

спектру сучасних загроз кібербезпеці держави. Законодавча влада України повина продовжити допрацювання нормативно-правових актів та надати повне тлумачення ключових понять таких як «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфраструктура», «критична кіберінфраструктура», які зможуть ефективно застосовуватись в практиці правоохоронної діяльності.

Література

1. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім «СофтПрес», 2005 – 316 с.
2. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964 – IV // Відомості Верховної Ради України - №39. – 2003 р. – ст. 351.
3. Закон України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638 – IV // Відомості Верховної Ради України - №25. – 2003 р. – ст. 180.

ОСОБЛИВОСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Коваль О.І.

курсант 312 взводу факультету №3

Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.

кандидат юридичних наук, майор поліції

завідувач кафедри кібербезпеки та інформаційного забезпечення

Одеського державного університету внутрішніх справ

Інформаційні злочини - суспільно небезпечні посягання, які зустрічаються все частіше та їх суспільна небезпечність з кожним днем зростає. Це зумовлене прискоренням розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Варто звернути увагу на те, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України (2001року) вперше передбачив самостійний розділ про ці злочини - розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, але потребує вдосконалення хоча б на рівні тлумачення основних понять, таких як: кіберзлочинність, кіберзлочини та інше.

Історія у сфері комп технологій показала, що розвиток і прогрес, супроводжуються не тільки позитивними, а й негативними явищами. Хоча комп'ютеризація спростила процеси, полегшила їх існування та змінила уявлення про роботу, кар'єру, проте вона зробила незахищеним суспільство. Тому вирішення питань, які стосуються комп'ютеризації стали такими актуальними та потребують системного, стратегічного підходу [1, с.134]. Питання кіберзлочинності та аналіз окремих елементів злочинів

пов'язаних з використанням засобів комп'ютерної техніки розглядалися у працях Ю.М. Батуріна, П.Д. Біленчука, В.Б. Вехова, В.О. Голубєва, М.Д. Діхтяренко, Б.Х. Толеубєкова, А.А. Васильєва, О.Г. Волеводза, О.В. Мещерякова, Т.Л. Тропіної та інших науковців.

Злочини у сфері комп'ютерної інформації не мають державних кордонів, тому 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. Не залишилась осторонь і Україна, вона приймає безпосередню участь у боротьбі з кіберзлочинністю [2, с. 71].

На жаль, ступінь загрози, що несуть у собі комп'ютерні злочини, не до кінця ще усвідомлена й оцінена в суспільстві, проте незначний досвід, який вже є в цій галузі, а тим більше досвід найбільш розвинених країн світу, зі всією очевидністю свідчить про уразливість будь-якої держави і злочинець здатний однаково загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Для подолання комп'ютерних злочинів необхідно погоджений міжнародний підхід.

На будь-якому рівні для розслідування кіберзлочинів необхідні добре підготовлені кадри і вдосконалене законодавство для створення ефективної правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з подібними злочинами, а також необхідні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах [3].

Важливим кроком спрямованим на вирішення цієї проблеми, є прийняття Радою Європи 23 листопада 2001 р. Конвенції про кіберзлочинність. Конвенція про кіберзлочинність - перший міжнародний договір у галузі протидії злочинам, що вчиняються через комп'ютерні мережі. Основна мета - проведення загальної політики у сфері кримінального права, спрямованої на захист суспільства від комп'ютерних злочинів.

Форми міжнародної співпраці включають видачу, надання допомоги в галузі права, визнання судових рішень, неофіційна співпраця правоохоронних органів різних країн.

Зважаючи на теперішню ситуацію в галузі міжнародної співпраці виникає ризик утворення міждержавних угруповань, найбільше це стосується співпраці при розслідуванні [4].

Хоча й було здійснено велику кількість спроб щодо більш тісного міжнародного співробітництва, проте на наш погляд варто систематизувати всі версії, які були надані, як науковцями, так і законодавчими органами різних країн та створити більш зручні підходи для тісного контакту між державами у сфері боротьби із кіберзлочинністю.

Міжнародне співробітництво регулюється такими принципами:

1) найширші обсяги співпраці шляхом застосування відповідних міжнародних документів, укладених угод на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства;

2) здійснення співробітництва з метою розслідування або судового переслідування щодо злочинів, пов'язаних з комп'ютерними системами і комп'ютерними даними.

Також не менш важливим є усунення прогалів у міжнародних відносинах, щодо таких питань як:

- 1) доступ до даних без отримання згоди користувача чи власника, але з наступним обов'язковим повідомленням особи чи компетентних органів держави, де знаходиться комп'ютерна система чи дані;
- 2) відсутність регулювання механізму відмови у транскордонному доступі особі, яка володіє законним правом на управління комп'ютерною системою і даними;
- 3) порядок оскарження рішення про збирання комп'ютерних даних при транскордонному доступі;
- 4) захист конфіденційності інформації, отриманої вказаним вище способом;
- 5) судовий та відомчий контроль національних судів і компетентних органів за законністю дій іноземних органів;
- 6) не передбачається можливість проведення транскордонного обшуку у комп'ютерних мережах компетентними органами держави, в якій розслідується комп'ютерний злочин[5].

Підсумовуючи вищезазначене, ми вважаємо, що необхідно створити більш дієвий механізм взаємодії держав у питаннях правової допомоги. Варто також звернути увагу на створення нових та доповнення існуючих нормативно-правових актів для врегулювання всіх прогалин, які існують, проте їх варто не тільки розробити, а й імплементувати в їх національне законодавство, що дозволило б ефективно розслідувати кіберзлочини. А також створити компетентні органи, які будуть виконувати свої функціональні обов'язки на більш високому рівні та матимуть доступ до всієї інформації, необхідної для більш кращого виконання роботи. Не менш важливим є систематизація даних, створення загальних умов на національному рівні для всіх банків, а саме однаковий порядок організації роботи та видачі інформації стосовно певної особи та її рахунку і надання доступу патрульним до даних необхідних для якіснішого виконання ними своїх повноважень.

Таким чином, вирішення проблеми інформаційної безпеки можливо лише за створення та ратифікування документів, які стосуються сфери інформаційної безпеки держав та створення необхідних умов для розслідування цих злочинів.

Література

1. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку / М. В. Карчевський // Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення : матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 61-64.
2. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7.09.2005 № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.
3. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо – поліграфічний центр «Київський університет», 2009. – Вип. 19. – С. 338–342.
4. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Вид. дім «Скіф», 2012. – 736 с.