РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 341+342

КІБЕРБЕЗПЕКА В УКРАЇНІ: НАЦІОНАЛЬНА СТРАТЕГІЯ ТА МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

CYBER SECURITY IN UKRAINE: NATIONAL STRATEGY AND INTERNATIONAL COOPERATION

Дешко Л.М.,
доктор юридичних наук, доцент,
завідувач кафедри міжнародного публічного права
Київського національного торговельно-економічного університету

Бондарєва К.Д.,
магістр кафедри міжнародного публічного права
Київського національного торгово-економічного університету

У статті встановлено особливості правового регулювання відносин у сфері кібербезпеки, процесу впровадження національної стратегії з кібербезпеки, а також міжнародного співробітництва України у цій сфері. Охарактеризовано організаційно-правовий механізм співпраці у сфері кібербезпеки в Україні. Проаналізовано нормативно-правовий та організаційно-правовий механізми міжнародного співробітництва у цій сфері.
Ключові слова: кібербезпека, стратегія кібербезпеки, віртуальний простір, інтернет, інформаційна безпека, кіберзлочини, кіберзлочинність, міжнародне співробітництво, міжнародне право.

В статье определены особенности правового регулирования отношений в сфере кибербезопасности, процесса внедрения национальной стратегии кибербезопасности, а также международного сотрудничества Украины в данной сфере. Охарактеризован организационно-правовой механизм сотрудничества в сфере кибербезопасности в Украине. Проанализированы нормативно-правовой и организационно-правовой механизмы международного сотрудничества в этой сфере.
Ключевые слова: кибербезопасность, стратегия кибербезопасности, виртуальное пространство, интернет, информационная безопасность, киберпреступления, киберпреступность, международное сотрудничество, международное право.

The article defines the legal regulation peculiarities of relations in the field of cybersecurity, the process of implementing the national strategy of cybersecurity, as well as international cooperation of Ukraine in this field. The organizational and legal mechanism of cooperation in the field of cybersecurity in Ukraine is described. The article analyzes regulatory and organizational mechanisms of international cooperation in the field of cybersecurity.
Key words: cybersecurity, cybersecurity strategy, cyberspace, internet, information security, cybercrimes, international cooperation, international law.

Сьогодення характеризується низкою проблем глобального характеру, вирішення яких зусиллями однієї або навіть декількох держав є неможливим. Це зумовлює активну співпрацю держав у рамках спеціалізованих міжнародних установ [1; 2]. Така співпраця не лише створює умови для розв'язання проблем у певних сферах, а й забезпечує однорідність, стабільність та узгодженість кооперації держав та інших міжнародних акторів у цій сфері. Критерієм виміру успіху міжнародного співробітництва у цих сферах є не лише існування ефективного організаційно-правового та нормативно-правового механізмів співпраці держав, результатом яких є вироблення певних міжнародних стандартів, а й імплементація норм міжнародного права у національне право [3; 4].

Стрімкий розвиток технологій Інтернету зумовлює появу та розвиток нових видів кіберзлочинів, які тягнуть за собою серйозні та незворотні наслідки. Величезний технічний потенціал та безмежні можливості у віртуальному просторі все частіше використовуються кіберзлочинцями для шахрайства, тероризму та для реалізації політичної мети. Тому так важливо на сучасному етапі встановити систему національного кіберзахисту та співпрацювати з іншими державами, міжнародними організаціями у цій сфері.

Питань правового регулювання відносин у сфері кібербезпеки торкалися у своїх дослідженнях вітчизняні та закордонні автори. Водночас із 2016 року правове регулювання цих відносин зазнало змін.

З огляду на це дослідження правового регулювання відносин у сфері кібербезпеки є актуальним та теоретично і практично вчасним.

Мета статті – встановити особливості правового регулювання відносин у сфері кібербезпеки в Україні, процесу впровадження національної стратегії з кібербезпеки та міжнародного співробітництва України у цій сфері.

Відповідно до Кримінального кодексу України до інформаційних злочинів (кіберзлочинів) належать такі: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення для використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [5].

У відповідь на масштабні кібератаки останніх років у 2016 році в Україні було прийнято Національну стратегію

кібербезпеки. Створення Національного координаційного центру з кібербезпеки та оновлення законодавства в галузі кіберзлочинності відповідно до вимог Будапештської конвенції є двома основними кроками у підвищенні кіберстійкості країни. Ці заходи супроводжуються налагодженням співпраці з міжнародними партнерами в кіберсфері з питань кіберзлочинності та кіберзахисту.

Збільшення оцифрування послуг та дуже активне використання Інтернету призвело до еволюції кіберпростору, що також викликало значні проблеми для безпеки урядів у всьому світі щодо злочинів, вчинених за допомогою комп'ютерних систем.

В Україні це було продемонстровано кібератаками на енергетичні компанії у грудні 2015 р., нападами на основні українські телеканали в день місцевих виборів у 2017 р. 27 червня 2017 року сталась масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80% підприємств в Україні, а також перекинулась на підприємства за кордоном нашої держави. Зловмисники викрадали інформацію з підприємств та відкривали доступ до їх комп'ютерних мереж.

Заступник голови адміністрації Президента України Дмитро Шимків (колишній директор представництва фірми Microsoft в Україні) заявив, що внаслідок атаки хробаком NotPetya було виведено з ладу близько 10% персональних комп'ютерів в Україні (особистих, у державних та недержавних установах і підприємствах). Усунення наслідків атаки вірусом-винищувачем NotPetya потребувало істотних зусиль та часу. Так, наприклад, компанія Reckitt Benckiser заявила, що частина комп'ютерних систем відновить свою нормальну роботу лише у серпні 2017 року [6]. Концерн Maersk оцінив втрати компанії, особливо підрозділів Maersk Line, Damco та APM Terminals, у 200–300 млн доларів. Технічний персонал був змушений протягом 10 днів заново встановлювати і налаштовувати все програмне забезпечення на 4 000 серверів, 45 000 робочих станцій. Робітники були змушені вручну опрацьовувати інформацію про виробничі процеси. У вересні 2017 року американська логістична та поштова компанія FedEx оприлюднила оцінку збитків у своєму дочірньому підприємстві у Нідерландах TNT Express. Так, через порушення нормальних робочих процесів підприємство оцінює свої збитки на рівні до 300 млн доларів за перше півріччя 2017 року. Внаслідок цієї проблеми американська фармацевтична компанія Merck заявила про тимчасову зупинку виробництва вакцини проти вірусу папіломи людини [7].

На думку експертів з міжнародного права Майкла Шмітта та Джефрі Білера, тотальний характер поширення вірусу та свідомий вибір цивільних об'єктів для початку атаки свідчать про те, що організатори атаки порушили міжнародне право звичаїв військового конфлікту, тобто такий вчинок може вважатись воєнним злочином. Оскільки від атаки постраждали треті країни, її організатори ще й порушили міжнародні норми стосовно нейтральності країн [7].

Ці інциденти відповідають таким загальним тенденціям, які Україна спостерігає останнім часом:

– посилене використання атак Distributed Denial of Service (напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена);

– вразливість так званого нульового дня, використовуваного для проникнення та виведення з ладу важливих інфраструктур.

Аналіз ситуації також вказує на цільові напади на дипломатів, правоохоронні органи, державні підприємства, засоби масової інформації, політиків та громадських діячів, а також на дезінформаційні кампанії через Інтернет для впливу на людей заради лобіювання власних інтересів. Вплив цих нападів може бути дуже істотним, оскільки пошкодження критичних інформаційних інфраструктур та перешкоджання ефективному функціонуванню національних органів влади може призвести до жахливих наслідків [8]. Також не слід забувати про кібератаки, ініційовані урядами інших держав. Інформаційно-психологічна війна спрямована на дискредитацію державної влади та сприяє дестабілізації соціально-політичної ситуації.

У відповідь на ці виклики Указом Президента Україна прийняла свою національну стратегію кібербезпеки від 15 березня 2016 року. Стратегія також включає річний План дій для її реалізації та має загальну мету створити умови, які б забезпечили відповідні умови для кіберпростору та його використання в інтересах осіб, суспільства та уряду [9]. Увага Стратегії зосереджується на трьох основних завданнях:

1) розвиток національної системи кібербезпеки;

2) сприяння новим можливостям в секторі безпеки та оборони;

3) забезпечення кібербезпекою критичних інформаційних інфраструктур та державних інформаційних ресурсів.

Національна система кібербезпеки, запроваджена Стратегією, забезпечує співпрацю між усіма державними установами, місцевими органами влади, військовими підрозділами, правоохоронними органами, науково-дослідними та навчальними закладами, цивільними групами, підприємствами та організаціями незалежно від форм власності або осіб, що є власниками критичної інформаційної інфраструктури [10]. У 2015 році був створений Департамент кіберполіції Національної поліції України – міжрегіональний територіальний орган Національної поліції України, який забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції. Завданням Департаменту кіберполіції є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [11]. Департамент також сприяє іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень [12]. Щорічно кількість виявлених кіберзлочинів завдяки Департаменту збільшується в середньому на 2 500. У 2017 році працівники органу супроводжували близько 7 тис. кримінальних проваджень, з них 4,5 тис. – виключно кіберзлочини.

Ключовим кроком у реалізації Стратегії було створення Національного координаційного центру з кібербезпеки у червні 2016 р., який є робочим органом Ради національної безпеки і оборони. Основним завданням Центру є аналіз стану кібербезпеки, результатів проведення огляду національної системи кібербезпеки, стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури, даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Центр прогнозує та виявляє потенційні та реальні загрози у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки, а також оперативне, інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки.

Центр бере участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів, розробляє відповідні методичні документи і рекомендації. Центр має право запитувати та одержувати від орга-

нів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, зокрема й урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами тощо. Керівником Центру за посадою є Секретар Ради національної безпеки і оборони України, секретарем – керівник структурного підрозділу Апарату Ради національної безпеки і оборони України, до відання якого віднесені питання кібербезпеки.

У 2017 році Верховна Рада України ухвалила законопроект «Про основні засади забезпечення кібербезпеки України», а робота над ним тривала понад два роки. Закон є надзвичайно важливим з погляду створення системи забезпечення кібербезпеки держави в цілому. У ньому визначено, кого і що мають захищати від кібератак, хто це має робити. Під захист потрапляють комунікаційні системи, якими користуються органи влади і правопорядку, та ресурси у сферах електронного урядування і комерції. Крім того, захищеними мають бути критично важливі об'єкти інфраструктури [13], які законодавці розуміють як низку підприємств і установ, наприклад, у галузі енергетики, інфраструктури, банківського сектору, стратегічних підприємств. Перевіряти дотримання інформаційної безпеки будуть за допомогою незалежного аудиту, що має проходити за стандартами ЄС та НАТО.

Крім того, як держава-учасниця Будапештської конвенції про кіберзлочинність Україна прагне до повної імплементації Конвенції [14; 15]. Проект закону був підготовлений і зараз обговорюється в Парламенті. Він передбачає посилення відповідальності за кіберзлочинність, а також визначає важливу термінологію та оновлену відповідальність постачальників послуг Інтернету відповідно до Конвенції.

Окрім роботи над національним законодавством, Україна визнає необхідність міцного міжнародного співробітництва та розбудови спроможності для вирішення потреб та загроз, пов'язаних із кібербезпекою, яка також висвітлена в новій Стратегії. Україна співпрацює з багатьма партнерами в кіберсфері. Україна є партнером спільних проектів Європейського Союзу та Ради Європи "CyberCrime EAP II" та "CyberCrime EAP III", які мають регіональний аспект та включають країни Східного партнерства. Перший проект спрямований на посилення взаємної правової допомоги у міжнародній співпраці з питань кіберзлочинності та електронних доказів, на посилення ролі контактних пунктів 24/7 [16; 17]. Другий проект, який був започаткований у Києві у квітні 2016 року, полягає у вирішенні питань державного та приватного співробітництва [18]. За рекомендаціями Ради Європи встановлюється співпраця між національною владою та інтернет-провайдерами. Така співпраця сприятиме структурованому діалогу з інтернет-провайдерами, що допоможе встановити засоби довіри до розуміння та реагування на потреби кожного.

Крім того, британські та естонські партнери надали українським правоохоронним органам сучасне обладнання та програмне забезпечення, щоб провести професійну комп'ютерну кримінальну експертизу і ретельно вивчити кіберзлочини.

У сфері кібербезпеки Україна також співпрацює з Цільовим фондом НАТО з питань кіберзахисту задля підвищення технічних можливостей країни у боротьбі з кіберзагрозами. 4 липня 2017 в Україні було підписано угоду «Про реалізацію Трастового фонду України – НАТО з питань кібербезпеки». Зокрема, угодою передбачено розбудову в Україні мережі ситуаційних центрів реагування на комп'ютерний інцидент та розгалуженої мережі автоматизованих датчиків подій, інтегрованих в інформаційні мережі об'єктів критичної інформаційної структури [19]. Також було ухвалено рішення про подальший напрямок розбудови національної системи кібербезпеки з урахуванням можливостей Трастового фонду, яке передбачає підвищення технічних можливостей України у сфері кібербезпеки шляхом її оснащення автоматизованими датчиками подій та підключення до національної мережі ситуаційних центрів Держспецзв'язку, а також створення центрів кібернетичної безпеки в системах Збройних сил України та Національної поліції з їх подальшим інтегруванням в національну мережу ситуаційних центрів. Разом з партнерами НАТО Україна проводила заняття та тренінги з кіберзахисту, в рамках яких учасники навчалися, як реагувати на великі кібернапади на національну оборонну інфраструктуру.

Україна не лише бере участь у міжнародних ініціативах у сфері протидії кібернетичним загрозам, але також сприяє розвитку регіональних ініціатив. За ініціативи та на чолі з Україною в рамках Організації за демократію та економічний розвиток (до якої входять Азербайджан, Грузія, Молдова, Україна) була створена робоча група з питань кібербезпеки. Група зараз обговорює розробку Меморандуму про взаєморозуміння для прийняття його урядами. Організація вже запровадила захищену систему зв'язку, яка, зокрема, забезпечує безпечний обмін даними в Інтернеті та проведення відеоконференцій.

Досвід України показує, що для подолання постійних кіберзагроз та нападів існує потреба в поглибленій співпраці на різних рівнях (між національними органами, приватним сектором та міжнародними партнерами) для створення необхідних можливостей та ефективного реагування на такі загрози.

Висновки. Провівши дослідження, ми дійшли таких висновків:

1) матеріальні норми, які містять правила поведінки у сфері кібербезпеки, не мають якоїсь суто однієї галузевої належності. Вони стосуються і галузі конституційного права, і кримінального права, і цивільного та господарського, міжнародного права тощо. Вони регулюють певну сторону однорідних суспільних відносин. Сьогодні правове регулювання правовідносин у сфері кібербезпеки в Україні здійснюється незначною кількістю нормативно-правових актів. У 2016 році було прийнято Національну стратегію кібербезпеки України. Вона передбачає вдосконалення національного законодавства, запровадження безпечних умов користування Інтернетом та створення спеціальних органів з кібербезпеки, які змогли б попереджати та усувати наслідки кібератак;

2) особливості процесу впровадження Національної стратегії з кібербезпеки такі: розроблено та затверджено План дій для її реалізації, а також створено організаційно-правовий механізм співпраці між усіма державними установами, місцевими органами влади, військовими підрозділами, правоохоронними органами, науково-дослідними та навчальними закладами, цивільними групами, підприємствами та організаціями незалежно від форм власності або осіб, що є власниками критичної інформаційної інфраструктури;

3) особливістю міжнародного співробітництва України у сфері кібербезпеки є те, що створено нормативно-правовий (імплементація Будапештської Конвенції про кібербезпеку, Угоди про реалізацію Трастового фонду України тощо) та організаційно-правовий механізми співпраці (Україна–ЄС, Україна–Нато та інші).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Deshko L. Structural Elements of International Legal Mechanisms for Ensuring The Everyone's Right to Seek Rights Protection in International Judicial Institutions or in the Relevant Bodies of International Organizations. Закон и жизнь. 2013. № 12/3. С. 64–67.
2. Дешко Л. Критерії ефективності національного засобу юридичного захисту щодо невиконання чи затримок у виконанні рішень національних судів (за матеріалами практики Європейського суду з прав людини). Правничий часопис Донецького Університету. 2012. № 1. С. 84–91.
3. Deshko L. The Subjective Legal Right Structure to Apply to the International Judicial Institutions or to the Relevant Bodies of International Organizations. Ценности и интересы современного общества: материалы Международной научно-практической конференции (Москва, 14 ноября 2013 г.). URL: http://www.mesi.ru/our/ events/detail/124931/.
4. Дешко Л.М. Конституційне право на звернення до міжнародних судових установ та міжнародних організацій: монографія. Ужгород, 2016. 486 с.
5. Кримінальний кодекс України від 05.04.2001 р. № 2341-III Відомості Верховної Ради України. 2001. № 25. Ст. 131.
6. Anton Cherepanov. Analysis of TeleBots' cunning backdoor. We livesecurity magazine. 2017. 4 July. URL: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.
7. Michael Schmitt, Lieutenant Colonel Jeffrey Biller (2017-07-11). The NotPetya Cyber Operation as a Case Study. URL: https://medium.com/@rsatter/cyberattacks-healthcare-and-international-law-65f09e259d8.
8. Пирет Перник. What Ukraine needs to defend against cyber, information and psychological operations. International Centre for defense and security. 2014. September. URL: https://www.icds.ee/ru/blog/article/what-ukraine-needs-to-defend-against-cyber-information-and-psychological-operations/.
9. Про Стратегію кібербезпеки України: Указ президента від 27 січня 2016 р. Відомості Верховної Ради України. 2016. № 96 Ст. 4.
10. Oleksii Tkachenko. Cybersecurity in Ukraine: National Strategy and international cooperation. The Global Cyber Expertise Magazine. 2017. May. 3d issue.
11. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 р. № 242/2016. Відомості Верховної Ради України. 2016. № 242.
12. Про національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40–41. Ст. 379.
13. Nikolai Holmov. Cybersecurity/cyberdefence Ukraine. Structural changes ahead. 2017. November. URL: http://www.odessatalk.com/2017/11/cyber-securitycyber-defence-ukraine-structural-changes-ahead/.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 1, п. 15.
15. Конвенція про кіберзлочинність від 23 листопада 2001 р. Відомості Верховної Ради України. 2001.
16. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року. № 2824-IV. Відомості Верховної Ради України. 2005. № 2824-IV.
17. Assessment report on international cooperation in cybercrime in the EAP region, September 2016. Reports under CyberCrime EAP II. 2016. September. P. 3–4.
18. Cybercrime strategies, procedural powers and specialized institutions in the Eastern Partnership region – state of play, June 2017. Reports under CyberCrime EAP III.2017. June. P. 6.
19. Про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації: угода від 23 липня 2015 р. Відомості Верховної Ради України. 2015. Ст. 5.