УДК 004.056

ВІЙНА В УКРАЇНІ НА КІБЕРПРОСТОРІ. ДОСВІД КАНАДИ ЩОДО ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

Жигаревич О.К. (ORCID: 0000-0002-7154-9733)
Волинський національний університет імені Лесі Українки, Луцьк, Україна

WAR IN UKRAINE IN CYBER SPASE. CANADA'S EXPERIENCE IN COUNTERING CYBERTERRORISM

Zhyharevych O.K.
Lesya Ukrainka Volyn National University, Lutsk, Ukraine

Abstract. The strategy for developing cybersecurity in Ukraine during the war is based on strengthening international cooperation. Legislative changes relate to active counteraction in cyberspace to the placement of state information resources in the «clouds» and the protection of Ukraine's critical infrastructure. Work is also underway on regulations that would regulate the response to events in cyberspace. Modern wars are fought on several fronts, one of which is information, so preventing cyberattacks is one of the most important lines of defense for the country. Ukraine's reliable partners in cyber defense are the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the European Union Agency for Cybersecurity (ENISA), and the Computer Emergency Response Team (CERT-EU). A National Cybersecurity Cluster was created, a coordination platform that brings together the resources, capabilities, and competencies of the National Security and Defense Council of Ukraine and the U.S. Civilian Research and Development Foundation (CRDF Global), government organizations, the private sector, and international partners.

Keywords: Cyberwar, CISA, ENISA, CERT-EU, CRDF Global, CERT-UA, USAID.

Вступ. Стратегія розвитку кібербезпеки в Україні під час війни базується на посиленні міжнародної співпраці. Законодавчі зміни стосуються активної протидії у кіберпросторі розміщення у «хмарах» державних інформаційних ресурсів, та захисту критичної інфраструктури України. Робота триває і над нормативно-правовими актами, які дозволяють врегулювати питання на реагування на події у кіберпросторі. Сучасні війни відбуваються у декількох фронтах, один з яких інформаційний, тому запобігання кібератакам є однією з найважливіших ліній захисту країни. Надійні партнери України у сфері кіберзахисту – Агенство з кібербезпеки та безпеки інфраструктури США (CISA), Агенство Європейського Союзу з питань кібербезпеки (ENISA), команда реагування на комп'ютерні надзвичайні події CERT-EU. Створений Національний Кластер Кібербезпеки – координаційна платформа, яка об'єднує ресурси, можливості, компетентності Ради Національної безпеки та оборони України та Фонду Цивільних Досліджень та розвитку США (CRDF Global), урядових організацій, приватного сектору, міжнародних партнерів. Основними напрямками розвитку у сфері кібербезпеки є посилення кадрового потенціалу. Державна служба спеціального зв'язку та захисту інформації в Україні затвердила перших шість професійних стандартів для нових професій у галузі кібербезпеки, які були розроблені за підтримки проекту USAID «Кібербезпека критично важливої інфраструктури України». Досвід країн світу у сфері кіберзахисту є надзвичайно важливим для розвитку країни.

Методологія дослідження. Канада приймає активні дії для посилення свого захисту у кіберпросторі та запобіганню кібертероризму, а зважаючи на темпи з якими відбувається технологічний прогрес у нашій країні доцільно переймати досвід від найкращих, в тому числі й Канади. Актуальність теми зумовлена прискореним

технологічним розвитком України та необхідністю активно запобігати кіберзлочинам, і кібертероризму в умовах війни [1].

Кібертероризм – це навмисна, політично вмотивована атака на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій [2].

На найвищому рівні уряд Канади займається профілактикою, виявленням, реагування та припиненням кібертерористичної діяльності на кордоні, розвідкою та спостереженням, імміграцією, фінансами та транспортуванням через кілька відділів і агенцій та їх захищений сектор [3].

Стратегія кібербезпеки країни визначає кібертероризм та ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) основними загрозами кібернетичній безпеці держави, а ключовим органом, на який покладено координація та контроль за імплементацією вказаної стратегії, реалізація державної політики та координація заходів у сфері кібербезпеки та протидії кіберзагрозам визначене Міністерство громадської безпеки Канади (Public Safety Canada) [4].

Старання держави цілком виправдані, оскільки, за прогнозами 2023 рік принесе постійний стрес для організацій, які намагаються захистити свої активи. Операційна технологія і надалі залишатиметься метою зловмисників. Кіберзловмисники усвідомлюють, що безпека більшості програмних середовищ, як правило слабка – приклад злому у 2021 році Colonial Pipeline, Oldsmar Water і JBS Meats [4].

Результати дослідження та їхнє обговорення. До складу Міністерства громадської безпеки Канади увійшли: Канадська служба розвідки та безпеки (Canadian Security Intelligence Service), Агентство прикордонної служби Канади (Canada Border Services Agency), Королівська кінна поліція(Royal Canadian Mounted Police) й інші відомства. Пізніше до її складу приєднався Офіс із захисту критичної інфраструктури та надзвичайних ситуацій (Office of Critical Infrastructure Protection and Emergency Preparedness), який до цього перебував у відомстві Міністерства оборони Канади. Саме на базі Міністерства громадської безпеки Канади, як ключового органу в сфері кібербезпеки, боротьби з тероризмом і протидії загрозам критичної інфраструктуридержави, був створений Центр реагування на кіберінциденти Канади (Canadian Cyber Incident Response Centre), головне завдання якого полягає у здійсненні моніторингу та наданні допомоги у протидії кіберзагрозам, організації взаємодії між державними установами і громадськістю у сфері кіберзахисту, а також здійснення відповідного державного реагування на будь-який інцидент, що загрожує кібербезпеці держави [5].

Громадська безпека Канади відповідає за національну стратегію держави Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy: канадська контртерористична стратегія, яка вирішує питання кібертероризму безпосередньо та спільно через згадані відділи та партнери у чотирьох областях концентрації: профілактика зосереджується на мотивації осіб, які займалися терористичною діяльністю або мають потенційну можливість брати участь у терористичній діяльності вдома та за кордоном. Відмова в доступі сприяє розвитку та покращенню стійкості життєво важливих активів і систем проти терористичних атак та ідентифікації ризиків для зменшення вразливості безпеки. Security Readiness and Response за винятком інформаційних технологій федерального уряду та інформаційних систем управління, витрачає рівень зміцнення систем і можливості, пов'язані з реагуванням і відновленням.

Уряд Канади планує витратити 80 мільйонів доларів на нову федеральну мережу кібербезпеки. Планується, що нова канадська програма кібербезпеки буде підтримана 80 мільйонами канадських доларів протягом наступних чотирьох років [6].

Об'єкти кричної інфраструктури будь якої країни дуже вразливі під час кібервійни. У Канаді можна сформувати 10 об'єктів критичної інфраструктури: енергія, комунікація, фінанси, охорона здоров'я, харчування, вода, транспортування, безпека, уряд та виробництво. Безумовно, значної шкоди таким об'єктам можуть завдати і природні катаклізми, але в XXI ст., кібератаки завдають нищівного удару в даних сферах [7].

Рис.1. Надійність підбору правильного паролю для захисту особистих даних

Упродовж наступних п'яти років Канада планує виділити 875,2 млн канадських доларів (близько 730 млн дол. США) на посилення кіберзахисту державних систем.

В умовах війни в Україні, Канада з перших днів вторгнення надсилає нам гуманітарну, військову (летальну та нелетальну) та фінансову допомогу. На гуманітарну допомогу жителям України та українським біженцям Канада перерахувала 100 млн канадських доларів, які будуть використані на невідкладну медичну допомогу, захист та підтримку внутрішньо переміщених осіб та біженців, а також забезпечення їхніх першочергових потреб у продуктах харчування, питній воді, засобах гігієни й даху над головою. Канадські авіакомпанії організовували чартерні рейси для біженців з України. Країна також запровадила грошові виплати для українських біженців. Україна підписала кредитну угоду з Урядом Канади про надання 500 мільйонів канадських доларів на пільгових умовах. Країна союзник також передала летальне озброєння чотири 155-мм гаубиць M777 і вісім броньованих автомобілів Roshel Senator APC. Канада також відправить Україні більш маштабну військову допомогу, включаючи сюди системи протиповітряної оборони ближньої, середньої та дальньої дії [8].

Висновки. Україна може почерпнути декілька моментів з досвіду та дій уряду Канади. Прийняття потрібних законів та виділення фінансування, а саму ідею зможуть підхопити наші спеціалісти у різних галузях як приватних так і у державних установах. Запровадження професійних стандартів у галузі кібербезпеки: Розробник систем захисту інформації, Адміністратор мереж і систем, Фахівець сфери захисту інформації, Аналітик з безпеки інформаційно-телекомунікаційних систем, Фахівець з питань безпеки,

Інструктор-методист з інформаційної та кібербезпеки. CERT-UA планує до кінця року збільшити кількість професій у сфері кібербезпеки та захисту інформації до двадцяти. Канада співпрацює з провайдерами інтернет – послуг з метою сприяння у визначенні загроз у кіберпросторі та розроблення ефективних заходів з протидії ним. Українська інформаційна та кіберспільнота згуртувались фактично в єдину ІТ-армію. Співпраця між Україною та Канадою є запорукою розбудови ефективного захисту у кіберпросторі.

Бібліографія

1. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. *Public Safety Canada / Sécurité publique Canada*. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (date of access: 23.04.2023).
2. CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/ (date of access: 23.04.2023).
3. Top Cybersecurity Budgets Around The World. *Analytics India Magazine*. URL: https://analyticsindiamag.com/top-cybersecurity-budgets-around-the-world/ (date of access: 23.04.2023).
4. National Cybersecurity Strategies. *ENISA*. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies (date of access: 23.04.2023).
5. National Security. *Public Safety Canada / Sécurité publique Canada*. URL: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/index-eng.aspx (date of access: 23.04.2023).
6. Findlay V. Cyber-Terrorism and Canada's Cyber-Security Strategy. *Security Sector Reform Resource Centre.* CATA Conference Ottawa Presentation, Nov 2014, 2014.
7. Cybersecurity in Canada. *Grant Thornton LLP Canada*. URL: https://www.grantthornton.ca/insights/cybersecurity-in-canada/ (date of access: 23.04.2023).
8. Система корелювання подій та управління інцидентами кібербезпеки на об'єктах, критичної інфраструктури / Гнатюк С.О. та ін. *«Кібербезпека: освіта, наука, техніка»*. 2023. Т. 3, № 19. С. 176–196. URL: https://doi.org/10.28925/2663-4023.2023.19.176196 (дата звернення: 23.04.2023).

References

1. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. *Public Safety Canada / Sécurité publique Canada*. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (date of access: 23.04.2023).
2. CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/ (date of access: 23.04.2023).
3. Top Cybersecurity Budgets Around The World. *Analytics India Magazine*. URL: https://analyticsindiamag.com/top-cybersecurity-budgets-around-the-world/ (date of access: 23.04.2023).
4. National Cybersecurity Strategies. *ENISA*. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies (date of access: 23.04.2023).
5. National Security. *Public Safety Canada / Sécurité publique Canada*. URL: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/index-eng.aspx (date of access: 23.04.2023).
6. Findlay V. Cyber-Terrorism and Canada's Cyber-Security Strategy. *Security Sector Reform Resource Centre.* CATA Conference Ottawa Presentation, Nov 2014, 2014.
7. Cybersecurity in Canada. *Grant Thornton LLP Canada*. URL: https://www.grantthornton.ca/insights/cybersecurity-in-canada/ (date of access: 23.04.2023).
8. System for cyber security events correlation and incident management in critical infrastructure objects / S. Gnatyuk et al. *Cybersecurity: Education, Science, Technique*. 2023. Vol. 3, №. 19. P. 176–196. URL: https://doi.org/10.28925/2663-4023.2023.19.176196 (date of access: 23.04.2023).