ЛІТЕРАТУРА:

1. Білоус В. Т. Координація боротьби з економічною злочинністю. – К.: Академія держ. податк. служби України, 2012. – 449 с.
2. Бойко А. Економічна злочинність як соціальне явище // Львівський університет: Вісник Львівського університету. Серія юридична. – Вип. 37. – Львів: ЛДУ, 2015. – С. 461 – 466.
3. Вівчар О. І. Сучасні проблемні домінанти злочинних груп у соціогуманітарному просторі України (безпекознавчий вимір системи підприємницьких структур) / О. І. Вівчар // Проблеми системного підходу в економіці. – Збірник наукових праць. – Випуск 3(59). – Київ, 2017р. – С. 55-61.
4. Вівчар О. І. Соціогуманітарне пізнання у контексті протидії злочинності в системі підприємницьких структур ["Societas Familia – Parantela] / О. І. Вівчар. – Redakcja: ks. prof. Dr hab. Jan Zimny – Stalowa Wola. – 2017. – (p. 144-169).
5. Гуцалова К. Поняття та ознаки економічної злочинності: огляд літератури та проблемні питання // Підприємництво, господарство і право. – 2016. – № 10. – С. 87 – 89.

Карий В.В.
студент ІІ курсу магістратури юридичного факультету
Тернопільського національного
економічного університету
***Науковий керівник**: к.ю.н., доцент кафедри*
кримінального права та процесу ТНЕУ
Олійничук Р.П.

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ З ВИКОРИСТАННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ УКРАЇНИ

Конституція України проголосила, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються найвищою соціальною цінністю, а права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави (ст. 3). Значної шкоди соціальній цінності завдає злочинність, яка втручається у всі сфери життєдіяльності людини.

Сучасний світ майже не можливо уявити без інформаційно-телекомунікаційних технологій, які впливають на більшість аспектів життєдіяльності суспільства. Але, на жаль, інформаційно-телекомунікаційні технології використовуються і для вчинення злочинів, які є найбільш суспільно небезпечними. Сьогодні в Україні з проявами кіберзлочинності стикаються у банківській, кредитно-фінансовій, соціальній, культурній, духовній та інших сферах суспільного життя. За різними оцінками фахівців, кіберзлочинність посідає п'яте місце після торгівлі зброєю, наркотиками, злочинами у банківській сфері та економіки [1, с.216]. Проблема боротьби з кіберзлочинністю сьогодні розглядається як одна з глобальних проблем сучасності, і потребує вирішення на

міжнародному рівні. На вітчизняному просторі, в системі Національної поліції створенні підрозділи по боротьбі з кіберзлочинністю, які, поки що, можна сказати знаходяться на стадії становлення та розвитку і потребують правового, організаційного, кадрового, матеріально-технічного та іншого забезпечення.

У законодавстві та юридичній літературі не сформувалося єдиного підходу до методики виявлення, документування та розслідування даного виду злочинів. Значний внесок у вивчення зазначеної проблеми зробили провідні українські та зарубіжні вчені-юристи, а саме: О.Я. Баєв, Р.С. Бєлкін, В.Д. Гавловський, Ю.В. Гаврилін, В.О. Голубєв, Б.Д. Завідов, І.В. Лазарева, В.А. Мещеряков, О.М. Піменов, Н.А. Розенфельд, Г.В. Семенов, О.І. Усов та інші.

Організація протидії цьому виду злочинності в Україні складалася тривалий час не досить ефективно що, в першу чергу, пов'язувалось з відсутністю необхідної законодавчої бази. Тому можна констатувати той факт, що раніше зазвичай не приділялося достатньої уваги цьому виду суспільно небезпечних злочинних діянь. І лише після того, коли, наприклад, матеріальні збитки від вищевказаних діянь досягли таких розмірів, що стали різко виділятися на загальному рівні збитків від загально кримінальної злочинності, прийшов час, коли на цьому новому злочинному явищі зосереджено увагу, зроблено акцент [2, с.67].

Джерелом кібернетичних загроз можуть бути не тільки міжнародні злочинні групи хакерів, добре обізнані у сфері інформаційних технологій злочинці,а й іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як "транзитного майданчика" для приховування кібернетичної атаки на інформаційні ресурси третьої держави, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового і воєнного характеру. Вказані чинники перевели проблему боротьби з кіберзлочинністю із загально-кримінальної у військово-політичну, про що свідчить активність з боку провідних країн світу у кіберпросторі, глибинні зміни у їх зовнішній та внутрішній інформаційній політиці, формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі – все це обумовлює необхідність створенняв Україні ефективної національної системи кібернетичної безпеки, що знайшло підтримку на рівні вищого політичного керівництва держави [3, с.119].

За даними міжнародної служби щодо забезпечення безпеки в області кіберзагроз «SymantecSecurity», щосекунди в світі піддаються кібератаці 12 осіб, а щорічно в світі реєструється близько 556 млн кіберзлочинів, збиток від яких становить понад 100 млрд дол. США [4, с.37]. Глобальна природа кіберзлочинності проявляється в її транснаціональному характері: готується і вчиняється кіберзлочин в одній країні, а шкода завдається в інший. Так, в списку країн з високим рівнем скоєних злочинів у віртуальному середовищі Україна неодноразово обіймала найвищі позиції і водночас належить до групи найбільш незахищених від кіберзагроз держав. Відповідно до останніх кримінологічних

досліджень, середньорічний темп приросту кіберзлочинності в Україні протягом 2002–2015 рр. складає 107,5 %, що надає могутній поштовх для вироблення своєчасних і ефективних заходів для запобігання цьому виду злочинів і запозичення найкращих практик країн ЄС.

Одним із основних міжнародних актів у цій галузі є Конвенція про кіберзлочинність (Будапештська конвенція), ухвалена Радою Європи 23 листопада 2001 р. і ратифікована Україною 7 вересня 2005 р. із деякими застереженнями і заявами [5, с. 25]. Станом на 2016 р., Будапештську конвенцію ратифікували усі держави Ради Європи (за винятком Російської Федерації і Сан-Маріно), а також США, Канада, Австралія, Японія та деякі інші країни, іще понад сто держав взяли документ за основу для національного законодавства у сфері протидії кіберзлочинності. Серед ключових вимог Конвенції можна виокремити наступні: - встановлення кримінальної відповідальності за дії, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними у національному законодавстві; - створення спеціальних інститутів дотримання правопорядку у кіберпросторі; - забезпечення належного балансу між правоохоронними інтересами і повагою до основних прав людини; - активна участь у міжнародному співробітництві з указаних питань.

Таким чином, для того щоб національна система кібербезпеки відповідала рівню економічно розвинених країн, необхідно вжити послідовні дії з боку держави, спрямовані на підвищення ефективності та розвиток системи взаємодії учасників кіберпростору. Ці та інші положення знайшли відбиток у нещодавно затвердженій Указом Президента Стратегії кібербезпеки України, покликаній захистити життєво важливі інтереси людини і громадянина, суспільства та держави в кіберпросторі за допомогою цілісного комплексу правових, організаційних та інформаційних заході. Проте, її позитивна імплементація залежатиме, перш за все, від дотримання належного балансу між захистом від кіберзагроз і забезпеченням основоположних прав людини; уникнення корупціогенних законодавчих новел, а також своєчасного виявлення та розробки заходів протидії новітнім протиправним практикам (фішинговим атакам, використанню зі злочинною метою хмарних сховищ і криптовалюти тощо)

ЛІТЕРАТУРА:

1. Головкін Б. М. Поняття, предмет, система кримінології та її завдання на сучасному етапі розвитку / Б. М. Головкін // Питання боротьби зі злочинністю : зб. наук. пр. – Харків, 2014. – Вип. 28. – 59–68с. – 67 с.

2. Довгань О.Д., Климчук О.О., Панченко В.М. та ін. Організаційно-правові засади критичної інфраструктури України від кіберзагроз: моногр. – К. : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2013. – 244 с.

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]: Верховна Рада України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/96/2016