Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОРТЬБІ ІЗ КІБЕРЗЛОЧИННІСТЮ

Слободянюк А.В..
слухач1 курсу магістратури ОПП «Право» ОДУВС
Форос Г.В.
т.в.о завідувача кафедри кібкрбезпеки та
інформаційного забезпечення ОДУВС, к.ю.н., доцент

Відповідно до статті 5 Закону України «Про інформацію»: «Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів». З кожним роком розширюється застосування інформаційних технологій. Деякі галузі діяльності людини не можуть повноцінно функціонувати без використання інформаційних технологій.

Актуальність даної теми полягає у збільшенні ефективності сучасних інформаційних технології в боротьбі зі кіберзлочинністю, дослідження законодавства, яке регулює застосування сучасних інформаційних технології та визначення проблем, що виникають під час його застосування. Необхідно визначити, які інформаційні технології повинні бути вдосконалені, на основі практики інших країн.

Окремі аспекти розвитку та становлення інформаційних відносин, питання здійснення протидії кіберзлочинності розглядались провідними вітчизняними науковцями М. О. Будаковим, В. М. Бутузовим, М. М. Галамбою, Р. А. Калюжним, В. В. Коваленко, Я. Ю. Кондратьєвим, Б. А. Кормичем, Ю. Є. Максименко, А. І. Марущаком, Г. В. Новицьким та іноземними фахівцями А. Робертом, К. Осакве, Т. Блентаном, Д. Банісаром та ін.

Найбільшою цінністю нашого століття це є інформація. Це може бути як інформація простих громадян так і до стратегічних державних програм. В сучасному суспільстві використання новітніх технологій, а саме на основі персональних комп’ютерів, інформаційно обчислювальних мереж і комп’ютеризованих комунікаційних систем забезпечило людству новий етап розвитку і нові види злочинності. Доступ до інформації став набагато швидшим, що спричинило збільшення злочинності.

Нові технології призвели до виникнення нових злочинів, які стали глобальною проблемою аналіз спеціалізованої літератури дозволив до них віднести: розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації, порушення правил експлуатації автоматизованих електронно-обчислювальних систем. Цей тип злочинів називають кіберзлочинами або комп’ютерні злочини [1, с-45].

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання ЕОМ, систем та комп'ютерних мереж» чинного Кримінального кодексу України. 3 квітня 2003 на засіданні Верховної Ради України був прийнятий за основу проект Закону «Про внесення змін до Кримінально-процесуального кодексу України», відповідно до якого будуть розширені можливості Служби безпеки України при розслідуванні порушень в роботі автоматизованих систем. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні. Одним із можливих підходів до боротьби з

кіберзлочинністю у транснаціональному аспекті і розвитку міжнародної співпраці є вироблення і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першими документами у цій сфері стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р., та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [3, с-10].

Прийняття цих актів ознаменувало закладення правового фундаменту у сферу захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання державами, які не є членами Ради Європи. Єфективне міжнародне співробітництво в боротьбі з кіберзлочинністю неможливо, якщо в законодавстві однієї країни діяння вважається злочином, а в іншій – кримінальної відповідальності за це діяння не передбачено. Відсутність однаковості в національному кримінальному законодавстві країн може негативно вплинути на розвиток методів ефективної боротьби з кіберзлочинністю – явищем, для якого не існує державних кордонів. Наявність глобальних інформаційних мереж стирає межі інформаційного простору, а "віртуальні" кордони між державами легко перетинаються кіберзлочинцями, які орудують в будь-якому місці кіберпростору, незалежно від юрисдикції держав, з допомогою комп'ютера й доступу в Інтернет. Ефективне протистояння кіберзлочинності, враховуючи її транскордонний характер, неможливе, якщо розслідування злочинів, видача правопорушників, їх переслідування в суді ускладненні або взагалі нездійсненні через невідповідності національного кримінального законодавства окремих країн [2, с-45].

Виявлення як вид діяльності передує розслідуванню (згідно ЗУ «Про оперативно-розшукову діяльність» (ст.7 ч.3)). Основні засоби та пошукові процедури, які застосовують у процесі виявлення кіберзлочинів, вивчають у курсі оперативно-розшукової діяльності. Сьогодні можна визначити наступних суб'єктів оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів:

1. Національна поліція України (НП), відповідно до § 3 Стратегії кібербезпеки України, належить до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі та здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Як суб'єктів виявлення кіберзлочинів можна структурні підрозділи НП можна поділити на дві групи.

Підрозділи Департаменту кіберполіції (ДКП), які згідно з п. Положення про ДКП НП України, уповноважені щодо протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця сфера діяльності іменується в Положенні «протидія кіберзлочинності». В Україні правові основи боротьби з кіберзлочинами визначаються передусім Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП прямо зобов'язані здійснювати оперативно-розшукову діяльність властивими їм методами з метою протидії конвенційним злочинам (відповідальність за які фактично передбачена ст. 163, 176, 185, 190, 200, 301, 361–363-1 КК України). ДКП є міжрегіональним територіальним органом , юридичною особою публічного права. До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах).

1.2. Інші оперативні підрозділи НП (Департамент карного розшуку, або Департаменту захисту економіки, або Департаменту протидії наркозлочинності тощо), що здійснюють протидію іншим, альтернативним злочинам.

Верховною Радою України 28 січня 2021 року був прийнятий Закон про Бюро економічної безпеки України. Урядом було створено Бюро 12 травня 2021 року, як центральний орган виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Початок діяльності Бюро економічної безпеки було заплановане на 25 листопада 2021 року. Таким чином створення органу з фінансових розслідувань остаточно ліквідує податкову міліцію та підрозділи контррозвідувального захисту інтересів держави у сфері економічної безпеки СБУ. Бюро економічної безпеки аналізуватиме бенефіціарів фінансових операцій і визначатиме, чи є порушення закону в обігу коштів тих чи інших бізнес- або державних структур.

2. Підрозділи контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, захисту національної державності Служби безпеки (ДКІБ СБ України). До завдань СБ України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства,

тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [4, с-10].

Отже, можемо зробити висновок, що сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому ми маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки, оскільки вона є невід'ємним напрямком побудови інформаційного суспільства, розвиток якого повинен йти не лише через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів та забезпечення безпеки держави, у тому числі враховуючи зарубіжний досвід протидії кіберзлочинності в сфері адміністративно-правового забезпечення.

Література:

1. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О. В. Бойченко ; Крим. юрид. ін-т ОДУВС. – Сімферополь : Сімферопол. міська друк., 2009. – 288 с.
2. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – Київ : КНТ, 2007. – 160 с.
3. Конвенція [Ради Європи] про кіберзлочинність : від 23 листоп. 2001 р. ; ратиф. Україною 7 верес. 2005 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.
4. Самойленко О.А. Основи методики розслідування злочинів, вчинену кіберпросторі: монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. - 372 с