинністю у складі однойменного Управління. Згідно з Положенням про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України, затвердженого наказом МВС України від 31 травня 2012 р. № 494 [3], основним завданням управління є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж

електрозв'язку, а також іншим злочинам та правопорушенням, учиненим із їх використанням.

При цьому слід зазначити, що в Україні першим та найбільш практично корисним за останні роки кроком у напрямку міжнародного співробітництва у сфері боротьби з кіберзлочинністю була ратифікація Конвенції Ради Європи про кіберзлочинність, при цьому відповідний Закон України «Про ратифікацію Конвенції про кіберзлочинність» набрав чинності 1 липня 2006 р. [4]. На виконання доручення Президента України від 3 грудня 2010 р. № 02/78475-01 МВС України вжито заходів з реалізації положень ст. 35 Конвенції про кіберзлочинність щодо створення контактного пункту з реагування на кіберзлочини (національний контактний пункт), який цілодобово впродовж тижня здійснює свою діяльність у структурі Управління боротьби з кіберзлочинністю МВС України з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, чи з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

Міжнародна мережа таких пунктів реагування охоплює понад 60 країн світу та з огляду на практичну значущість є найбільш дієвим засобом боротьби з кіберзлочинністю, оскільки більшість злочинів даної спрямованості має саме транснаціональний характер і боротьба з ними потребує безпосереднього та оперативного контакту правоохоронних органів різних країн.

Незважаючи на вищезазначене, в діяльності міжнародної мережі національних контактних пунктів є питання, що потребують негайного вирішення, наприклад внесення змін до діючого законодавства щодо порядку та підстав виконання запитів, отриманих від правоохоронних органів країн, у зв'язку з ратифікацією Конвенції про кіберзлочинність та взятих ними зобов'язань та інших проблемних питань, які неодноразово доповідались Управлінням боротьби з кіберзлочинністю МВС України.

Отже, з вищезазначеного можна зробити такі **висновки:**

– інформаційна безпека набуває дедалі більшої актуальності в системі національної безпеки України;

– інформаційна безпека є однією із ключових у системі функціонування правоохоронних органів;

– актуальними є питання, пов'язані з транснаціональними комп'ютерними злочинами, та співпраця з іншими країнами безпосередньо на рівні підрозділів, особливо в контексті мережі міжнародних контактних пунктів із реагування на кіберзлочини.

Список використаної літератури

3. Доктрина інформаційної безпеки України [Електронний ресурс] : затв. указом Президента України від 8 лип. 2009 р. № 14/2009. – Режим доступу: http://zakon.rada.gov.ua/laws/show/514/2009.

4. Стратегія національної безпеки України «Україна у світі, що змінюється» [Електронний ресурс] : затв. указом Президента України від 12 лют. 2007 р. № 105. – Режим доступу: http://zakon.rada.gov.ua/laws/show/389/2012. – У ред. від 8 черв. 2012 р. № 389/2012.

5. Положення про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України [Електронний ресурс] : затв. наказом Міністерства внутрішніх справ України від 31 трав. 2012 р. № 494. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/MVS416.html.

6. Конвенція про кіберзлочинність [Електронний ресурс] : ратифік. Верховною Радою України 7 верес. 2005 р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

Надійшла до редколегії 14.03.2013

МАРКОВ В. В. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ В СИСТЕМЕ МЕЖДУНАРОДНОЙ КООРДИНАЦИИ

Проанализирована нормативно-правовая база в сфере борьбы с киберпреступлениями. Определена роль и компетенция подразделений по борьбе с киберпреступлениями. Раскрыты проблемы международного сотрудничества правоохранительных органов по противодействию киберпреступлениям.

Ключевые слова: *информационная безопасность, нормативно-правовая база, международный опыт, анализ законодательства, международное сотрудничество, киберпреступность.*

MARKOV V. ACTUAL PROBLEMS OF INFORMATIONAL SECURITY IN UKRAINE AND INTERNATIONAL COORDINATION

Normative and legal base in the sphere of cybercrime counteraction is analyzed. The role and jurisdiction of the anti-cybercrime departments are defined. The problems of international cooperation of law enforcement bodies in the field of cybercrime counteraction are considered.

Keywords: *informational security, normative and legal base, international experience, legal analysis, international cooperation, cybercrime.*