УДК 351.76.1

ЧЕХОВСЬКА Марія Миколаївна
НИЧИТАЙЛО Ірина Михайлівна

БОРОТЬБА З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: НОРМАТИВНО-ПРАВОВИЙ ТА ОРГАНІЗАЦІЙНИЙ АСПЕКТИ

Постановка проблеми. Глобальна інформатизація суспільства створила передумови для появи таких нетрадиційних загроз національній безпеці, як загрози інформаційній сфері. Зокрема, Закон України "Про основи національної безпеки" від 19 червня 2003 року № 964-IV серед реальних та потенційних загроз національній безпеці визначає комп'ютерну злочинність та комп'ютерний тероризм. Зазначимо, що за даними МВС України, протягом 2012 року було зареєстровано 2011 злочинів, вчинених із використанням комп'ютерних технологій, в той час як лише у першому півріччі 2013 року таких злочинів зареєстровано вже 1878 [1]. Таким чином, стрімкий розвиток технологій, їх активне застосування, зокрема й злочинними угрупованнями, зумовлюють *актуальність досліджень* щодо функціонування нормативно-правових та організаційних важелів у механізмі протидії комп'ютерній злочинності.

Аналіз останніх досліджень і публікацій. Комплексному вивченню проблемних питань національної безпеки присвячені роботи В.Горбуліна, А.Качинського, Г.Новицького [2-4]. Дослідження у сфері протидії комп'ютерній злочинності проводилися В.Бутузовим, В.Голубєвим, М.Гуцалюком тощо [5-7]. Водночас питанням співвідношення комп'ютерної злочинності та національної безпеки науковці приділяли недостатньо уваги.

З огляду на зазначене **метою статті** є дослідження нормативно-правових та організаційних складових у системі протидії комп'ютерній злочинності як загрози національній безпеці України.

Виклад основного матеріалу. Відповідно до чинного законодавства сутність сфери національної безпеки полягає у "захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам", зокрема у сфері інформацій-

ної безпеки [8]. Серед загроз національним інтересам і національній безпеці у цій сфері статтею 7 Закону України "Про основи національної безпеки" визначаються комп'ютерна злочинність та комп'ютерний тероризм.

На існуванні такого негативного чинника, як кіберзлочинність, що загрожує безпековому середовищу України, наголошується у Стратегії національної безпеки України "Україна у світі, що змінюється". Не виокремлюючи серед проблем, що загрожують національній безпеці у внутрішньому безпековому середовищі, безпосередньо загрози інформаційній безпеці, у Стратегії наголошується на збереженні невідповідності вітчизняного сектору безпеки й оборони завданням захисту національних інтересів, що зокрема характеризується нездатністю нашої країни протистояти сучасним викликам національній безпеці, "пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед, кіберзагрозам" [9].

Водночас серед ключових завдань політики національної безпеки у внутрішній сфері йдеться про напрями забезпечення інформаційної безпеки, зокрема шляхом створення національної системи кібербезпеки та імплементації вимог Конвенції про кіберзлочинність, яка, зокрема, регулює боротьбу із цим видом правопорушень на регіональному рівні.

Зважаючи на результати комплексного аналізу викликів і загроз національній безпеці, на виконання Рішення Ради національної безпеки і оборони України "Про виклики та загрози національній безпеці України у 2011 році" в інформаційній сфері уповноваженим органом було вирішено створити Єдину загальнодержавну систему протидії кіберзлочинності, розробити та затвердити "перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак" [10].

Ще одним нормативно-правовим актом, що визначає перспективні напрями реалізації державної політики, зокрема у сфері національної безпеки, є Закон України "Про засади внутрішньої і зовнішньої політики" від 1 липня 2010 року № 2411-VI. Однак, на відміну від інших конституційно-правових засад забезпечення національної безпеки України, цей Закон не конкретизує напрями внутрішньої політики ані в інформаційній сфері, ані шляхи реалізації заходів із забезпечення кібербезпеки у сфері національної безпеки і оборони.

Зважаючи на той факт, що на сьогодні складовою практично усіх сфер національної безпеки є інформаційна безпека, стратегічне значення має Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009. У Доктрині серед реальних та потенційних загроз інформаційній безпеці України у зовнішньополітичній сфері наголошується на проявах комп'ютерної злочинності та комп'ютерного тероризму як факторах негативного впливу на функціонування національних інформаційно-комунікаційних систем [11].

Крім того, слід зупинитися на законодавчо затверджених "Основних

засадах розвитку інформаційного суспільства в Україні на 2007-2015 роки", в яких розвиток інформаційного суспільства, впровадження сучасних інформаційно-комунікаційних технологій не лише в усі сфери суспільного життя, а й у діяльність органів державної влади та місцевого самоврядування, визначаються одними із пріоритетних напрямів державної політики. Зазначимо, що серед основних стратегічних цілей розвитку інформаційного суспільства в Україні визначено покращання стану інформаційної безпеки саме в умовах використання сучасних інформаційно-комунікаційних технологій. Актуальність цього напряму діяльності пов'язана зокрема із фактом залежності державної безпеки країни від стану захищеності інформаційної інфраструктури. Негативно впливати на останню, застосовуючи можливості інформаційного простору, можуть практично всі, хто має вихід або на глобальну, або на корпоративну комп'ютерну мережу.

Наголосимо також, що стрімкий розвиток інформаційної сфери є частиною не лише міжнародного співробітництва, але й суперництва. Адже не можна заперечувати той факт, що країни з високорозвиненою інформаційною інфраструктурою мають змогу формувати напрями діяльності інформаційних структур в інших країнах, впливати на їх подальший розвиток.

Саме на етапі розвитку інформаційно-комунікаційних технологій, їх поширення на всіх ланках суспільної та економічної діяльності й виникають загрози національній безпеці країни.

Відповідно до зазначеного, спираючись на міжнародний досвід у цій сфері, виникає необхідність забезпечення захисту так званих критичних елементів інформаційної інфраструктури держави. Тут, на нашу думку, необхідною є не лише констатація наявності таких елементів, але й чітке їх визначення відповідно до вітчизняної дійсності.

Зважаючи на євроінтеграційні спрямування нашої країни, зауважимо на активну співпрацю державних органів влади із Організацією Північноатлантичного договору (НАТО) у процесі забезпечення кібербезпеки та боротьби із кіберзлочинністю. Зокрема, у 2010 році Україна першою серед країн-партнерів започаткувала співробітництво з НАТО у сфері кібернетичного захисту та провела чотири засідання Консультацій експертів Робочої підгрупи Україна-НАТО з питань кібернетичного захисту під егідою Спільної робочої групи Україна-НАТО з питань воєнної реформи. 27-28 вересня 2012 року у Києві в Дипломатичній академії України при МЗС України відбулася міжнародна конференція "НАТО і Партнери: Нові виклики безпеці", присвячена обговоренню широкого спектру питань енергетичної безпеки, боротьби проти тероризму та кібернетичного захисту.

Програмним документом, що регламентує спільну діяльність, є Указ Президента України від 5 липня 2013 року № 371/2013 про затвердження Річної національної програми співробітництва Україна-НАТО на 2013 рік. Зокрема, Міністерству оборони України у сфері удосконалення системи військового управління та

зв'язку наголошується на необхідності розвивати власні спроможності щодо кібероборони та інформаційних операцій [12].

Відповідно до Програми співробітництва перед Службою безпеки України постають такі завдання, як ужити заходів щодо становлення національної системи кібернетичної безпеки; провести з державами-членами НАТО консультації з питань захисту національної інформаційної інфраструктури від кібернетичних атак, протидії кіберзлочинності та використанню кіберпростору з терористичною метою; здійснити виконання мети партнерства "Кіберзахист" у межах участі Служби безпеки України у процесі планування та оцінки сил.

Пріоритетними завданнями спільної роботи Україна-НАТО на поточний рік, зокрема, є: розширення можливостей кіберзахисту шляхом активізації співробітництва з міжнародними організаціями у цій сфері, зокрема Агентством НАТО з комунікацій та інформації, Підрозділом з реагування на комп'ютерні інциденти НАТО (NCIRC), а також у межах Програми НАТО "Наука заради миру та безпеки"; забезпечення взаємодії з відповідними органами іноземних держав і міжнародними організаціями в режимі реального часу через команду реагування на комп'ютерні надзвичайні події України CERT-UA (Центр реагування на комп'ютерні інциденти). Передбачається, що виконання цих завдань здійснюватиметься шляхом консультацій експертів Україна-НАТО у межах робочої підгрупи із питань кібернетичного захисту; сприяння розвитку співробітництва з питань кібернетичного захисту між органами державної влади та відповідними компетентними органами Альянсу, а також на двосторонній основі з державами-членами НАТО (США, Сполучене Королівство Великої Британії та Північної Ірландії, Королівство Нідерланди та інші); опрацювання питань щодо можливості залучення України до спільних кібернетичних навчань держав-членів Альянсу ("Eurocybex" та інші); опрацювання питань щодо можливості налагодження співробітництва України з Агентством НАТО з комунікацій та інформації (NCI); продовження взаємодії з відповідними органами іноземних держав і міжнародними організаціями в режимі реального часу через команду реагування на комп'ютерні надзвичайні події України CERT-UA.

Основним інструментом у боротьбі із комп'ютерною злочинністю є застосування положень Кримінального кодексу України, зокрема статей 361-363 Розділу XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку".

Система органів державного управління національною безпекою, зокрема й в інформаційній сфері, визначена у Законі України "Про основи національної безпеки України". Відповідно до ст. 4 Закону до складу такого механізму (системи) входять такі суб'єкти забезпечення національної безпеки, як Президент України; Верховна Рада України; Кабінет Міністрів України; Національний банк України; міністерства, інші центральні органи виконавчої влади. Служ-

ба безпеки України та Служба зовнішньої розвідки України у межах своїх повноважень; місцеві державні адміністрації та органи місцевого самоврядування; Воєнна організація держави; правоохоронні органи; суди загальної юрисдикції; прокуратура України; громадяни України.

Заходи із протидії зовнішнім та внутрішнім інформаційним загрозам в Україні належать до компетенції Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, а також Міністерства внутрішніх справ України. До здійснення цієї діяльності залучаються також Міністерство оборони України та інші центральні органи виконавчої влади.

Зрозуміло, що виконання основних завдань із протидії злочинам в інформаційній сфері покладено на Службу безпеки України та Міністерство внутрішніх справ України.

Так, у структурі СБ України діяльність у цій сфері здійснює Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

У структурі МВС України функціонує окремий підрозділ боротьби з комп'ютерними злочинами – Управління боротьби з кіберзлочинністю. Основним завданням Управління боротьби з кіберзлочинністю МВС України є організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються із використанням інформаційних технологій та телекомунікаційних мереж (у сфері інформаційно-телекомунікаційних технологій, у сфері електронних платежів і господарської діяльності, зокрема, порушення прав інтелектуальної власності та заняття гральним бізнесом, злочини проти інформаційної безпеки, зокрема незаконні дії із спеціальними технічними засобами негласного отримання інформації), а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень.

Необхідно зазначити, що на виконання статті 35 Конвенції про кіберзлочинність у МВС України функціонує Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені комп'ютерні злочини. У складі Державної служби спеціального зв'язку та захисту інформації України утворена і функціонує Команда реагування на комп'ютерні надзвичайні події України, яка пройшла акредитацію у міжнародних інституціях.

Висновки. Отже, зазначимо, що на сьогодні в Україні сформована нормативно-правова база, яка регламентує діяльність із протидії комп'ютерній злочинності відповідними суб'єктами забезпечення національної безпеки в інформаційній сфері. Діяльність останніх також знаходить підтримку з боку міжнародних безпекових організацій, зокрема НАТО. Однак, слід наголосити на тому, що розвиток нормотворення у цій сфері гальмується, не зважаючи на факти стрімкого поширення та осучаснення комп'ютерної злочинності. Серед перспектив подальших досліджень у цьому напрямі можна виокремити необхідність обґрунтування змін та доповнень у вітчизняне законодавство із метою його адаптації до сучасних умов, а також у відповідності до засад європейського законодавства.

Список використаних джерел

1. В Україні набирає обертів кіберзлочинність [Електронний ресурс]. – Режим доступу : http://newsradio.com.ua/2013_08_28/V-Ukra-n-nabira-obert-v-k-berzlochinn-st/.

2. Горбулін В.П. Національна безпека: український вимір / В.П.Горбулін, О.В.Литвиненко. – К. : ПІІ "Інтертехнологія", 2008. – 104 с.

3. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень : моногр. / А.Б.Качинський. – К. : НІСД, 2013. – 104 с.

4. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України : моногр. / Г.В.Новицький. – К. : Інтертехнологія, 2008. – 496 с.

5. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : моногр. / В.М.Бутузов. – К. : КИТ, 2010. – 408 с.

6. Голубєв В.О. Розслідування комп'ютерних злочинів : моногр. / В.О.Голубєв. – Запоріжжя : Гуманітарний університет "ІДМУ", 2003. – 296 с.

7. Гуцалюк М. Протидія комп'ютерній злочинності [Електронний ресурс] / М.Гуцалюк. – Режим доступу : http://www.pravo.vuzlib.org/book_z726_page_24.html.

8. Закон України "Про основи національної безпеки" від 19 червня 2003 року № 964-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/964-15.

9. Стратегія національної безпеки України "Україна у світі, що змінюється", затверджена Указом Президента України від 12 лютого 2007 року № 105 (в редакції Указу Президента України від 8 червня 2012 року № 389/2012) [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/105/2007.

10. Рішення Ради національної безпеки і оборони України "Про виклики та загрози національній безпеці України у 2011 році" [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/.

11. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/n0008525-10.

12. Указ Президента України від 5 липня 2013 року № 371/2013 "Про затвердження Річної національної програми співробітництва Україна-НАТО на 2013 рік" [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/371/2013.

Аннотация: В статье рассматривается украинское законодательство через призму противодействия киберпреступности как одной из угроз национальной безопасности. Очерчиваются основные субъекты обеспечения национальной безопасности, функцией которых является выполнение основных заданий по противодействию преступлениям в информационной сфере.

Ключевые слова: нормативно-правовая база, компьютерная преступность, национальная безопасность, национальные интересы.

Abstract: The article considers the Ukrainian legislation in the framework of counteracting cyber-crime as one of threats to national security. The basic subjects of ensuring national security, the function of which is implementation of basic tasks on counteracting the crimes in information sphere are outlined as well.

Key words: regulatory framework, cyber-crime, national security, national interests.