ЗАЛУЧЕННЯ ГРОМАДСЬКОСТІ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ (ЗА ПРИКЛАДОМ ВЕЛИКОБРИТАНІЇ)

Черниш Р.Ф.
к.ю.н., доцент кафедри правознавства

Постановка проблеми. Протягом останніх років глобальний кіберпростір усе більшою мірою розглядається світовою спільнотою, як один із найважливіших безпекових пріоритетів, оскільки його функціонування є визначальним чинником розвитку економіки, військового, соціального та інших секторів. Загроза злому інтернет-систем із злочинним умислом або в інтересах спеціальних служб іноземних держав знаходиться на одному рівні з тероризмом, шпигунством і зброєю масового ураження.

Беручи до уваги необхідність унеможливлення втручання у внутрішню політику держав, здійснення впливу на свідомість громадян тощо, на систематичній основі розробляються нові способи забезпечення інформаційної безпеки.

При цьому, відмічаються тенденції залучення до зазначеного виду діяльності як представників спеціальних Інтернет – спільнот (насамперед осіб із середовища т.зв. "хакерів"), так і пересічних громадян (в першу чергу перспективної молоді шкільного віку "тінейджерів"). Передові позиції у вказаній сфері займають США, Великобританії та РФ.

Аналіз останніх досліджень і публікацій. Серед дослідників, які системно досліджують питання кібербезпеки, варто відмітити праці таких, як М. Лібіцкі, Дж. Най, В. Бутузов, К. Демчак, О. Довгань, П. Домбровський, А. Марущак, В. Пилипчук, В. Цимбалюк та інших.

Мета, завдання та методика досліджень. Вважається, що одним із першочергових завдань для України є формування дієвого механізму забезпечення безпеки інформаційного простору з врахуванням передового досвіду іноземних держав у вказаній сфері. В особливій мірі зазначене стосується нашої країни, беручи до уваги Євроінтеграційні сподівання, необхідність впровадження ефективних механізмів розвитку економіки тощо та перебування, при цьому, в умовах фактичного стану "неоголошеної війни" з РФ. В інформаційному просторі держави прихильниками терористичних утворень "ДНР"/"ЛНР"

та РФ систематично поширюються тенденційні матеріали пропагандистського характеру. Основна тематика: негативна економічна ситуації в Україні, відсутність узгодженості в діяльності вищих органів державної влади, заборгованість із виплатою заробітної платні, "переддефолтний" стан економіки, непослідовність реформ, які проводяться в державі тощо [11]. На жаль, розробка способів протидії вказаному виду злочинної діяльності значно відстає від потреб правоохоронної практики [12].

Результати досліджень. Починаючи з 2000-х років, спеціальними службами РФ цілеспрямовано реалізуються кампанії з дестабілізації суспільно-політичної ситуації в США та країнах ЄС. Під час виступу в Сент-Ендрюському університеті Шотландії міністр оборони Великобританії М. Феллон звинуватив Російську Федерацію у кібератаках, перетворенні "дезінформації у зброю", "регулярній брехні" та втручанні у перебіг вільного волевиявлення громадян (парламентські вибори у Чорногорії в жовтні 2016р., референдум в Нідерландах про асоціацію ЄС і України в квітні 2016 р. тощо). Зокрема, політик відзначив: "Росія явно випробовує НАТО і Захід. Вона прагне розширити сферу свого впливу, дестабілізувати країни і послабити Північноатлантичний Альянс. Це підриває національну безпеку цілого ряду союзників і міжнародну систему, засновану на правилах. У зв'язку з цим, у наших інтересах і в інтересах Європи зберегти сильні позиції НАТО, стримати Росію і відрадити її від прямування цих курсом" [6]. Аналогічної думки дотримується й Глава американської нацрозвідки Дж. Клеппер. З його слів: "Росія намагалася вплинути на результат виборів в "парі десятків" країн" [9]. К.Мартін (голова Національного центру кібербезпеки Великої Британії, NCSC), заявив, що російські хакери, скоріш за все, причетні до частини атак на заклади урядового рівня. Крім цього, керівник центру кібербезпеки Англії вважає, що хакери з РФ можуть викрасти нові дослідження англійських вчених, а ще їх персональні дані. Він підкреслив, що в їх число входять спроби нібито причетних до РФ хакерів викрасти закриту інформацію про зовнішню політику і оборону країни [2]. На думку Генерального директора британської розвідслужби MI5 Е. Паркера, Росія є зростаючою загрозою для стабільності Великобританії і використовує всі сучасні засоби, наявні в її розпорядженні, для досягнення своїх цілей, в тому числі і кібератаки [4].

Зважаючи на викладене, у Сполученому Королівстві в листопаді 2015р. було прийнято основний документ військового і зовнішньополітичного планування на найближчі п'ять років - "Стратегію національної безпеки і огляд стратегічної оборони і безпеки Великобританії до 2020 року". У вказаному нормативно-правовому акті сформульовано підходи уряду до політичних, оборонних, економічних та інших аспектів забезпечення безпеки королівства, адаптовані до наявних і прогнозованим загрозам і викликам.

Згідно з новою Стратегією, метою національної безпеки Великобританії є захист населення, території, економіки, інфраструктури і способу життя, зниження можливості виникнення загроз для королівства, її інтересів і інтересів союзників [2].

В цілому, Урядом Британії на стратегію кібербезпеки було виділено 1,9 млрд. фунтів стерлінгів (2,3 млрд. $). Заплановано, що держкошти буде витрачено на розвиток системи автоматичного захисту сайтів від хакерських атак і спроб несанкціонованого доступу до ресурсів офіційних доменів. Крім того, будуть посилені заходи по перехопленню електронних листів-пасток, а також закрито сайти, за допомогою яких хакери отримують доступ до банківських рахунків інтернет-користувачів. Також планується збільшити штат кіберполіцейських. "Наша нова стратегія ... дозволяє нам зробити більш суттєві кроки для самозахисту в кіберпросторі і завдати у відповідь удар, якщо на нас нападуть", – заявив міністр фінансів Ф.Хеммонд.

У вступному слові до документа екс-прем'єр-міністр Д. Кемерон зазначив, що за останні два роки Великобританія перетворилася в найбільш швидко зростаючу сучасну економіку світу, що дозволило з урахуванням зростаючих загроз з боку ІГІЛ, нестабільності

на Близькому Сході, кризи на Україні, збільшення кількості кібератак і ризиків пандемій здійснити додаткові інвестиції у власну національну безпеку.

На нашу думку, на особливу увагу заслуговують слова політиків про те, що "підвищенні вартості здійснення атаки проти будь-якого громадянина Великобританії буде досягатися, в тому числі, й за рахунок підвищення рівня кібернавиків. Кібербезпека – це вже не просто проблема IT-відділу, а й всієї робочої сили. Кібернавики повинні стати частиною кожної професії" [7].

З цією метою у Великобританії реалізується ряд програм із залучення громадськості до забезпечення безпеки інформаційного простору держави (насамперед учнівської та студентської молоді). Зокрема, Центром урядового зв'язку (GCHQ, веде радіоелектронну розвідку і забезпечує захист інформації органів уряду і армії), ініційовано програму із залучення тінейджерів в сферу кібербезпеки. Так, дівчатка у віці від 13 до 15 років, які проводять багато часу в інтернеті, візьмуть участь в тестах на логіку і кодування, створення мереж і криптографію. Зазначене пов'язане з тим, що на сьогодні жінки складають лише 10% від загального числа співробітників служб кібербезпеки по всьому світу, відзначають представники спецслужби. Змагання є частиною національної стратегії кібербезпеки, оголошеної в листопаді минулого року і розрахованої на п'ять років. Його організацією буде займатися новий Національний центр з кібербезпеки (NCSC). Об'єднавшись в команди по 4 людини, юні учасниці змагання будуть виконувати завдання в дистанційному режимі на своїх шкільних комп'ютерах. З кожним новим етапом труднощі завдань буде зростати. 10 груп з найвищою кількістю балів будуть запрошені до фіналу змагання під назвою CyberFirst, їм належить справитися зі складною кіберзагрозою. Команда-переможниця отримає комп'ютерне обладнання для своєї школи вартістю в 1000 фунтів, а також індивідуальні призи. За словами прес-секретаря NCSC, "жінки можуть і вже вносять величезний вклад у справу кібербезпеки, це змагання може надихнути багатьох зробити перші кроки в цій динамічній і гідної кар'єрі". "Я працюю разом з деякими воістину талановитими жінками, які допомагають захищати Британію від різноманітних онлайн-загроз, - зазначив директор Центру урядового зв'язку Р. Ханніган. – Змагання CyberFirst для дівчаток допоможе командам підлітків заглянути в цей хвилюючий світ і дасть їм прекрасну можливість використовувати нові навички " [3].

Також, з метою пошуку потенційних експертів для захисту держави від хакерських атак, у школах Англії дітям запропонують відвідувати заняття з кібербезпеки. Уряд країни заявив, що таким чином має намір уже нині працювати над проблемами кібербезпеки в майбутньому.

Ініціатори програми планують запросити до участі в програмі близько шести тисяч школярів віком від 14 років. Вони будуть відвідувати заняття тривалістю чотири години на тиждень з вересня 2017 року.

На проект, розрахований на п'ять років, буде витрачено близько 25 мільйонів доларів. Надалі планується найперспективнішим студентам виділяти університетські гранти і забезпечувати їх роботою в цій галузі [10].

Іншим кроком у сфері формування інформаційної безпеки Великобританії є залучення для забезпечення кібербезпеки держави молоді з великим досвідом відеоігор.

Учасники програми, які успішно пройдуть відбір в урядові розвідувальні агентства, прослухають основний дворічний курс з комунікацій, безпеки і проектування в університеті De Montfort. Вони стануть фахівцями в IT, програмному забезпеченні і телекомунікації. Закінчивши навчання, вони отримають професійні навички, необхідні для роботи в Центрі урядового зв'язку (GCHQ), а також в розвідувальних і оборонних службах MI5 і MI6 [5].

Також, велика увага приділяється проведенню активної роз'яснювальної роботи серед населення щодо небезпек кіберзагроз. Так, у Великобританії спільно з

Європейськими, американськими і канадськими партнерами було проведено захід під назвою GetSafeOnlineWeek для підвищення розуміння загроз кібербезпеки серед загального населення [1].

Що ж до України, то незважаючи на те, що 2014-2017р.р. стали періодом "загострення кібервійни", основними суб'єктами протидії інформаційному впливу залишаються спеціально створені державні органи, зокрема: Міністерство оборони України, Служба безпеки України, Служба зовнішньої розвідки, Державна служба спеціального зв'язку та захисту інформації, Міністерство внутрішніх справ України, кіберполіція тощо.

При цьому, на нашу думку, потенціал громадськості використовується не в повній мірі.

Висновки та перспективи подальших досліджень. Підсумовуючи вищевикладене, зважаючи на необхідність організації дієвої протидії країні-агресору у всіх сферах суспільного життя (насамперед недопущення інформаційного впливу на свідомість громадян), враховуючи міжнародний досвід у боротьбі з загрозами інформаційної безпеки, вважається що основні кроки держави повинні бути спрямовані на:

– створення Національного центру протидії кіберзагрозам, який би виконував керівну й координуючу функцію у сфері забезпечення кібербезпеки, за аналогом з тим, як це відбувається в іноземних державах (США, Великобританія, Австралія тощо);

– налагодження плідної співпраці державних органів, які займаються забезпеченням інформаційної безпеки, з групами незалежних патріотично настроєних програмістів ("FalconsFlame", "Trinity", "RUH8", "CyberHunta" тощо) в контексті проведення відповідних навчань, передачі досвіду тощо;

– посилення якісного складу відомств у системі забезпечення кібербезпеки України шляхом збільшення кількості навчальних закладів, які готують відповідних фахівців, розширення спеціальностей, а також забезпечення спроможності студентів підтримувати постійний контакт з практикою та оперативно впроваджувати технологічні інновації у навчальний процес;

– ініціювання на рівні Міністерства освіти України впровадження в загальноосвітніх навчальних закладах учбових програм, спрямованих на підвищення комп'ютерної обізнаності молоді, проведення олімпіад та інших конкурсів з метою виокремлення перспективної молоді;

– проведення активної роз'яснювальної роботи серед населення щодо небезпек кіберзагроз та загальних способів протидії останнім.

Література

1. Get Safe Online week [Електронний ресурс]. Режим доступу: http://www.cabinetoffice.gov.uk/news/get-safe-online-week.

2. Британия предупредила об ответных мерах в случае хакерских атак [Електронний ресурс]. Режим доступу: https://www.rbc.ua/rus/news/britaniya-predupredila-otvetnyh-merah-sluchae-1478018271.html.

3. Британская разведка ищет кибер-агентов среди девочек-подростков [Електронний ресурс]. Режим доступу: http://ru.delfi.lt/abroad/global/britanskaya-razvedka-ischet-kiber-agentov-sredi-devochek-podrostkov.d?id=73490964.

4. Великобритания потратит 1,9 млрд фунтов стерлингов(2,1 млрд евро) на усиление кибербезопасности в стране в течение ближайших пяти лет. [Електронний ресурс]. Режим доступу: https://www.ukrinform.ru/rubric-world/2112238-britania-gotovit-na-kiberbezopasnost-21-milliarda.html.

5. Кибербезопасность Великобритании будут обеспечивать любители видеоигр [Електронний ресурс]. Режим доступу: http://www.securitylab.ru/news/431575.php.

6. Міноборони Британії звинуватило РФ у кібератаках [Електронний ресурс]. Режим доступу: http://ua.korrespondent.net/world/3809809-minoborony-brytanii-zvynuvatylo-rf-u-kiberatakakh.

7. Правительство Великобритании потратит $2,3 млрд на укрепление кибербезопасности [Електронний ресурс]. Режим доступу: http://www.securitylab.ru/blog/personal/tsarev/321169.php.

8. Руководитель центра кибербезопасности Великобритании объявил о росте атак русских хакеров Kremlin Press http://kremlinpress.com/2017/02/12/rukovoditel-centra-kiberbezopasnosti-velikobritanii-obyavil/ [Електронний ресурс]. Режим доступу: http://kremlinpress.com/2017/02/12/rukovoditel-centra-kiberbezopasnosti-velikobritanii-obyavil/.

9. США:Москва намагалася втрутитися у вибори 20 країн [Електронний ресурс]. Режим доступу: http://ua.korrespondent.net/world/3798975-sshamoskva-namahalasia-vtrutytysia-u-vybory-20-krain.

10. У школах Англії введуть заняття з кібербезпеки [Електронний ресурс]. Режим доступу: https://bdzhola.com/news/u-shkolah-angliji-vvedut-zanjattja-z-kiberbezpeki.

11. Черниш Р. Ф. Окремі кроки протидії сепаратизму в інформаційній сфері, як передумова реалізації євроінтеграційних процесів / Р. Ф. Черниш // Актуальні проблеми державно-правового розвитку України в контексті євроінтеграційних процесів : матеріали Міжнар. наук.-практ. конф., присвяч. 20-річчю Конституції України, 23–24 черв. 2016 р. – Запоріжжя : Просвіта, 2016. – С. 427.

12. Черниш Р. Щодо окремих аспектів протидії інформаційному тероризму в сучасних умовах / Р. Черниш, І. Осауленко // Протидія терористичній діяльності: міжнародний досвід і його актуальність для України : матеріали міжнар. наук.-практ. конф. (30 верес. 2016 р.). – К. : Нац. акад. прокуратури України, 2016. –с. 367.