УДК 323:351

СТРАТЕГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Дубов Дмитро Володимирович,
кандидат політичних наук, старший науковий співробітник

Розглянуто ключові проблеми розвитку кібербезпекового сектору України. Сформульовано основні проблеми на шляху його розбудови як ефективного механізму захисту національних інтересів держави в сучасному світі. Акцентовано увагу на необхідності вироблення спільного бачення кібербезпекових проблем як державними органами, так і бізнес-структурами.

***Ключові слова*: кібербезпека, механізми забезпечення, неурядові організації, бізнес.**

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 залишаться 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 «клієнт-патрон», формування своєрідних «феодальних 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 тягаря 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 (передусім активізація розвідувальної діяльності всіх сторін глобального протистояння), перенесення конфліктів на територію третіх країн (наприклад у формі протистоянь за сфери впливу) 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.

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.

Відповідно, актуальність дослідження даної теми 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. Льюіс та ін. Серед вітчизняних учених відзначимо передусім дослідження М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева, В. Бутузова, О. Довганя та ін.

Метою даної статті є визначення ключових стратегічних проблем і шляхів їх вирішення задля розбудови ефективних механізмів забезпечення кібербезпеки України.

Попри те, що останніми роками (особливо протягом 2011–2013 рр.) 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 [11], 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 досі не визначене в національному законодавстві, відповідно не зрозуміло, з чим, власне, пропонується боротись.

Інший показовий приклад неоднозначності нормативно-правового вирішення проблем інформаційної сфери – визначення змісту поняття «інформаційний суверенітет». Його становлення визнано одним із пріоритетів державної політики. При цьому Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР визначає його [12] як «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» (ст. 1). Однак це правильне за своєю сутністю визначення в умовах сучасного розвитку інформаційних технологій стає беззмістовним, оскільки, по-перше, не пояснено суть «інформаційних потоків», що дозволяє включати сюди майже будь-що, а по-друге, залишається незрозумілим, що саме має розумітись під «інформацією з-поза меж держави», а відповідно як саме має здійснюватись «контроль і регулювання».

Майже аналогічний підхід до «інформаційної безпеки» спостерігається і в Доктрині інформаційної безпеки України [2], яка пропонує доволі еклектичний набір загроз інформаційній безпеці України, починаючи від «поширення у світовому інформаційному

просторі викривленої, недостовірної та упередженої інформації» та «негативних інформаційних впливів», «недосконалості партійно-політичної системи, непрозорості політичної та громадської діяльності» і аж до «відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав». Таким чином, згідно із Доктриною «інформаційна безпека» стає всеосяжною, яка охоплює будь-які сфери людського буття. Маємо зазначити, що подібне розуміння змісту даного поняття спостерігається не лише в Україні, а й у більшості країн пострадянського простору.

Водночас у вітчизняному нормативно-правовому полі визначення поняття «інформаційна безпека» зафіксоване у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [13]. У ньому під інформаційною безпекою розуміється «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Внесення в дане визначення проблеми «негативних інформаційних впливів», на нашу думку, багато в чому розмиває поле «інформаційної безпеки», що дозволяє постійно включати до нього нові елементи безпекової сфери, штучно розмиваючи предметне поле цього поняття.

У європейському ж (а власне, і вже традиційному для світової спільноти) розумінні зміст поняття «інформаційна безпека» викладений в оновленій редакції Стратегії національної безпеки України «Україна у світі, що змінюється» [14], яка більшою мірою зосереджується на кібербезпеці та навіть артикулює завдання створення національної системи кібербезпеки.

Не можна сказати, що кібербезпека в Україні перебуває поза увагою інституцій безпекового сектору. Говорячи про механізми практичного забезпечення кібербезпеки держави, ми передусім звертаємо увагу на зусилля декількох основних відомств.

Традиційно у структурі Служби безпеки України захист інтересів держави у сфері інформаційної безпеки покладався на Департамент контррозвідувальної діяльності, однак у 2012 р. Указом Президента України [17] було створено спеціальний Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, до основних завдань якого має відноситись «сприяння концентрації сил та засобів, вирішення завдань із захисту законних інтересів держави і прав громадян в інформаційній сфері від розвідувально-підривної діяльності іноземних спецслужб, протиправних посягань організацій, груп та осіб» [3].

Про увагу СБУ до проблематики кібербезпеки свідчить і те, що ця загроза все частіше згадується у виступах її очільників. Так, в одному з інтерв'ю екс-голова Служби безпеки України І. Калінін, зазначив, що «статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів» [4].

Важливу частину роботи з убезпечення громадян від найбільш розповсюджених кіберзлочинів здійснює МВС. 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 [5].

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,

розробленні 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 [6].

У структурі Міністерства оборони України принаймні два основних управління відповідають за питання, що пов'язані з кібербезпекою держави. Так, в Апараті МОУ цією діяльністю опікується Управління інформаційних технологій, що підпорядковане заступнику Міністра оборони України – керівнику апарату. В Генеральному штабі Збройних сил України функціонує Головне управління зв'язку та інформаційних систем, на які серед іншого покладено такі обов'язки:

– організація зв'язку і автоматизованого управління військами у ЗСУ та здійснення оперативного управління телекомунікаційними мережами України в інтересах оборони держави;

– підготовка системи зв'язку і автоматизації управління військами ЗСУ та контроль за підготовкою телекомунікаційних мереж України в інтересах оборони держави;

– участь у реалізації державної політики у сфері захисту інформації та протидії кіберзагрозам в інформаційно-телекомунікаційних системах ЗСУ;

– участь у військовому співробітництві з питань, пов'язаних із розвитком системи та засобів зв'язку ЗСУ, захисту інформації та протидії кіберзагрозам [7].

Крім того, у структурі МОУ функціонує Головне управління розвідки, на яке покладено завдання здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, воєнній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково-технічного розвитку, захисту та охорони державного кордону [8].

Водночас не можемо не відзначити, що кібербезпекова тематика лише побіжно згадується у стратегічних документах воєнного сектору. Наприклад, Воєнна доктрина України [9] згадує кібернетичний складник лише у двох випадках. Уперше в контексті поширення тероризму (в тому числі – «кібертероризму»), а вдруге – у переліку дій, які Україна вважає необхідними умовами для виникнення воєнного конфлікту та застосування воєнної сили. Йдеться про «проведення акцій, що порушують безпеку функціонування об'єктів ядерної, хімічної промисловості, оборонно-промислового комплексу, об'єктів, на яких зберігаються озброєння, військова техніка, боєприпаси, інших потенційно небезпечних об'єктів, у тому числі кібернетичних атак на зазначені об'єкти».

Майже в аналогічному обсязі приділено увагу цьому питанню у Стратегічному оборонному бюлетені України [10]. Зокрема, кібернетичні загрози виділені як один із прогнозних викликів національній безпеці України на довгостроковий період. Крім того, зазначається необхідність «забезпечення високого ступеня захисту та живучості систем управління, військ (сил) і важливих об'єктів від ударів різноманітних засобів ураження, насамперед високоточної зброї, від диверсій, радіоелектронних перешкод, інформаційного впливу, у тому числі кібернетичних атак».

Незважаючи на подібну розгалуженість відомств, що задіяні в системі забезпечення кібербезпеки держави, вітчизняній кібербезпековій сфері притаманні певні стратегічні проблеми, які все ще потребують вирішення. Причому про майже аналогічні проблеми йшлося ще 2–3 роки тому [18], однак ситуація й досі принципово не змінилась.

Передусім ідеться про очевидну проблему **відсутності однозначного розуміння того стану, в якому перебуває умовний «вітчизняний кібербезпековий сектор»**. Вочевидь, перед тим, як здійснювати справді масштабні та стратегічно значущі кроки в цій сфері, доцільним було б здійснити його принциповий огляд, який би вказав на системні проблеми та можливі шляхи їх вирішення, зміг би виявити дублювання функцій відомств (або не притаманні певним відомствам функції), чи навпаки – які елементи кібербезпекової сфери залишились поза увагою сектору безпеки.

Оскільки питання кібербезпеки відносно нове для України та зачіпає інтереси не лише державних інституцій, а й приватного сектору та громадянського суспільства, видається доцільним піти в даному випадку шляхом, який пропонує європейська практика. Зокрема, спо-

чатку варто підготувати «Зелену книгу», яка має поставити на широке обговорення дане питання та привернути увагу до нього більш широких верств громадян, а потім і «Білу книгу», яка дасть ключові відповіді на проблемні питання та визначить шляхи їх вирішення.

Щоправда, маємо визнати, що у вітчизняній практиці подібні механізми вироблення політики з певного питання є відносно новими та не завжди успішними – українські державні структури хоч і мають певну практику написання «Білих книг» (особливо з питань реформування державних органів), однак їх реальний вплив на здійснення змін незначний. Це можна пояснити, в тому числі, відсутністю усталеної практики наступності політики, що проводилась попередніми керівниками державних органів.

Своєрідним наслідком відсутності цілісного обговорення кібербезпекових питань у ширшому колі є і проблема того, що **в Україні досі відсутні системні нормативні документи, які описували б загрози Україні саме в кіберпросторі, визнали б їх і стали основою для цілісної державної політики з кібербезпеки.** Досить умовно чи не єдиним документом, у якому прямо йдеться про кіберзагрози, – це ратифікована Верховною Радою України Конвенція про кіберзлочинність [15]. Однак, по-перше, сама Конвенція, хоч і стосується проблеми убезпечення кіберпростору, проте зосереджена більше на протидії карним діянням (шахрайство, підроблення, поширення дитячої порнографії, порушення авторських прав тощо) з використанням комп'ютерної техніки та різноманітних мереж, а по-друге, в Конвенції відсутнє визначення терміна «кіберзлочинність». І хоча нова редакція Стратегії національної безпеки вже враховує кібербезпекову проблематику, в Україні все ще відсутня цілісна термінологічна система, що сформувала б єдиний термінологічний апарат у сфері кібербезпеки.

Останнім часом розпочалися процеси щодо унормування даної проблеми та пошуку шляхів її вирішення, зокрема через створення відповідних нормативних документів. На нашу думку, пріоритетним тут залишається створення та прийняття принаймні Стратегії забезпечення кібернетичної безпеки України, зобов'язання щодо розробки якої Україна вже брала на себе перед закордонними партнерами. Цей документ має визначити зміст основних понять у даній сфері, загрози, принципи та напрями забезпечення кібернетичної безпеки, зокрема заходи з удосконалення державного управління та нормативно-правового поля у сфері кіберзахисту. Це той шлях, яким активно йдуть провідні країни світу, і передусім країни-члени НАТО.

Крім суто нормативно-правової проблеми, спостерігається й очевидний брак міжвідомчої координації з питань забезпечення кібербезпеки держави. На жаль, досі в Україні **відсутні загальнонаціональні міжвідомчі координаційні структури**, що могли б узгоджувати та координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створення ефективної системи захисту вітчизняного кіберпростору (в тому числі у військовій сфері). Співпраця існує швидше не на системному (чітко визначеному), а неформальному (міжособистісному) рівні, а отже, є уразливою з точки зору довгострокової перспективи.

Такі координуючі функції могла б узяти на себе або Рада національної безпеки і оборони України (через свої структури), або спеціально створений державний орган (до чого схиляється все більше експертів).

Певні сподівання були на відновлення повноцінної роботи Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України, однак вона досі, незважаючи на окремі ініціативи, так і не стала ефективно діючим майданчиком для обговорення зазначених проблем.

Кібербезпека – це передусім людський ресурс, однак більшість представників відомств, задіяних у системі забезпечення кібербезпеки України, відзначають **незадовільне кадрове забезпечення відомств відповідними фахівцями** у сфері кібернетичної безпеки. Незважаючи на те, що низка вищих навчальних закладів (військових, цивільних та відомчих) здійснюють підготовку фахівців за різноманітними ІТ-спеціальностями, якість їх підготовки багато в чому є незадовільною, а силові структури все ще не мають реальних можливостей залучити молодих спеціалістів високого класу до своїх структур передусім через брак матеріальних і нематеріальних стимулів.

Ще однією проблемою є те, що, незважаючи на зусилля спеціально уповноважених відомств, **Україна досі залишається принципово уразливою у сфері використання сучасних ІТ, й не останньою чергою через надмірно широке запровадження іноземних програмних продуктів та використання матеріально-технічної бази іноземного виробництва**. І це при тому, що з кожним роком зростає занепокоєність провідних держав світу в тому, що різноманітні «закладки» можуть з'являтись навіть не на рівні програмних продуктів, а наприклад, процесорів, які можуть бути уражені ще під час виробництва. Однак

навіть у програмних продуктах вкрай складно віднайти відповідні «не документовані можливості», що створює загрозливий рівень залежності Української держави від подібних продуктів. Актуальними залишаються проблеми створення національної операційної системи (принаймні для використання у системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку вітчизняних безпекових організацій), відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

Фактично ж **ідеться про побудову повноцінного кібернетичного суверенітету держави, без якого ми будемо змушені весь час залишатись в умовах наздоганяючих трансформацій безпекового сектору**. Тим більше, що створення цих елементів є принциповим складником цифрового суверенітету держави, а в подальшому – її кібермогутності.

Ще одне питання, характерне не лише для України, а й для всього пострадянського простору, – це **традиційно низька взаємодія органів державної влади та приватного сектору, а також з неурядовими організаціями**. Однак якщо ми говоримо про загальні питання обороноздатності країни чи інші традиційні сфери державного управління, де подібна взаємодія налагоджена в межах інституційних форм співробітництва, то у сфері кібербезпеки вона лише з'являється.

Водночас саме це питання стає чи не ключовим, зважаючи на те, що **значна кількість інформаційної інфраструктури (в т.ч. критичної) перебуває у приватній власності**, а нині навіть пересічні громадяни відіграють усе більшу роль у забезпеченні кібербезпеки держави. Інституалізація такої поліаспектної взаємодії у трикутнику «держава – бізнес – суспільство (неурядові організації)» в жодній країні не відбувається безболісно, оскільки, з одного боку, виникають питання щодо припустимих меж втручання держави в діяльність приватних структур і життя пересічних громадян, а з іншого – відповідальності бізнесу за загальну безпеку держави та громадян. Однак логіка останніх подій (передусім випадки масштабних кібератак і викривальні заяви, наприклад, Е. Сноудена) говорить про те, що цей баланс поступово зміщується саме в бік ширшої участі держави, однак при одночасному посиленні її зобов'язань перед своїми громадянами та бізнес-структурами.

При цьому маємо зазначити, що всі найбільш кіберпотужні держави не просто розуміють необхідність залучення «третього сектору», а й активно сприяють цьому процесу. Показовим прикладом такого взаємопроникнення є проект *FIRST*[1] – комерційний проект, з яким активно співпрацюють і державні структури в межах окремих *CERT*[2]-ів.

Крім того, все більшу роль у глобальних протистояннях у кіберпросторі, й передусім у відстеженні та подальшому аналізі кібератак, відіграють різноманітні **приватні безпекові організації,** які часто поєднують свою основну діяльність з виробництвом антивірусних продуктів. Серед таких компаній відзначимо *McAfee, Avast, Kaspersky Lab, ESET, F-Secure* та ін. Саме вони завдяки більшій свободі у своїй діяльності все частіше стають викривальниками масштабних кібероперацій, у т.ч. таких, як *Stuxnet, Flame, Red Octobr*. В Україні організацій подібного масштабу немає, а чи не єдиний антивірус національного виробництва (*Zillya!*) лише намагається увійти на цей ринок.

Варто пам'ятати, що в **Україні відсутні й мінімально потужні ІТ-ТНК** (хоча б рівня *Mail.ru* чи *Yandex*), на які припадає значна частина задоволення інформаційних потреб громадян, а отже, і можливостей ефективно впливати на їх безпеку. Україна так і не змогла напрацювати реальних механізмів, які дозволили б ефективно підтримувати обдарованих українських фахівців та сприяти їх виходу на міжнародний ринок. На противагу цьому окремі державні керівники хизуються аж ніяк не позитивним фактом зростання аутсорсингового потенціалу держави.

Питання взаємодії з приватним сектором пов'язане і з тим, що для кібератак характерна значна латентність. Відповідно, якщо компанії самі не повідомлятимуть про них урядові структури, ті тривалий час можуть нічого не знати про проведення такої атаки та не вживати необхідних заходів. Це пов'язано з тим, що існують **проблеми взаємної довіри між бізнесом і державними інституціями**

[1] *Forum of Incident Response and Security Teams* – Форум команд реагування на інциденти безпеки. Форум як постійно діюча структура створений у 1990 р., після перших масових проблем із розповсюдженням вірусів на міжнародному рівні.

[2] *Computer Emergency Response Team of Ukraine* – команда реагування на комп'ютерні надзвичайні події. В Україні функціонує на базі Державного центру захисту інформаційних ресурсів Державної служби спеціального зв'язку та захисту інформації України.

й передусім упевненість перших у тому, що другі не передадуть дані про кібератаки на компанії або третім особам, або просто не нададуть їм гласності.

Важливість цієї проблеми продемонстрували кроки уряду США, які окремими нормативними документами фактично примусили приватні компанії сповіщати уряд про атаки на них. Водночас уряд США намагався впорядкувати це питання через законодавчі механізми: при підготовці *Cybersecurity Act 2012* питанню спеціального центру, куди має потрапляти подібна інформація, було присвячено дуже багато уваги.

Не можемо не відзначити, що в Україні під час розробки різноманітних проектів Закону України «Про кібернетичну безпеку» саме питання взаємовідносин між структурами сектору безпеки та приватним сектором/неурядовими організаціями (НУО) були виписані мінімально, а в окремих випадках їх взагалі намагались ігнорувати.

Однак не лише бізнес-сектор є важливим для забезпечення кібербезпеки держави. НУО також можуть впливати на його посилення. Наприклад, через можливість здійснення зовнішніх, незалежних досліджень у цій сфері, що допоможе приймати урядовим структурам більш виважені рішення, ґрунтуючись на широкому масиві експертних думок. Наприклад, у США документ «Убезпечення кіберпростору для 44-го президентства» [16], що був підготовлений для нового президента США Б. Обами фахівцями Центру стратегічних та міжнародних досліджень, справді суттєво вплинув на політику Білого дому й неодноразово згадувався в урядових матеріалах, присвячених кібербезпековій проблематиці. Той же центр продемонстрував й іншу реальну можливість задіяності НУО: за його ініціативи та посередництва вже декілька років проводяться кібернавчання між військовими США та КНР.

На жаль, для України ця сфера державно-приватного партнерства залишається чи не найбільш нереалізованою. Однак і тут спостерігаються певні національні особливості. Проблема в тому, що в Україні фактично відсутні дійсно фахові НУО безпекового спрямування, а ті, що є, мають занадто широку сферу діяльності, що унеможливлює побудову конструктивних відносин з ними саме в контексті проблем кібербезпеки. В окремих випадках при підготовці таких матеріалів профільними НУО спостерігаємо і низький рівень цих матеріалів. Водночас українські НУО експертного спрямування так і не змогли напрацювати дійсно ефективні механізми донесення своїх розробок і пропозицій до посадових осіб.

Таким чином, для України залишається актуальною низка проблемних питань, вирішення яких потребуватиме часу та певних зусиль як з боку держави, так і бізнесу/НУО. 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 – бізнес – громадяни».

Список використаних джерел

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. *Про Доктрину* інформаційної безпеки України : указ Президента України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009
3. *Пояснювальна* записка до проекту Закону України «Про внесення змін до деяких законів України щодо структури та порядку обліку кадрів Служби безпеки України» // Верховна Рада України [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1? pf3511=41867
4. *СБУ :* Головні проблеми для України – тероризм і кіберзлочинність // Українська Правда [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/
5. *Управління* боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754
6. *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&cat_id=89828
7. *Головне* управління зв'язку та інформаційних систем Генерального штабу Збройних сил України // Міністерство оборони України [Електронний ресурс]. – Режим доступу: http://www.mil.gov.ua/index.php?part=department&lang=ua&sub=guz_is

8. *Напрями* діяльності ГУР МОУ // Головне управління розвідки Міністерства оборони України [Електронний ресурс]. – Режим доступу: http://www.gur.mil.gov.ua/content/directions.html

9. *Про Воєнну* доктрину України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/648/2004/print1361272038412688

10. *Про Стратегічний* оборонний бюлетень України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/771/2012/print1361272038412688

11. *Конституція* України. Прийнята на 5 сесії Верховної Ради України 28.06.1996 р. – К., 1996. – 119 с.

12. *Про Національну* програму інформатизації : закон України від 4.02.1998 р. №74/98-ВР [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/74/98-%D0 %B2 %D1 %80

13. *Про Основні* засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537–16

14. *Про Стратегію* національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007

15. *Конвенція* про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

16. *Securing* Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies [Електронний ресурс]. – Режим доступу: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

17. *Про внесення* зміни до Указу Президента України від 27.12.2005 р. № 1860 : указ Президента України від 25.01.2012 р. № 34/2012 // Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/34/2012

18. *Дубов Д. В.* Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.