https://www.scilook.eu/index.php/slif/article/view/slif17-02-035
DOI: 10.30888/2415-7538.2020-17-02-035

УДК 34.03

CYBER CRIMES IN THE MODERN INFORMATION SPACE ON THE WAY OF EUROPEAN INTEGRATION PROCESS

КІБЕРЗЛОЧИНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ НА ШЛЯХУ ЄВРОІНТЕГРАЦІЙНОГО ПРОЦЕСУ УКРАЇНИ

Bakalo V.O. / Бакало В.О.
master / магістр
Myroshnychenko V.O. / Мирошниченко В.О.
scientific director / науковий керівник
c.t.s., as.prof. / к.т.н., доц.
ORCID iD: https://orcid.org/0000-0002-7508-737X
Dnepropetrovsk State University of Internal Affairs
Ukraine, Dnipro city, Gagarin Ave. 26, 49005
Дніпропетровський державний університет внутрішніх справ
Україна, м. Дніпро, пр. Гагаріна 26, 49005

Анотація. *Наша держава, як і всі країни світу, кожного дня стикається із викликами у сфері кібербезпеки, так як із стрімким розвитком технологій зростає кількість злочинів у даній сфері. Щороку в Україні вчиняються десятки тисяч злочинів із використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. В роботі розглянуті питання боротьби з кіберзлочинністю на державному та міжнародному рівнях. Для вирішення даної проблеми авторами надані рекомендації законодавчого та соціального характеру.*

Ключові слова: *міжнародне співробітництво, суспільні відносини, кіберзлочини, кібербезпека, комп'ютерні технології, комп'ютерні мережі.*

Вступ.

На сьогоднішній день інформатизація суспільства досить активно та стрімко вторгається у різні сфери діяльності нашого життя. Усі найважливіші функції, так чи інакше, здійснюються із використанням автоматизованих комп'ютерних мереж та систем. Динамічний розвиток комп'ютерних технологій надав можливість для появи нових невідомих раніше такого роду правопорушень, а також рецидивів традиційних злочинів із використанням інформаційних технологій, що становить собою одну із найбільш актуальних та дискусійних проблем як у державному, так і міжнародному просторі.

Водночас розвиток та ускладнення суспільних відносин, посилення транскордонної злочинності, а також вагомі досягнення у сфері технологій, які повністю змінили методи взаємодії на людей, що призвели до появи такого явища, як кіберзлочинність, яка сьогодні повністю опанувала середовище соціальних, комп'ютерних мереж та мобільних пристроїв.

Широке використання сучасних інформаційних технологій у суспільстві та державних структурах висуває необхідність вирішення проблем інформаційної злочинності якої однією з основних у рамках державного регулювання системи національної безпеки.

Виклад основного матеріалу дослідження.

На жаль, Україну також не оминула проблема, пов'язана з кібербезпекою. Попри те, у жодному міжнародно-правовому акті відсутня інтерпретація такого

поняття та водночас явища як - кіберзлочинність. Більше того, експерти, що входять до групи Всебічного дослідження проблеми кіберзлочинності та відповідних заходів зі сторони держав-членів міжнародного співтовариства, відповідно до Резолюцій Генеральної Асамблеї Організації Об'єднаних Націй від 23.01.2013 року, вказують на відсутність необхідності формування такого єдиного узагальнюючого поняття, окреслюючи це тим, що: «визначення діапазону спеціальних слідчих повноважень та можливостей в міжнародній галузі, співробітництва не потребує пошуку широкого, штучного визначення концепції кіберзлочинності» [1].

Розповсюдження комп'ютерних вірусів, несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж, виготовлення та розповсюдження шкідливого програмного забезпечення, втручання у політичні процеси в країнах та особисте життя громадян, що в переважній більшості носить транснаціональний організований характер, атаки на українські об'єкти фінансового та енергетичного секторів, викрадення інформації – це ще не повний перелік кіберзлочинів, які відомі в Україні на сьогодні.

Також поза увагою не можна залишити ті злочини об'єктом яких є не тільки комп'ютерні дані інформаційних систем, але й інші злочини, які вчиняються з використанням кіберпростору, наприклад торгівля наркотичними засобами, психотропними речовинами та прекурсорами через мережу-Інтернет, поширення порнографічних матеріалів, дитячої порнографії, протиправні дії з платіжними картками, шахрайство, вимагання, погроза вбивством, булінг, фінансування терористичних заходів та терористичних угрупувань, незаконна торгівля вогнепальною зброєю, вибуховими речовинами та вибуховими пристроями, тощо. Досить популярним явищем на сьогоднішній день є Веб-моделінг, суть якого полягає у веденні еротичних, а іноді навіть порнографічних онлайн-відеочатів.

Із збільшенням числа користувачів Інтернет та засобів доступу до мережі, збільшується потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. Електронні дані передаються з однієї держави в іншу за декілька секунд, а контролювати передачу даних, з урахуванням їх обсягу та кількості користувачів, майже не неможливо [2].

У ході аналізу щорічного звіту Європолу під назвою «Оцінка загроз, організованих через інтернет (IOCTA)» за 2016 – 2019 роки можна визначити, що розповсюдження програм-вимагачів «Ransomware» становить одну з основних загрозу у кіберпросторі. Вони поширили свій вплив на різноманітні галузі як у державному, так і в приватному секторах. Активне розповсюдження таких програм аргументується тим, що у порівнянні з іншими програмами, які викрадають інформацію, за програми-вимагачі легше отримати викуп, а також за допомогою криптовалют (наприклад Bitcoin) здійснити подальше відмивання злочинних грошей. Проте цифрові валюти адаптовані для використання організованими злочинними угрупованнями, оскільки вони досить поширені в міжнародному обігу та забезпечують необхідний рівень анонімності. Загроза відмивання грошей, пов'язаних з віртуальними валютами, демонструє, що кримінальний світ може використовувати віртуальні валюти для доступу до

чистої готівки і одночасно приховувати сліди транзакцій [3].

Використання глобальних інформаційних мереж та швидкість передачі інформації дає змогу використовувати ці переваги не тільки для розвитку інформаційного суспільства, але й для вчинення протиправних діянь. Цьому сприяє і те, що інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавство та правоохоронні органи можуть на це реагувати. Тому злочинність у кіберпросторі – одна з найгостріших проблем, яка постала сьогодні перед українською спільнотою.

Загальновідомо, що наша держава є однією з лідерів за кількістю кібератак у всьому світі. Україна опинилася на четвертому місці після Росії, Тайваню і Німеччини. Це відбувається тому, що українські закони, які повинні врегульовувати питання кіберпростору і злочинних посягань на його просторах недостатньо розроблені та реалізовані у практичній діяльності [4].

На даний момент законодавче регулювання кібербезпеки в Україні знаходиться на початку свого формування. Невирішеними є питання державно-приватної взаємодії, триває розробка напрямків до кібероборони, попереду ще великий обсяг роботи, спрямований на нормативно-правове врегулювання у сфері кібербезпеки [5].

Прийнятий Верховною Радою України Закон «Про основні засади забезпечення кібербезпеки України» визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [6].

Необхідно також відзначити значну роль міжнародних договорів у сфері співробітництва боротьби з кіберзлочинністю у кримінальних справах. Наприклад, Угода між Кабінетом Міністрів України і Урядом Турецької Республіки про співробітництво передбачає надання взаємної допомоги в попередженні й розкритті кіберзлочинів. Це означає, що у разі виникнення такої необхідності правоохоронні органи обох держав зобов'язані всебічно та двосторонньо сприяти діяльності один одному [7].

Чинним Кримінальним Кодексом України встановлена відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361); 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 (ст. 362);

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 обробляється (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) [8].

В Україні на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері. Станом на початок 2019 р. до правової основи кібернетичної безпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України [8].

На нашу думку боротьба з кіберзлочинністю на рівні держави є майже безрезультатною, оскільки наші навички та досвід поки що не дають нам такої змоги. Колізії, які існують в нашому законодавстві, на належному рівні не усуваються, а навпаки все більше загострюються, у зв'язку із цим при виявлені нових кіберзлочинів законодавство нашої держави залишається не адаптованим до сучасних викликів у цій сфері та не дієвим.

Висновки.

Аналіз розглянутої проблеми дозволяє зазначити, що законодавча регламентація потребує механізму сприяння правоохоронним органам України, так як проблема відсутності дієвого законодавства в сфері регулювання інформаційних віртуальних відносин загострюється, що у свою чергу дає можливість злочинцям залишатися безкарними та сприяти зростанню кількості кіберзлочинів. Міжнародне співробітництво у розслідуванні кіберзлочинів (насамперед використання механізмів, передбачених Угодою між Україною та Європолом про оперативне та стратегічне співробітництво) можна вважати основним напрямом подолання існуючого розриву між розвитком інформаційних технологій та відповідного правового регулювання, спрямованого на захист інтересів особи, суспільства і держави. Для здійснення ефективного протистояння з кіберзлочинністю на національному і міжнародному рівнях, необхідно адекватно оцінювати зміни процесуальних норм ведення розслідування і переслідування в судовому порядку, а також враховувати вимоги часу і потреби практики.

Список використаних джерел:

1. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов международного сообщества и частного сектора URL: http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/unodc_cc

pcj_eg4_2013_2_r.pdf (дата звернення: 25.02.2020).

2. Проблеми розслідування кіберзлочинів в Україні. URL http://nbuv.gov.ua/UJRN/ecfipr_2018_1_7 (дата звернення: 27.02.2020).

3. Сучасні тенденції організованої кіберзлочинності. URL http://nbuv.gov.ua/UJRN/Infpr_2019_1_15 (дата звернення: 27.02.2020).

4. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю. URL: http://nbuv.gov.ua/UJRN/Tpdu_2013_3_3 (дата звернення: 26.02.2020).

5. Закон України «Про основні засади забезпечення кібербезпеки України». режим доступу: URL: http://zakon3.rada.gov.ua (дата звернення: 25.02.2020).

6. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект. URL: https: //iful.edu.ua/wp-content/uploads/2018/08/dysertatsiya_buyadzhy.pdf (дата звернення: 27.02.2020).

7. Кримінальній Кодекс України : чинне законодавство зі змінами та допов. станом на 1 квіт. 2019 року: (офіц.текст). – к.: Паливода А.В., 2019. – 264 с. -(Кодекси України).

8. Кібербезпека: вразливі моменти. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 29.02.2020).

Abstract. *Our country, like all countries in the world, faces cyber security challenges every day, as the number of crimes in this field is increasing with the rapid development of technology. Each year, tens of thousands of crimes are committed in Ukraine using information and communication technologies, software, hardware, other technical and technological tools and equipment. The paper deals with issues of combating cybercrime at the national and international levels. To address this issue, the authors have provided legislative and social guidance.*

Key words: *international cooperation, public relations, cybercrime, cyber security, computer technology, computer networks.*

Стаття відправлена: 09.04.2020 р.