

УДК 343.9:343.346.8:004

ГРЕБЕНЮК М.В., кандидат юридичних наук, доцент,
керівник Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю при РНБО України
ЛЕОНОВ Б.Д., доктор юридичних наук, старший науковий співробітник,
головний науковий співробітник Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю при РНБО України

ДОСВІД ІЗРАЇЛЮ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. У статті аналізується досвід держави Ізраїль у сфері забезпечення кібербезпеки. Висвітлюється система органів, які відповідають за кібербезпеку. Аналізуються законодавчі ініціативи держави Ізраїль у сфері забезпечення кібербезпеки.

Ключові слова: Ізраїль, кібербезпека, кібертероризм.

Summary. The article analyzes the experience of Israel in the field of providing cyber security. The system of bodies responsible for cyber security is covered. The legislative initiatives of Israel in the field of ensuring cyber security are analyzed.

Keywords: Israel, cybersecurity, cyberterrorism.

Аннотация. В статье анализируется опыт Израиля в области обеспечения кибербезопасности. Освещается система органов, ответственных за кибербезопасность. Анализируются законодательные инициативы государства Израиль в области обеспечения кибербезопасности.

Ключевые слова: Израиль, кибербезопасность, кибертерроризм.

Постановка проблеми. Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави [1]. Кібербезпека – це сфера майбутнього, яка потребує вкладення потужних державних та приватних інвестицій на перманентній основі. Розвиток цієї важливої складової світової національної безпеки є одним із головних чинників прискорення галузевої трансформації усїєї світової економіки в найближчі десятиліття. Таким чином, у найближчій перспективі сфера кібербезпеки має стати ключовим параметром визначення рівня економічного розвитку будь-якої країни, її конкурентоспроможності на глобальному ринку.

Феномен кіберпростору пов'язаний з тим, що, з одного боку, він тісно поєднаний з технічною складовою (інформаційно-телекомунікаційні мережі), а з іншого – можливості, які він надає завдяки своїй експлуатації, дедалі більше виводять його за межі суто технічних аспектів кібербезпеки, оскільки від цього залежить стабільність світової економіки, безпека людей, суспільний розвиток, а зрештою – і безпека держав в широкому розумінні [2, с. 7-8].

Результати аналізу наукових публікацій. Вагомий внесок у дослідження кібербезпеки зробили такі зарубіжні вчені, як Д. Шелдон, Г. Раттрей, П. Домровський, Дж. Наямол, С. Старр, А. Клімбург.

Проблема кібертероризму дедалі активніше досліджується і вітчизняними вченими. Окремі аспекти цього феномену висвітлені у працях Д. Дубова, В. Пилипчука, В. Петрова, М. Ожевана, М. Погорецького.

Однак в науковій літературі відсутні системні наукові дослідження, присвячені вивченню досвіду Ізраїлю у сфері забезпечення кібербезпеки в контексті удосконалення вітчизняної моделі кібербезпеки.

Метою статті є аналіз передового досвіду держави Ізраїль у сфері забезпечення кібербезпеки для його використання правоохоронними органами України.

Виклад основного матеріалу. Особливістю кіберпростору є його самоочевидна екстериторіальність, хоча дедалі більше держав ставить на міжнародному рівні питання щодо необхідності проведення кордонів та встановлення принципів національно-державного суверенітету і в цьому специфічному “просторі”. Провідні світові держави включаються в процес нарощування своїх потенціалів ведення агресивних дій в кіберпросторі, де-факто збільшуючи свою кібермогутність. Це має прояв у спробах вироблення та застосування дедалі складніших програмних комплексів, основним завданням яких є саме заподіяння шкоди об’єктам атаки [2, с. 8-9]. За оцінкою експертів, світовий ринок кібербезпеки дорівнює \$ 1 млрд. а до 2021 року цей показник може збільшитися до \$ 200 млрд. На цьому фоні найбільші темпи збільшення інвестицій у цю сферу демонструє Ізраїль, на частку якого припадає 15 % світових надходжень у розвиток кібербезпеки. Також світовий досвід демонструє, що сьогодні сфера забезпечення кібербезпеки виходить за межі юрисдикції певних країн і має глобальний та міжнародний характер, що зумовлює потребу в розробці не тільки національної, а й відповідної міжнародної стратегії забезпечення безпеки у кіберпросторі. Все це призводить до того, що кіберпростір зазнає випробувань спробами його мілітаризації. Геополітичні суб’єкти розуміють загрозовість процесу стрімкої мілітаризації кіберпростору та намагаються віднайти механізми уникнення масштабних бойових дій в кіберпросторі, наслідком яких можуть стати атаки, спрямовані проти критичної інфраструктури держави з непередбачуваними наслідками. З метою недопущення цього небажаного сценарію розвитку подій, провідні держави розпочали низку діалогів різних рівнів, а також формують власні цілісні стратегії поведінки в кіберпросторі [2, с. 7-8].

Сьогодні провідні держави світу в цілому дедалі більше покладаються, і відповідно залежать від безперешкодного функціонування кіберпростору, при цьому захист інтересів держав та громадян у кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ- мереж на питання безпеки і оборони, оскільки фактори потенційної небезпеки можуть загрожувати системам державного та військового управління, економіки та промисловості [3, с. 37-38]. Невипадково в багатьох провідних країнах світу вже сформовані загальнодержавні системи кібербезпеки – як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [4, с. 175].

За таких умов актуальним та своєчасним є висвітлення прогресивного досвіду держави Ізраїль щодо організаційно-правового забезпечення побудови національної системи кібербезпеки, враховуючи також провідні позиції цієї країни у світових рейтингах. Небезпідставно відповідно до індексу конкурентоспроможності-2016 (опублікованого IMD World Competitiveness Center [5]) серед 61-єї країни в питаннях

забезпечення кібербезпеки переможцем визнано саме Ізраїль. Сьогодні інфраструктура сфери кібербезпеки Ізраїлю включає приблизно 450 компаній, у тому числі вже відомі фірми, такі як Check Point, стартапи, венчурні фонди, що інвестують саме в цю сферу, зокрема Jerusalem Venture Partners (JVP) Cyber Labs, а також науково-дослідні проекти, що забезпечують співпрацю між високотехнологічними компаніями і науково-дослідними центрами. У 2017 році інвестиція у сферу кіберзахисту в Ізраїлі дорівнювала 10,8 млн. доларів, що на 26 % більше, ніж у 2016 році.

Слід зазначити, що на даний час Ізраїль є другим у світі після США експортером програмного забезпечення. Отже, з постачальника стартапів Ізраїль поступово перетворюється на міжнародний центр високих технологій і, насамперед, одного з провідних світових лідерів в галузі кібербезпеки. У 2012 році в Ізраїлі розроблено спеціальну трирічну програму фінансування розробок у сфері кібербезпеки – KIDA[5], суть якої полягає в бюджетному фінансуванні приватних компаній (на це виділяється \$ 26,5 млн.), які спеціалізуються на створенні кіберпродуктів і послуг. Завдяки виваженій та оптимізованій стратегії з урахуванням існуючих ризиків та загроз терористичного спрямування, ця країна зуміла побудувати одну з найнадійніших систем кіберзахисту, яка повноформатно функціонує як у секторі оборони, так і у цивільному секторі, включаючи такі провідні галузі, як транспорт, державне управління, медицина, енергетика, фінансово-банківська система тощо.

У червні 2010 року у зв'язку із збільшенням проявів кібератак з боку ісламських екстремістів при службі безпеки (ШАБАК) [6] Ізраїлю був створений відділ з інформаційної безпеки, який контролює критично важливі національні інфраструктури, котрі спеціалізуються на запобіганні кібертероризму, проведенні спеціальних операцій в глобальному інформаційному просторі. Реальність кіберзагрози стало підставою для прийняття рішення про створення спеціальної групи, яка розробила рекомендації з протидії майбутнім загрозам в умовах кібервійни. Ці рекомендації стосувалися не тільки розробки конкретних технологій, а й створення необхідної інфраструктури, яка передбачає співпрацю промислових і наукових кіл із структурами національної безпеки, розробку освітніх програм, створення наукових центрів підвищення кваліфікації, критичних національних систем, а також багато інших проектів.

Разом із тим, в будь-якій країні державна політика забезпечення кібербезпеки визначається стратегією кібербезпеки. З метою адекватного реагування на виклики та загрози в кіберпросторі в Ізраїлі прийнято два стратегічних документи: Національна кіберініціатива 2010 року та Резолюція уряду № 3611 від 7 серпня 2011 року, яка запроваджує План дій з реалізації Національної кіберініціативи. На виконання цих нормативно-правових актів у 2012 році урядом був створений Національний кіберштаб для реалізації засад національної кібербезпекової політики і нарощування технологічного потенціалу в кіберпросторі. Також у 2012 році в Ізраїлі була створена кіберполіція як суб'єкт забезпечення національної безпеки [7].

У 2015 році в Ізраїлі було створено Національне управління кібербезпеки (The National Cyber Bureau) як координаційний орган, діяльність якого спрямована на посилення цифрового захисту. Створення цієї структури було зумовлене тим, що в країні спостерігався досить високий рівень комп'ютеризації, що, однак, автоматично провокувало загрозливі тенденції в кіберпросторі, у зв'язку з чим багато державних інституцій та представників комерційного середовища стали уразливими до кібератак. Рішення про доцільність створення двох окремих підрозділів у рамках однієї системи пояснюється необхідністю здійснювати діяльність у двох напрямках: стратегічному, у рамках якого формується державна політика і нарощуються технологічні потужності, і

оперативному, який використовує напрацювання Штабу. Крім цього, відповідно до резолюції № 2444 від 15 лютого 2015 року та рекомендацій Національного кіберштабу, уряд Ізраїлю схвалив рішення про створення ще й Національного управління з кіберзахисту як центрального оперативного органу Національного кіберштабу.

З метою інституційної оптимізації процесів забезпечення кібербезпеки ізраїльський уряд 17 грудня 2017 року схвалив пропозицію Прем'єр-міністра країни про об'єднання Національного кіберштабу і Національного управління з кіберзахисту в єдину Національну службу кібербезпеки, яка буде відповідати за всі аспекти кіберзахисту: від формування засад державної політики та нарощування технологічних потужностей до оперативної роботи спеціальних підрозділів. Ця структура також відповідатиме за усі аспекти кібероборони в цивільному секторі з метою налагодження ефективної координації та взаємодії між державою та приватним сектором. Очікується, що Національна служба кібербезпеки Ізраїлю як новостворена комплексна державна структура стане платформою реалізації цілеспрямованої та виваженої політики у боротьбі з кіберзлочинністю, тероризмом, поєднуючи спроможності військового та цивільного секторів. Ця структура також відіграватиме важливу роль у захисті інтересів громадян, суспільства та держави в кіберпросторі.

У 2017 році Ізраїль увійшов у десятку найкращих країн світу за рівнем підготовки та результативності діяльності кібервійськ: щорічне фінансування складає 150 млн доларів США, а штат хакерів налічує понад 1000 осіб. Цей рейтинг очолюють США з фінансуванням галузі у розмірі 7 млрд. доларів США на рік та 9 тис. хакерів (друге місце посідає Китай – 1,5 млрд. доларів США державного фінансування та 20000 хакерів) [8].

Для забезпечення повноцінної та ефективної системи кібербезпеки уряд Ізраїлю ініціює і підтримує програми навчання спеціальних кадрів, а також інформаційні програми для населення країни, наприклад, навчання школярів навичкам цифрового захисту. Крім того, в країні підтримується кілька освітніх програм для молоді віком 16-18 років. Вважаємо, що освітня програма у сфері кібербезпеки є позитивним фактором, який дає змогу поширити серед населення відомості з інформаційної безпеки.

У рамках масштабної боротьби з хакерами Ізраїль спільно з США реалізує проекти шкільної та дошкільної освітньої підготовки у сфері кібербезпеки. З 2016 року Уряд Ізраїлю запровадив нову категорію робочих віз для іноземних спеціалістів, які залучаються вітчизняними компаніями у сфері високих технологій. Отже, з постачальника стартапів Ізраїль поступово перетворюється на міжнародний центр високих технологій.

На цьому фоні держава Ізраїль дедалі активніше залучає до співпраці у сфері забезпечення кібербезпеки компанії приватного сектору. У 2017 році в Ізраїлі у секторі кібербезпеки було задіяно 420 підприємств, а на кіберіндустрію витрачено 815 млн. доларів США. Невипадково держава Ізраїль зарекомендувала себе як світовий лідер у сфері інноваційних кібертехнологій.

На ізраїльські передові підприємства, які співпрацюють із міжнародними корпораціями та стартапами, покладаються завдання щодо розробки сучасних та інноваційних систем захисту від кібератак з метою адекватного реагування на ситуативну динаміку та загрози в кіберпросторі. Тільки у 2017 році інвестори вклали в розвиток ізраїльської “кібернетичної екосистеми” рекордну суму – 815 млн. доларів США, що становить 16 % від світових інвестицій у промисловість кібербезпеки. Також у рамках державно-приватного партнерства індустрія кіберзахисту розширює використання новітніх методик шифрування в мережах та системах зберігання інформації. При цьому

приватні компанії з кіберзахисту використовують штучний інтелект для розпізнавання шкідливого програмного забезпечення та виявлення агресивної активності у Інтернет.

У 2017 році ізраїльський державний оборонний концерн “Рафаель” став переможцем конкурсу із забезпечення безпеки критичної інфраструктури в банківській та фінансовій сферах. Цей концерн планує розширити оперативний обмін інформацією серед банківських установ про можливі загрози щодо об’єктів критичної інфраструктури. Планується, що мережа банківських установ буде обробляти фінансову інформацію, в тому числі й інформацію про споживчі кредити. Це, у свою чергу, сприятиме розподілу дефіцитного капіталу між конкуруючими способами використання для більш ефективного кредитування.

Слід зауважити, що в Ізраїлі не тільки успішно розвивається сфера кібербезпеки, а й проводяться власні розробки кіберзброї. Такі ініціативи мають за мету створити в Ізраїлі аналог Інтерполу в кіберпросторі, а також запровадити систему обміну інформацією між усіма суб’єктами кіберзахисту у поєднанні зі спроможностями державного та приватного секторів.

Однією з основ забезпечення кібербезпеки є протидія тероризму. З цією метою 15 червня 2016 року ізраїльський Парламент прийняв новий закон “Про боротьбу з тероризмом” (далі – Закон), який набув чинності 1 листопада 2016 року. Цей Закон містить положення, що стосуються використання Інтернету та соціальних мереж у терористичних цілях. За Законом до терористичної діяльності належить, зокрема: використання терористами кіберпростору з метою пропаганди своєї злочинної діяльності; вербування найманців; радикалізація суспільства, підбурювання до насильства; фінансування тероризму. Вважаємо вельми корисним впровадження законодавчих ініціатив у практичну площину у цьому форматі, оскільки в Інтернеті постійно зростають масштаби кібератак, наслідком яких є знищення майна або пошкодження критичної інфраструктури [8]. Досвід Ізраїлю у боротьбі з тероризмом у кіберпросторі відображає ці тенденції повною мірою. Ізраїльське кримінальне законодавство доповнено нормою про відповідальність за підбурювання до тероризму і “демонстрацію солідарності з терористичною організацією або підтримку акту тероризму”. Положення цієї норми охоплюють, зокрема, діяльність в мережі Інтернет з підтримки та заохочення актів тероризму проти Ізраїлю та його громадян.

У зв’язку з прийняттям Закону також передбачено кримінальну відповідальність за: вербування осіб до терористичної організації; участь у навчаннях, що проводяться терористичною організацією; публікацію закликів до вчинення терористичного акту; оприлюднення повідомлень, що схвалюють або підтримують тероризм [9].

Дія Закону також розповсюджується і на боротьбу з терористичною пропагандою в соціальних мережах. Передбачається, що суд має право вимагати від адміністраторів Facebook, YouTube, Twitter та інших соціальних платформ видалення контенту, який пропагує тероризм. На початку 2018 року до Закону внесено зміни, які передбачають можливість застосування покарання у виді смертної кари до винних терористів [10].

Такі законодавчі ініціативи дають підстави стверджувати, що держава Ізраїль має свій стратегічний погляд на вирішення проблеми забезпечення кібербезпеки.

Висновки.

Оптимізація в Ізраїлі структур, які відповідають за кібербезпеку, зумовлена масштабами потенційних та реальних кіберзагроз в умовах протиборства з арабськими країнами. Держава Ізраїль виділяє великі фінансові ресурси для забезпечення кібербезпеки, у т.ч. за рахунок збільшення кількості підготовлених хакерів, удосконалення багаторівневої системи підготовки відповідних кадрів.

На підставі аналізу законодавчих ініціатив Ізраїлю в контексті імплементації кращих світових практик вбачаємо доцільним: створити центр боротьби з тероризмом та радикалізацією в мережі Інтернет; розглянути питання щодо внесення зміни до Кримінального кодексу України шляхом доповнення розділу X його Особливої частини новими кримінально-правовими нормами, що встановлюють відповідальність за пропаганду і поширення ідеології тероризму, у т.ч. у мережі Інтернет.

З урахуванням викладеного, перспективним напрямом розбудови національної системи кібербезпеки є активізація зусиль уповноважених правоохоронних органів України у напрямку міжнародного співробітництва з державою Ізраїль, що надасть змогу впровадити у практичну площину кращі практики зарубіжного досвіду в контексті удосконалення вітчизняної моделі кібербезпеки.

Використана література

1. Стратегія кібербезпеки України : Указ Президента України від 15.03.16 р. № 96 // Офіційний вісник України. – 2016. – № 23. – Ст. 899.
2. Дубов Д.В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України : дис. на здобуття наук. ступеня док-ра політ. наук : спец 21.01.01 / Дмитро Володимирович Дубов. – К., 2016. – 435 с.
3. Діордіца І. Поняття та зміст національної системи кібербезпеки // National law journal : theory and practice. – 2016. – № 6. – С. 36-42.
4. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України // Підприємництво, господарство і право. – 2017. – № 5. – С. 174-180.
5. The Global competitiveness Report 2016 – 2017. – Режим доступу : http://www3.weforum.org/docs/GCR2016017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf. – Заголовок с екрана.
6. Спецслужбы Израйля – список специальных подразделений. – Режим доступу : <http://www.pro-israel.ru/specslujbi-israelya.html>. – Заголовок с екрана.
7. В Израйле появилась Национальная система кибербезопасности – Режим доступу : http://mignews.com/news/politic/171217_221926_94739.htm. – Заголовок с екрана.
8. Израйль вошел в ТОП-10 стран по уровню кибервойск. – Режим доступу : <https://stmegi.com/posts/41238/izrail-voshel-v-top-10-stran-po-urovnyu-kibervoysk>. – Заголовок с екрана.
9. Новый израильский закон о борьбе с терроризмом в киберпространстве. – Режим доступу : <https://www.geopolitica.ru/article/novyy-izrailskiy-zakon-o-borbe-s-terrorizmom-v-kiberprostranstve>. – Заголовок с екрана.
10. В Израйле собрались ввести смертную казнь для террористов. – Режим доступу : <https://www.segodnya.ua/world/wnews/v-izraile-sobralis-vvesti-smertnuyu-kazn-dlya-terroristov-1099386.html>. – Заголовок с екрана.

~~~~~ \* \* \* ~~~~~