

Безуглий Л.А., доцент кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, кандидат юридичних наук

ВЗАЄМОДІЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ З МІЖНАРОДНИМИ ПРАВООХОРОННИМИ ОРГАНАМИ У ЗАПОБІГАННІ КІБЕРЗЛОЧИННОСТІ

У результаті швидкого розвитку нових технологій не менш швидкими темпами з'являються нові форми комп'ютерної злочинності, які отримують поширення при використанні нових методів, наприклад, технології Bluetooth, бездротових систем зв'язку Wi-Fi та WiMAX, пірингових мереж (P2P), спаму та інших [1, с. 28]. Масштаб даної проблеми не обмежується кордонами однієї держави, адже сучасні глобальні комп'ютерні мережі охоплюють переважну більшість країн світу, що додатково актуалізує цілий пласт науково-прикладних аспектів запобігання транснаціональним злочинам. Різке підвищення кримінального комп'ютерного професіоналізму, висока мобільність злочинців, їх організованість здатні виступати чинниками дестабілізації криміногенної обстановки в державі, регіоні та світі. Це ставить на порядок денний питання про необхідність адекватної, системної, узгодженої, випереджаючої реакції правоохоронних органів на швидкозмінні високотехнологічні кримінально-кібернетичні загрози. Одним із основних суб'єктів розгортання та нарощування такої реакції є Національна поліція.

Водночас, досвід запобігання кіберзлочинності показує, що жодна країна не здатна подолати зазначену проблему наодинці. Успіх можуть гарантувати лише спільні дії, як державних, так і комерційних структур. Крадіжки грошей з банківських карток, створення сайтів з дитячою порнографією, комп'ютерні віруси, пропаганда насилля та расової нетерпимості, інструкції з виготовлення саморобних вибухових пристроїв, кібератаки на комп'ютерні мережі державних установ - це лише мала частина злочинів, що вчиняються сьогодні у Інтернеті та яким намагаються запобігти правоохоронні органи різних країн [2, с. 164].

З метою запобігання будь-яким проявам кіберзлочинності та більш швидкого і повного розслідування кримінальних правопорушень у цій сфері, органи Національної поліції (зокрема, кіберполіція) повинні взаємодіяти із суб'єктами ринку телекомунікаційних послуг, зокрема операторами та провайдерами. Зазначена взаємодія повинна ґрунтуватися на зобов'язанні відповідних працівників цих організацій в залежності від функціональних обов'язків або їх власників повідомляти про будь-які випадки незаконного використання мережі, а також всіма доступними в межах закону засобами сприяти виявленню, припиненню, розслідуванню та іншим заходам запобігання кіберзлочинам. Налагодження таких зв'язків можливе через законодавче врегулювання відповідальності зазначених осіб за відмову від співробітництва (ненадання інформації, непредставлення доступу до мережі тощо) обов'язково із позбавленням права зайняття такою діяльністю, а для самих організацій - припинення діяльності.

Необхідним напрямком діяльності Національної поліції є удосконалення заходів взаємодії з підприємствами, установами, організаціями, діяльністю яких є розробка комп'ютерної техніки та програмного забезпечення. Така взаємодія має декілька цілей: по-перше, відстежувати осіб, які мають певні знання у цій сфері (особливо тих, які звільнилися та офіційно не працевлаштувалися або стали займатися індивідуальною підприємницькою діяльністю), тобто можуть бути потенційними суб'єктами аналізованих злочинів; по-друге, покращення форм та методів діяльності на підставі отримання інформації відносно розвитку комп'ютерних технологій; по- третє, удосконалення програмного забезпечення власних систем через перейняття досвіду [2, с. 166].

За своєю суттю злочини у сфері використання комп'ютерних систем є транскордонними. Достатнім підтвердженням цього є існування глобальної всесвітньої мережі Інтернет, яка об'єднує мільйони комп'ютерів в різних країнах світу, відкриває широкі можливості для отримання та обміну інформацією, що все частіше використовується у злочинних цілях. Крім того, перенесення господарської діяльності та забезпечуючих її механізмів у кіберпростір: поява віртуальних грошей і віртуальних банків, широке розповсюдження віртуальних магазинів, бірж, за допомогою

яких надаються реальні послуги та здійснюється придбання товарів, - беззаперечно виступає детермінантою вчинення аналізованих злочинів. На підставі цього, всі міжнародні організації закликають держави у співпраці з іншими зацікавленими сторонами розробляти необхідне законодавство, що передбачає проведення спільних розслідувань зазначених діянь з використанням існуючого міжнародного права, і, зокрема, Конвенції Ради Європи з кіберзлочинності [1, с. 27]. Вищезазначене обумовлює необхідність розроблення та удосконалення шляхів міжнародної взаємодії у сфері запобігання кіберзлочинності.

Доцільним заходом запобігання кіберзлочинності є підтримання та розширення співробітництва Департаменту кіберполіції Національної поліції з міжнародними організаціями, що спрямовують свою діяльність у зазначеній сфері. Наприклад, вельми необхідним заходом було відпрацювання у 2011 р. Службою безпеки України разом з НАТО загальних механізмів боротьби з кіберзлочинністю, а саме були розроблені експертні консультації відносно кібернетичного захисту [3]). Ініціатива щодо здійснення таких заходів повинна виходити від вищих органів державної влади, передусім від керівництва Національної поліції, Генеральної прокуратури України, СБУ та Міністерства закордонних справ України. Розвинення зазначеної взаємодії обумовлює не лише співпрацю органів у запобіганні злочинів, а й обмін досвідом діяльності у цій сфері.

Викликає кримінологічний інтерес, прийнятий у 2018 році американським Конгресом законопроект «Про співпрацю з Україною в питаннях кібербезпеки» [4]. Документ передбачає допомогу Україні в удосконаленні стратегії безпеки в кіберпросторі. При цьому наголошується на доцільності для Конгресу й уряду США здійснити низку конкретних кроків. Йдеться, насамперед, про посилення захисту урядових комп'ютерних мереж України, зменшення залежності від російських інформаційних систем і технологій, а також розширення можливостей для України в плані міжнародного обміну інформацією [4].

Доцільно також зазначити, що необхідною умовою запобігання кіберзлочинності є приєднання відповідних підрозділів Національної поліції до міжнародних програм, що

створюються та організовуються різними державами на підставі договорів та угод. Так, наприклад, відповідно до Конвенції «Про кіберзлочинність», яка ратифікована Верховною Радою України, держави-учасники повинні здійснити організаційні заходи стосовно розробки необхідних умов (організація контактних пунктів), на національному рівні, та приєднатися до мережі щоденного цілодобового доступу (міжнародне позначення «24/7 Network», що може бути розшифровано як «доступ 24 години 7 діб на тиждень»), що спрямована на співпрацю та надання допомоги при розкритті та розслідуванні кіберзлочинів [1, с. 29].

В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при запобіганні злочинам, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. Але, на сучасному етапі, не зважаючи на обов'язковість, зазначені умови не були виконані у необхідному обсязі. Укладення зазначених угод та приєднання до подібних програм є необхідним кроком для здійснення та розроблення заходів запобігання аналізованим злочинам. За логікою правового розмежування повноважень між МВС та новоствореною Національною поліцією вказана задача має перейти до сфери відання саме останньої. При цьому переконанні, що важливо зберегти на рівні правового регулювання та практичної реалізації координуючу роль в цьому процесі МВС.

Крім того, необхідним кроком міжнародної взаємодії, в зазначеній сфері, є не лише організація та прийняття участі у вказаних мережах, а й укладання угод, з відповідними підрозділами правоохоронних органів інших країн, з метою обміну інформацією відносно вчинених кіберзлочинів (способів, методів, застосованих технічних або інших засобів тощо) та заходів, що застосовуються щодо їх запобігання та розкриття (на сучасному етапі, наприклад, існує Меморандум «Про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом» [6]).

Налагодження таких зв'язків є доцільною умовою спрямованою на обмін інформацією у аналізованій сфері.

Необхідною та ефективною умовою запобігання кіберзлочинності є взаємодія Національної поліції з вітчизняними й міжнародними об'єднаннями, що створюються, у більшості випадків, різними суб'єктами (сукупність окремих осіб або підприємствами, установами чи організаціями, переважно приватної форми власності) на добровільних началах, і мають за мету захист інформаційної інфраструктури. Так, наприклад, ще на початку 1990-х років була створена організація FIRST - форум команд реагування на інциденти, яка об'єднує 80 бригад реагування, які складаються із працівників державних, комерційних, промислових та навчальних установ з 19 країн світу [6, с. 74]. Здійснення зазначених заходів дозволить, по-перше, слідкувати за процесами розвитку комп'ютерних технологій та програмного забезпечення, подруге, обмінюватися досвідом у сфері запобігання аналізованим злочинам, по-третє, слідкувати за існуванням підприємств, установ та організацій, що здійснюють діяльність або надають послуги у зазначеній сфері.

Список використаних джерел:

1. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27-30. URL: <http://www.nbu.gov.ua/e-journals/FP/2011-4/nbvmpmk.pdf>.
2. Кравцова М. О. Система заходів запобігання кіберзлочинності правоохоронними органами. *Митна справа*. 2014. Спец. випуск. С. 164-169.
3. СБУ отработывает с НАТО механизмы борьбы с киберпреступностью. «ЗАЗУБРИНА» Газета ВОО ЗУБР. URL: <http://za.zubr.in.ua/2011/10/18/13536/>
4. Про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом: Меморандум від 09.09.2009 р. URL: http://zakon2.rada.gov.ua/laws/show/528_031.
Про співпрацю з Україною в питаннях кібербезпеки: з'явився переклад нового закону США. *Експрес*. 2018. URL: <http://expres.ua/news/2018/02/09/283528-spiivpracyu-ukraymoyu-putannyah-kiberbezpeky-zyavyvsya-pereklad-novogo>-
Біленчук П. Д. Міжнародна високотехнологічна кіберзлочинність: поняття, сутність, шляхи подолання.
Актуальні проблеми держави і права. 2008. Вип. 44. С. 71-75.