

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 Трестового 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

інформаційно-комунікаційних технологій (ІКТ) в економічній, науково-технічній, інформаційній сферах, у сфері державного управління, в оборонно-промисловому і транспортному комплексах та їхніх критичних об'єктах, у національній системі зв'язку, секторі безпеки і оборони, робить їх уразливими з позиції розвідувально-підривної діяльності з боку окремих держав, їхніх спецслужб або хакерських угруповань у кіберпросторі. Реалії сучасності переконливо доводять, що важливою складовою національної безпеки виступає саме кібербезпека держави та її забезпечення.

На сьогодні триває процес розбудови національної системи кібербезпеки і кіберзахисту, формування її організаційно-технічної моделі, здатної забезпечити оперативне і адекватне реагування на потенційні та реальні кіберзагрози. Проте в Україні лише розпочинає формуватися розуміння масштабів та наслідків сучасних кіберзагроз, необхідності забезпечення максимально захищеного кіберпростору.

Хоча, за останні 5–7 років глобальний кіберпростір усе більшою мірою розглядається всіма державами світу, як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. Стає все очевиднішою і подальша мілітаризація кіберпростору, а зусилля окремих держав, що намагаються попередити цей процес, вочевидь, малоефективні та залишаються такими ще тривалий час. Можна з упевненістю говорити, що нині кіберпростір переживає час «неосередньовіччя» з усіма його атрибутами: відсутність чіткого міжнародного права, розбудова системи відносин «клієнтпатрон», формування своєрідних «феодалних угідь» в інформаційній сфері. Однак якщо в класичному середньовіччі це було пов'язано передусім із питаннями земельної власності, то тепер ми маємо справу з кіберпростором. Як слушно відзначає Б. Шнаєр, «ми маємо справу із феодальною моделлю. Користувачі заявляють про свою вірність більш могутнім компаніям, які, своєю чергою, обіцяють їх захистити від тягара системного адміністрування та загроз безпеці» [1]. Цими «новими феодалами» стають потужні ІТ-ТНК на кшталт Apple, Google, Microsoft, Facebook та ін. Водночас сучасний кіберпростір і ті процеси, які нині відбуваються в ньому, значно нагадують проблеми часів холодної війни, для якої були характерні високі рівні латентних загострень на міжнародній арені, непрямі методи боротьби перенесення конфліктів на територію третіх країн та гонка озброєнь (у даному випадку – «кіберозброєнь»).

У таких умовах виняткового значення для забезпечення національних інтересів та їх захисту на міжнародному рівні набуває ефективність механізмів забезпечення кібербезпеки держави та вирішення тих проблем, які виникають на шляху їх розбудови. Національна безпека та її складники – Стратегічні пріоритети.

Стратегічні аспекти кібербезпеки України В Україні ці механізми все ще знаходяться на етапах становлення. Деякі з них потребують вдосконалення, однак для розробки більшості та їхніх окремих елементів передусім бракує концептуального обґрунтування. Крім того, в Україні досі відсутні критично важливі елементи національної системи кібербезпеки в належному системному укомплектованому ієрархічному розподілі структурованого підрозділу.

Відповідно, зумовлена необхідністю подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та часткової готовності Української держави відповісти на новітні кібербезпекові виклики. Серед дослідників, які системно досліджують питання кібербезпеки (в тому числі в контексті реалізації зовнішньої політики держав у сучасних умовах) варто виділити праці таких, як М. Лібіцкі, Дж. Най, Г. Раттрей, Дж. Шелдон, К. Демчак, П. Домбровський, С. Старр, А. Клімбург, М. Шмідт, Дж. Льюїс та ін. Серед вітчизняних учених відзначимо передусім дослідження М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева, В. Бутузова, О. Довганя та ін.

Попри те, що останніми роками тематика кібербезпеки в Україні все частіше артикулюється на найвищому державницькому рівні, реальні заходи в цій сфері все ще залишаються багато в чому фрагментарними та несистемними. Концептуально проблема розбудови ефективних механізмів кібербезпеки Української держави походить від відсутності законодавчо визначених термінів, що описують цю сферу. Не останньою чергою ця проблема є наслідком недосконалого чинного законодавства, а також до певної міри – своєрідною традицією штучного розширення предмету інформаційної безпеки на максимальну кількість сфер. Насамперед відзначимо, що самі терміни із префіксом «кібер» фактично не зустрічаються в нормативно-правових документах України. Натомість у дусі пострадянської наукової (а до певної міри і політичної) традиції значно ширше використовується поняття «інформаційна безпека» та низка інших, що тісно пов'язані з «інформаційним» складником, понять: «інформаційний суверенітет», «інформаційна інфраструктура», «інформаційні впливи» тощо.

При цьому зазвичай посилаються на ст. 17 Конституції України [2, с. 3], в якій зазначено, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу». Водночас таке

твердження в Основному Законі має як свої переваги, так і недоліки. З одного боку, наявність офіційно закріпленого змісту поняття «інформаційна безпека» дозволяє активно використовувати його в інших нормативно-правових документах. З іншого, саме закріплення конструкції «інформаційна безпека» часто суттєво ускладнює внесення змін до чинного законодавства, і особливо яскраво це проявляється саме у кібербезпековій проблематиці. Крім того, відсутність чіткого розуміння того, чим власне є «інформаційна безпека», призводить до того, що її предметна сфера штучно розширюється на дуже великий діапазон цілей: починаючи від іміджу держави, забезпечення інформаційних прав громадян і до боротьби з корупцією. Серед іншого до «інформаційної безпеки» відносять і ті її аспекти, які в західній науковій та юридичній практиці прийнято відносити саме до проблем кібербезпеки. Передусім – це протидія комп'ютерній злочинності та комп'ютерному тероризму. До речі, жодне з цих понять не визначене в повній мірі в національному законодавстві, відповідно не зрозуміло, з чим, власне, пропонується боротись і як вирішувати данні протиправні діяння з точки зору закону.

Важливу частину роботи з убезпечення громадян від найбільш розповсюджених кіберзлочинів здійснює НП України. У його структурі створено спеціальне Управління боротьби з кіберзлочинністю, на яке покладено низку завдань. Зокрема, до основних завдань Управління відноситься організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються з використанням інформаційних технологій та телекомунікаційних мереж (у сфері інформаційно-телекомунікаційних технологій, у сфері електронних платежів і господарської діяльності, зокрема, порушення прав інтелектуальної власності та заняття гральним бізнесом, злочини проти інформаційної безпеки, у тому числі незаконні дії зі спеціальними технічними засобами негласного отримання інформації), а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень [3].

Державна служба спеціального зв'язку та захисту інформації відповідно до своїх завдань безпосередньо включена до забезпечення кібербезпеки держави. Зокрема, серед її профільних завдань визначено:

- забезпечення формування і реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування. Стратегічні аспекти кібербезпеки України розроблені та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

- забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

- здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, а також за додержанням технічних вимог керівних документів у сфері надання послуг електронного цифрового підпису;

- розроблення та здійснення заходів щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності і сталого функціонування [4].

Таким чином, для України залишається актуальною низка проблемних питань, вирішення яких потребуватиме часу та певних зусиль з боку держави. Від ефективності їх вирішення залежатиме те, якою мірою Українська держава зможе ефективно відповісти на сучасні виклики, і зокрема кібербезпекові. Більшою мірою ці проблеми потребують вирішення або в інституційній, або нормативно-правовій площині, однак суттєва їх частина безпосередньо пов'язана із проблемою вироблення взаємної довіри у взаємовідносинах трикутника «держава – закон – громадяни».

Література:

1. The Battle for Power on the Internet [Електронний ресурс]. – Режим доступу: <http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>
2. Конституція України. Прийнята на 5 сесії Верховної Ради України 28.06.1996 р. – К., 1996. – 119 с.
3. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: <http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754>
4. Основні завдання Державної служби спеціального зв'язку та захисту інформації України // Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=89831&