УДК 343.98
DOI https://doi.org/10.15421/392023

Маланчук П. М.,
кандидат юридичних наук,
доцент кафедри правосуддя
Сумського національного аграрного університету

ПОРІВНЯННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ ТА ЗАРУБІЖНИХ КРАЇНАХ

COMPARISON OF CYBER CRIME IN UKRAINE AND FOREIGN COUNTRIES

Розглянуто та досліджено проблеми сучасної нормативної бази по боротьбі з кіберзлочинності як складової частини державної політики в галузі боротьби зі злочинами у сфері інформаційних, телекомунікаційних технологій і засобів державного регулювання та контролю над нею. Широке використання сучасних інформаційних технологій у державних та недержавних структурах, а також у суспільстві загалом робить вирішення проблем інформаційної безпеки одним з основних питань. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Показано, що сформована у світі ситуація з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами та побудову моделі, спрямованої на забезпечення кібербезпеки країни. У статті проведено дослідження у сфері боротьби з кіберзлочинами в зарубіжних країнах, виділено позитивні сторони, які було б доцільно запровадити в Україні. Також проаналізовано проблеми, що виникають в області боротьби з комп'ютерними злочинами в Україні, і надано пропозиції шляхів їх вирішення. Для підвищення ефективності боротьби з кіберзлочинністю Україна досить давно почала відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Незважаючи на це, Україна постійно стає жертвою кібератак, у зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності. Саме тому питання вивчення та запозичення міжнародного досвіду провідних країн світу у сфері державної діяльності щодо правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності є недослідженим та потребує вивчення. Як свідчать результати досліджень та численних суспільних опитувань, питання кіберзлочинності непокоїть не тільки державу загалом, а й кожного окремо взятого її мешканця. У цьому сенсі вивчення досвіду зарубіжних країн, які мають достатній досвід боротьби з кіберзлочинами, було б доволі актуальним.

Ключові слова: *інформація, інформаційний злочин, кіберзлочинність, кібербезпека, кіберзагроза.*

Analysed the problems of the modern cybercrime regulatory framework as an integral part of the state crime control policy in the sphere of information, telecommunication technologies and the means of state regulation and control are considered and investigated. The widespread using of modern information technologies in state and non-governmental structures, as well as in the society as a whole, puts the solution of information security problems among the main ones. In addition to the harm from possible unauthorized access to, modification or destruction of information, informatization can become a serious threat to national security and human rights. The situation in the world is shown to require continuous improvement of cybercrime methods and the creation of a model aimed at ensuring the country's cyber security. The article conducted research of combating cybercrime in foreign countries, identified the positive aspects that would be appropriate to introduce in Ukraine. The problems that arise in the field of combating computer crimes in Ukraine are analyzed and suggestions are given for ways to solve them. In order to increase the effectiveness of the fight against cybercrime, Ukraine has long since begun the necessary work necessary to create its own cyber security strategy. Despite this, Ukraine is constantly falling victim to cyberattacks, which makes the issue of counteracting cybercrime particularly relevant. That is why the issue of studying and drawing on the international experience of the leading countries in the sphere of state activity concerning the legal mechanisms of regulation of protection of information in modern conditions, counteraction to cybercrime is unexplored and needs to be studied. According to research and numerous public polls, the issue of cybercrime is of concern not only to the state as a whole, but also to its individual inhabitants. In this sense, it would be relevant to study the experience of foreign countries with sufficient experience in combating cybercrime.

Key words: *information, information crime, cybercrime, cyber security, cyber threat.*

Серед сучасних тенденцій розвитку суспільства вартозазначитиглобальнуінформатизаціюпрактично всіх сфер життєдіяльності людини. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Для підвищення ефективності боротьби з кіберзлочинністю Україна досить давно почала відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Верховною Радою України було зроблено спробу врегулювати відносини, що виникають у кіберпросторі, а саме ухвалено Закон України «Про основні засади забезпечення кібербезпеки в Україні». Незважаючи на ці кроки, Україна постійно стає жертвою кібератак, у зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності. Саме тому питання вивчення та запозичення міжнародного досвіду провідних країн світу у сфері державної діяльності щодо правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності є недослідженим та потребує вивчення.

Окремі аспекти розвитку та становлення кібербезпеки, питання здійснення протидії кіберзлочинності розглядались провідними вітчизняними науковцями: М.О. Будаковим, В.М. Бутузовим, М.М. Галамбою, Р.А. Калюжним, В.В. Коваленко, Б.А. Кормичем, Ю.Є. Максименко, А.І. Марущаком та іншими.

Метою статті є аналіз та дослідження проблемних питань протидії кіберзлочинності в Україні та в зарубіжних країнах та на цій основі надання пропозицій щодо їх вирішення.

Ю.Є. Максименко зазначає, що становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. З одного боку, пришвидшилася передача інформації великого обсягу, прискорились її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо. Перетворення суспільства в інформаційне змінив статус інформації. Нині вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою [1, с. 1].

Кіберзлочинність – одне з п'яти найпоширеніших економічних злочинів в Україні. Кіберзлочинність – це п'ятий за значимістю вид економічної злочинності в Україні, слідом за незаконним привласненням майна, хабарництвом і корупцією, практикою підриву конкуренції і маніпуляцією з фінансовою звітністю. За результатами опитування, на кіберзлочинність припадає 23% випадків шахрайства у світі, про які повідомили учасники опитування, і 17% − в Україні [8]. До основних проблем виявлення, розкриття та розслідування «транскордонних» злочинів із використанням глобальної мережі Інтернет варто зарахувати територіальну розподіленість слідів злочину та зберігання їх протягом невеликого проміжку часу. Правоохоронцям іноді важко окреслити території, де здійснюються сучасні злочини. У злочинців у мережі Інтернет великий ступінь анонімності, а інформація, що зберігається в комп'ютерних системах, має короткостроковий характер.

У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки [2]. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. Звіт був складений спеціально для того, щоб допомогти урядам та організаціям зрозуміти, наскільки вони кібернетично захищені порівняно з іншими країнами.

Нині в багатьох зарубіжних країнах налагоджена система співробітництва та зумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та чинної стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на ключові позиції. Для України така тенденція є загалом позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють у зазначеному напряму не перший рік.

Сполучені Штати Америки стали першою країною, що прийняли відповідний закон та створили Національну стратегію безпеки в кіберпросторі. Причиною написання цього документа стала терористична атака 11 вересня 2001 р. Стратегія була частиною більш загальної Стратегії забезпечення національної безпеки (National Strategy for Homeland Security). Крім того, за оцінками фахівців, саме в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд дол., тому питання боротьби з кіберзлочинністю для цієї країни є надзвичайно актуальним [3].

Порядіз США активна боротьба з кіберзлочинністю проводиться в країнах Європейського Союзу. В ЄС створений необхідний нормативно-правовий фундамент із питань захисту кіберпростору. Стратегія кібербезпеки ЄС була прийнята в 2013 р. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика.

Разом із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

– свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

– застосування законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому суспільстві: від звичайних громадян до цілих держав;

– розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [4].

Незважаючи на прийняття такого важливого стратегічного документа, все ж існують численні загрози. Серед основних недоліків системи кібербезпеки ЄС можна виділити:

– по-перше, відсутність єдиної європейської системи реагування на кібератаки;

– по-друге, відмінність стандартів у сфері кібербезпеки в різних країнах;

– по-третє, відсутність чіткого уніфікованого категоріального апарату.

Проаналізувавши досвід роботи поліції багатьох країн світу у сфері протидії кіберзлочинності, варто зазначити, що цей напрям забезпечується такими основними шляхами, як покладення додаткових функцій на наявні підрозділи поліції або створення спеціальних підрозділів. Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах,

Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін.

Серед основних функцій цих підрозділів виділяють:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових та розвідувальних заходів із метою фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації;

– навчання працівників поліції.

Деякі зі спеціальних підрозділів поліції у сфері протидії кіберзлочинності (або їх ще називають спеціальними підрозділами щодо протидії злочинам із використанням інформаційних технологій) виконують ще й додаткові функції:

– розкриття кіберзлочинів;

– профілактики та нагляду за телекомунікаційними послугами;

– експертного дослідження доказів на електронних носіях;

– створення відповідної бази даних щодо злочинів у сфері кіберпростору та постійного її оновлення;

– надання послуг банкам щодо захисту персональної інформації клієнтів тощо.

Наприклад, в Індії підрозділи з розслідування кіберзлочинів для їх розкриття можуть залучати професійних хакерів. Варто зазначити, що під час розслідування кіберзлочинів значну увагу приділяють допомозі постраждалому у відновленні пошкодженої або втраченої інформації, вживають всі необхідні заходи для збереження доказів у справі [5, с. 193].

Зокрема, одним із важливих напрямків діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідуванням яких займається підрозділ Королівської канадської кінної поліції (федеральної поліції, КККП) із боротьби з комп'ютерною злочинністю, спираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами.

Діяльність підрозділу націлена на розслідування та розкриття злочинів, пов'язаних із комп'ютерами і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектора, дає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами. Враховуючи, що інформаційна система дозволяє передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2500 точок доступу, до яких входять близько 1285 федеральних і провінційних поліцейських відділень. 1180 підрозділів спеціалізованих відділів КККП підключені до ліній системи [6].

Нині в багатьох зарубіжних країнах налагоджена система співробітництва та зумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки:

США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинність на ключові позиції. Для України така тенденція є загалом позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють у зазначеному напрямі не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним.

Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн [7] можна виділити об'єднуючі ключові позиції:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дасть змогу приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі в міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– доказ необхідності нової програми освіти, в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці.

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»). У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак [9].

При цьому протягом останніх років кількість розкритих злочинів у сфері ІТ-технологій в Україні майже не змінилася, хоча у сфері комп'ютерних та інтернет-технологій кількість розкритих злочинів збільшилася в кілька разів. Така ситуація корелюється з перерахованими вище проблемами та свідчить про те, що збільшення рівня захищеності інформації в нашій країні потребує підтримки і розвитку.

В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України. У кожному із зазначених органів діють відповідні підрозділи.

Хоча Закон України «Про основні засади забезпечення кібербезпеки України» і дав великий поштовх для розвитку національного законодавства з питань забезпечення кібербезпеки, його все ж не можна назвати ідеальним. У процесі аналізу норм Закону України «Про основні засади забезпечення кібербезпеки України» було визначено такі основні проблеми: законом не визначено єдиний орган, основною функцією якого мало б стати оперативне керування над всіма суб'єктами забезпечення кібербезпеки, крім того, проблемою є загроза тотального шпигунства. За прийнятим законом, Службі безпеки України надається надмірне право проводити таємні перевірки щодо кібербезпеки критичних об'єктів. По суті, СБУ надається повноваження щодо проведення хакерських атак на приватний бізнес.

Вдосконалення правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу та врахування кращого міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження в європейське та світове правове поле.

ЛІТЕРАТУРА:

1. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 20 с.
2. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report. *Портал : An Intel Company*. URL: http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx (дата звернення 28.06.2013).
3. Youtsen M. Research on European Juvenile Delinquency. *HEUNI Publication Series.* 1987. № 7. С. 57−62.
4. . EU International Cyberspace Policy. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm.
5. Сень Р.Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С. 192–194.
6. Варунц Л.Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. … канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.
7. Государственные стратегии кибербезопасности. *Портал : Security Lab*. URL: http://www.securitylab.ru/analytics/429498.php.
8. Всесвітній огляд економічних злочинів. URL: https://www.pwc.com/ua/uk/Україна.
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.