ФП 2013-1
ISSN 1995-6134

УДК 343.1:65.012.8(477)

О.В. МАНЖАЙ, канд. юрид. наук,
Харківський національний університет внутрішніх справ

ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

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

Використання комп'ютерних технологій з протиправною метою є вже усталеним явищем, яке потребує прискіпливої уваги та належного реагування з боку правоохоронних органів. На тенденцію зростання кіберправопорушень звертають увагу по всьому світу. Зокрема, 2012 р. було визначено наступні тенденції щодо протиправного використання комп'ютерних технологій [1]:

1) підвищення атак на смартфонні та планшетні платформи, особливо Android;

2) збільшення використання уразливостей у програмному забезпеченні мобільних пристроїв для отримання даних кіберзлочинцями;

3) зменшення розмірів бот-мереж з одночасним збільшенням їх кількості, що зменшує ефективність боротьби з ними правоохоронними органами;

4) вибір для хакерських атак нетрадиційних об'єктів, у тому числі об'єктів важкої промисловості та медичних пристроїв;

5) удосконалення кіберзлочинцями шляхів протидії правоохоронним органам;

6) збільшення загроз з боку хакерських угруповань для організацій, які зберігають важливу інформацію;

7) збільшення використання соціального інженірінга щодо малого та середнього бізнесу;

8) збільшення кількості суб'єктів, які використовуватимуть інструментарій кіберзлочинця для досягнення власних цілей (групи активістів, корпорації, уряди);

9) збільшення кількості гучних втрат інформації у результаті кібератак.

Зважаючи на зростаючий рівень кіберзлочинності керівництво більшості країн світу докладає значних зусиль для боротьби з цим злом.

Протягом останніх двох десятиліть у світі стала активно розроблятися правова база, спрямована на попередження та припинення кіберзлочинів. Відповідні зміни до кримінального законодавства було внесено Канадою у 1985 р., Німеччиною у 1986 р., Японією у 1987 р., Англією у 1990 р., Ірландією, Португалією та Турцією у 1991 р., Люксембургом та Нідерландами у 1993 р., Ізраїлем у 1995 р., Бельгією у 2000 р.

Спеціальні норми або навіть розділи про кіберзлочини містять усі нові кримінальні кодекси, ухвалені у світі, починаючи з 1992 р., у тому числі кримінальні кодекси усіх країн СНД та Балтії [2, с.22].

В вітчизняній науці питання боротьби з кіберзлочинністю досліджували О.М. Бандурка, Л.В. Борисова, В.М. Бутузов, Н.Л. Волкова, І.О. Воронов, В.О. Голубєв, М.В. Гуцалюк, О.Ф. Долженков, В.Ю. Журавльов, В.П. Захаров, М.Ю. Літвінов, Ю.Ю. Орлов, Е.В. Рижков, М.М. Перепелиця, С.М. Рогозін, Л.П. Скалозуб, Ю.В. Степанов, В.П. Шеломенцев та ін. Різні аспекти застосування інформаційних технологій у правоохоронній діяльності розглядали російські дослідники С.С. Овчинський, В.С. Овчинський, А.С. Овчинський, А.Л. Осипенко, В.І. Попов, А.В. Борбат, В.В. Зорін, А.В. Макієнко, дослідники зі США С. Хейман, Д. Грін, В. Вайтлідж, білоруський дослідник В.Є. Козлов та ін. Незважаючи на позитивні зрушення у сфері нормативного регулювання боротьби з кіберзлочинністю, що відбуваються останніми роками в світі, слід констатувати, що багато проблем залишаються невирішеними. Така ситуація є особливо актуальною для України.

Сьогодні в Україні нормативно-правову базу у сфері боротьби з кіберзлочинністю складає, перш за все, Конституція України, у ст.17 якої відзначається, що забезпечення інформаційної

ISSN 1995-6134

безпеки України є найважливішою функцією держави, справою всього Українського народу.

Крім Конституції положення щодо боротьби з кіберзлочинністю містяться у Конвенції «Про кіберзлочинність» від 23.11.2001 р., ратифікованої Верховною Радою України 07.09.2005 р. (далі Конвенція) [3]. Відповідно до норм вказаної Конвенції країни-учасниці повинні здійснити низку заходів на національному рівні, спрямованих на боротьбу з кіберзлочинами. Загальну структуру таких заходів у сфері матеріального кримінального права, наведено на рис.1.

Рисунок 1 – Заходи у сфері матеріального кримінального права

Слід відмітити, що дані заходи майже у повному обсязі здійснено Україною шляхом доповнення та внесення змін до окремих статей Кримінального кодексу України.

У Конвенції також містяться норми, спрямовані на здійснення заходів, які б забезпечували збереження файлів протоколів провайдерів та операторів телекомунікаційних послуг (ст.16) та встановлення повноважень компетентних органів щодо отримання такої інформації (ст.18), а також здійснення окремих слідчих (розшукових) дій (обшук і арешт комп'ютерних даних, які зберігаються) та оперативно-розшукових або негласних слідчих (розшукових) дій (збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації).

Нормами Конвенції (ст.22) також закріплено юрисдикційні питання боротьби з кіберзлочинністю (рис.2).

Окремий розділ Конвенції присвячено міжнародному співробітництву країн-учасниць у сфері боротьби з кіберзлочиністю. Докладно висвітлюються принципи:

– *екстрадиції* (ст.24). В Україні органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, є Міністерство юстиції України (щодо доручень судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства).

– *взаємодопомоги* (статті 25–26), у тому числі за надзвичайних умов та добровільного надання інформації без наявності спеціального запиту.

ISSN 1995-6134

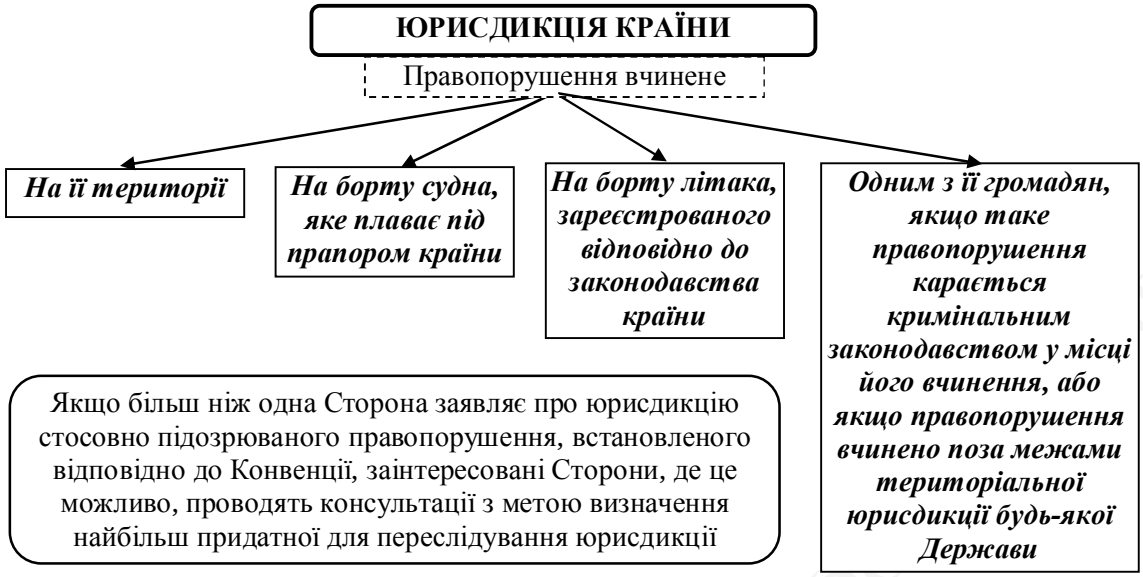

Рисунок 2 – Юрисдикція щодо кіберзлочинів

Важливою нормою Конвенції є право її учасників на здійснення без дозволу іншої сторони доступу до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи.

Для ефективної реалізації положень Конвенції щодо взаємодії правоохоронних органів у боротьбі з кіберзлочинністю створюється цілодобова мережа для здійснення контактів з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Зміст такої допомоги наведено на рис. 3.

Рисунок 3 – Структурна схема допомоги, яку надає цілодобова контактна мережа у боротьбі з кіберзлочинністю

ISSN 1995-6134

Крім Конвенції до нормативно-правової бази боротьби з кіберзлочинністю можна віднести норми Кримінального кодексу України (майже всі склади злочинів можуть охоплювати використання кіберпростору для їх вчинення), Кримінального процесуального кодексу України, зокрема, ст.263 (зняття інформації з транспортних телекомунікаційних мереж), ст.264 (зняття інформації з електронних інформаційних систем), ст.268 (установлення місцезнаходження радіоелектронного засобу), ст.274 (негласне отримання зразків, необхідних для порівняльного дослідження). Велику роль у боротьбі з кіберзлочинністю грає і Закон України «Про оперативно-розшукову діяльність» (ст.8) та низка інших законодавчих актів, серед яких можна виділити Закони України «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

Вказані нормативно-правові акти не в повній мірі регламентують питання, пов'язані із боротьбою з кіберзлочинністю, про що, зокрема, наголошують фахівці Національного інституту стратегічних досліджень при Президентові України, якими виділено три основних проблеми, що ускладнюють боротьбу проти злочинів в кіберсфері:

1. Відсутність не просто усталених визначень ключових термінів («кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфраструктура», «критична кіберінфраструктура»), але й таких, що можуть ефективно застосовуватись в практиці правоохоронної діяльності.

2. Несформованість (не реформованість) чинного нормативно-правового поля.

3. Відсутність Єдиної загальнодержавної системи протидії кіберзлочинності із відповідним нормативним забезпеченням [4].

Окремі проблеми щодо боротьби з кіберзлочинністю існують і у нормативно-правовому забезпеченні роботи підрозділів, які безпосередньо виконують функції з протидії таким правопорушенням. В Україні це підрозділи боротьби з кіберзлочинністю, які перебувають у структурі Управління боротьби з кіберзлочинністю МВС України (УБК), що є самостійним структурним підрозділом Міністерства внутрішніх справ України, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, у тому числі організовує та здійснює оперативно-розшукову діяльність. УБК діє на підставі відповідного наказу МВС України [5].

До компетенції УБК належать злочини та правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також інші злочини та правопорушення, учинені з їх використанням. Тобто компетенція УБК стосується досить широкого кола небезпечних посягань на суспільні відносини.

Слід відзначити, що до сьогодні чітко не окреслено повноваження та порядок дій підрозділів боротьби з кіберзлочинністю у різних сегментах кіберпростору. Особливо це стосується таких чутливих випадків, коли правоохоронцям доводиться проводити заходи, що можуть зачіпати юрисдикцію інших держав, оскільки чітких кордонів у кіберпросторі окреслити неможливо. Актуальним питанням є також невизначеність строків, протягом яких провайдери та оператори телекомунікацій повинні зберігати інформацію про транзакції своїх абонентів та ступінь деталізації такої інформації.

На теперішній час завдання по створенню єдиної загальнодержавної системи протидії кіберзлочинності, поставлене Президентом України у п.4.1 Указу № 1119/2010 від 10.12.2010 р., залишається невиконаним у повному обсязі. Це призводить до негативних наслідків не лише всередині країни, але й позначається на іміджеві держави в світі. Так, у цьогорічній вересневій доповіді Конгресу США Україну було названо у трійці країн-лідерів зі сприятливим кліматом для піратства та визнано «центром» пірінгових мереж, що містять піратські матеріали [6].

ISSN 1995-6134

Враховуючи вищевикладене, вважаємо що слід по новому підійти до питання удосконалення нормативно-правового забезпечення боротьби з кіберзлочинністю. Оскільки основні функції щодо боротьби з цими злочинами покладено на УБК МВС України, то відповідно саме ця структура, повсякденно стикаючись із проявами кіберзлочинності, є найбільш поінформовано про проблеми, які існують у нормативно-правовому забезпеченні цієї сфери. Отже, саме МВС України має стати центром з розробки необхідних пропозицій щодо внесення змін та доповнень до чинного законодавства та виконувати роль координатора у створенні єдиної загальнодержавної системи протидії кіберзлочинності. Така позиція також цілком узгоджується із положеннями Кримінального процесуального кодексу України від 13.04.2012 р.

ЛІТЕРАТУРА

1. 12 Security Predictions for 2012 [Електронний ресурс]. – Режим доступу: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp_12-security-predictions-for-2012.pdf?cm_re=HP:Sub:1-_-2012+Security+Predictions.

2. Додонов В. В. Сравнительное уголовное право. Общая часть: монография / В. В. Додонов ; под общ. ред. и науч. ред. С. П. Щербы. – М. : Юрлитинформ, 2009. – 448 с.

3. Конвенція Ради Європи «Про кіберзлочинність» : від 07.09.2005 р.

4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналітична записка / Д. Дубов, М. Ожеван [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454.

5. Наказ МВС України «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» : від 31.05.2012 р., № 494.

6. Congressional Anti Piracy Caucus 2012 Country Watch List [Електронний ресурс]. – Режим доступу: http://www.scribd.com/doc/106458437/Congressional-Anti-Piracy-Caucus-2012-Country-Watch-List.

Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні / О. В. Манжай // Форум права. – 2013. – № 1. – С. 646–650 [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/e-journals/FP/2013-1/13movkvu.pdf

Проаналізовано нормативно-правову базу у сфері боротьби з кіберзлочинністю. Визначено роль та компетенцію підрозділів боротьби з кіберзлочинністю. Розкрито проблеми, які існують у нормативно-правовому забезпеченні цієї сфери. Визначено механізм їх вирішення.

***

Манжай А.В. Проблемы нормативно-правового обеспечения борьбы с киберпреступностью в Украине

Проанализирована нормативно-правовая база в сфере борьбы с киберпреступностью. Определена роль и компетенция подразделений борьбы с киберпреступностью. Раскрыты проблемы, которые существуют в нормативно-правовом обеспечении этой сферы. Определен механизм их решения.

***

Manzhai O.V. Problems of the Normatively Legal Support of Cybercrime Combating in Ukraine

A normatively legal base is analyzed in the field of combating cybercrime. Role and jurisdiction of Cyber Crime Division are identified. Problems which exist in the normatively legal support of this sphere are exposed. Mechanism of their decision detected.