Проблемні питання та шляхи вдосконалення законодавства України у сфері забезпечення кібербезпеки

Чибиряк М.С.
слухач магістратури 2 курсу Навчально-наукового інституту №3
Національної академії внутрішніх справ
Науковий керівник: Федоровська Н.В.
старший науковий співробітник наукової лабораторії
з проблем забезпечення публічної безпеки та порядку
Навчально-наукового інституту №3 Національної академії внутрішніх справ

Понад двох десятиліть світ живе в інформаційній ері свого розвитку. Інформаційні технології, у наш час, є ключем до технічного та технологічного прогресу практично у всіх сферах діяльності. Швидкий розвиток ІТ-індустрії ставить перед державою нові завдання спрямовані на вдосконалення державного управління у цій сфері діяльності, розроблення нормативно-правової бази, яка б регламентувала діяльність відповідних державних органів, які забезпечують кібербезпеку в нашій державі.

На сьогоднішній день, держава здійснила ряд заходів спрямованих на посилення кібербезпеки, а саме:

1. З 1 липня 2015 року в Державній службі спеціального зв'язку та захисту інформації розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Його завдання – оцінити стан захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади [1].
2. Підписання 23 липня 2015 року Угоди «Про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації». Основна мета – надання фінансово-консультативної та методичної допомоги державами – членами Північноатлантичного альянсу у справі розбудови національної системи кібербезпеки, налагодження взаємодії з відповідними органами іноземних держав та міжнародними організаціями [2].
3. Створення 5 жовтня 2015 року Департамент кіберполіції Національної поліції України, який займається боротьбою із кіберзлочинністю [3, с. 126].

Окрім цього, слід зазначити про створення Стратегії кібербезпеки України, що була введена в дію указом Президента України від 15 березня 2016 року. Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, за якою мають діяти державні органи. Відповідно до даної стратегії Кабінет Міністрів України на поточний рік затверджує план заходів з реалізації Стратегії кібербезпеки України.

Головною метою зазначеної Стратегії є створення умов для безпечного функціонування кіберпростору держави, його використання в інтересах суспільства і особи. Документ також передбачає комплекс заходів, спрямованих на боротьбу із кіберзагрозами, поглиблення міжнародного співробітництва у цій сфері, забезпечення захисту державних електронних інформаційних ресурсів та інформаційної інфраструктури. Задля реалізації цієї стратегії РНБО утворило Національний координаційний центр кібербезпеки як робочий орган Ради [4; 5, с. 330].

На нашу думку, даний документ хоча і називається стратегією, проте він не містить переліку конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними. У нас це нагадує більше концепцію – напрями, куди треба рухатися зі своїми тактиками дій, власним, а не державним, фінансуванням і без ніякої відповідальності. При цьому національна система кібербезпеки має розглядатися як сукупність політичних, соціальних, економічних та інформаційних відносин разом з адміністративними і технологічними заходами, реалізація яких видається можливою тільки у тісній взаємодії державного і приватного секторів, а також розвинутого суспільства.

Ще однією із проблем нормативно- правового регулювання кібербезпеки в Україні є відсутність закріплення в Кримінальному Кодексі України термінології пов'язаною із кібербезпекою, в тому числі поняття «кіберзлочин».

В розділі XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» міститься перелік статей (ст. 361–363-1), що характеризують суспільно-небезпечні діяння, які вчиняються за допомогою електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [6].

Отже, розглядаючи проблематику нормативно-правового регулювання забезпечення кібербезпеки в Україні доцільно його вдосконалювати шляхом:

1. загальнодержавної системи протидії кіберзлочинності;
2. впровадження єдиного понятійного апарату та норм щодо кваліфікації комп'ютерних злочинів;
3. запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту [7, с. 128].

Підсумовуючи, слід зазначити, що кіберпростір, на сьогоднішній день, відіграє велику роль у забезпеченні інформаційної безпеки людини, суспільства, держави. І тому, державні органи повинні впроваджувати та удосконалювати нормативно-правову базу, яка регламентує діяльність правоохоронних органів та військових формувань. Адже від їхньої діяльності залежить безпека громадян інформаційному рівні.

Література:

1. У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам (02.07.2015). Державної служби спеціального зв'язку та захисту інформації України [сайт]. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=64E6106BCAE5A1B937A4E8DC156F33D6.app1?art_id=156473&cat_id=119123
2. Угода про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації від 23.07.2015р. // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/642_063 (дата звернення: 07.11.2017).
3. Сабіщенко О.В. Мокрієв М.В. Перспективи розвитку кіберпростору та напрями забезпечення кібербезпеки України. Новий погляд на розвиток економіки країни. Матеріали Міжнародної науково-практичної конференції (м. Львів, 25-26 березня 2016 року). – Херсон: Видавничий дім «Гельветика», 2016. – 156 с. – С. 125–129.
4. Стратегія кібербезпеки України: затвердж. указом Президента України №96/2016р. «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року» / База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/96/2016 (дата звернення: 07.11.2017).
5. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ України. 2016. Вип. 26.8. - С. 327–336.
6. Кримінальний Кодекс України: Закон від 05.04.2001 № 2341-III // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page11 (дата звернення: 07.11.2017).
7. Пестова К.В., Кравчук В.В. Т- законодавство: проблеми, пріоритети та напрями розвитку. ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. - С. 126–133.

Аспекти кібербезпеки України

Щирська В.С.
капітан поліції, кандидат юридичних наук
інспектор Херсонського факультету ОДУВС

Одним із основних завдань політичного керівництва будьякої держави є забезпечення гарантованого функціонування відкритого, надійного та захищеного кіберпростору. Через відсутність кордонів у кіберпросторі, а також відкритість, покладену в основу сучасних інтернет-технологій, та анонімність значно зростає кількість зовнішніх кібератак та кіберзагроз, що автоматично призводить до необхідності розробки чіткої стратегічної концепції як ідейної основи формування пріоритетів національної політики в кіберпросторі. Інакше кажучи, глобальний характер кіберпростору здатний підвищити ступінь ризику, впливаючи як на державний, так і на приватний сектор. Тому останнім часом у світі актуалізувалася проблема розробки концептуальних засад формування дієвого захисту кіберпростору та елементів системи стратегічних комунікацій сектору безпеки і оборони від загроз несанкціонованого втручання.

Практично безмежні можливості Інтернету підтверджують глобальну загрозу віртуальних злочинів, кібертероризму та ведення кібервійни в сучасних умовах. Широке використання