УДК 004.7.056.5 (045)

Даов Несрін,
Л. А. Радомська

СУЧАСНИЙ СТАН КІБЕРБЕЗПЕКИ В УКРАЇНІ

Вінницький національний технічний університет

Анотація

У дослідженні проаналізовано актуальні проблеми кібербезпеки в Україні; схарактеризовано ряд чинників, які потрібно врахувати для покращення сучасного стану захисту інформації та загалом для розвитку інформаційної безпеки в Україні.

Ключові слова: *кібербезпека, загроза, кібератака, кіберсередовище, захист інформації.*

Abstract

The study analyzes current issues of cybersecurity in Ukraine; a number of factors that need to be taken into account to improve the current state of information protection and in general to develop information security in Ukraine are described.

Keywords: *cybersecurity, threat, cyber attack, cyber environment, information protection.*

Вступ

Із розвитком технологій, штучного інтелекту, інформаційних систем, розвивається також і їхній «темний бік» – кіберагресія, кібератаки, віруси тощо. Питання кібербезпеки актуальне для чи не всіх країн світу, адже захист кіберпростору тісно пов'язаний з економічною, військовою, суспільною безпекою. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами [1]. Завдання держави – забезпечити інтереси громадськості в різних сферах діяльності.

Мета дослідження – проаналізувати актуальні проблеми кібербезпеки в Україні та визначити основні чинники для доступу до стабільного, безпечного цифрового простору, адже належний рівень кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Результати дослідження

Кібербезпека (КБ) – це захист цілісності комп'ютерних систем, апаратного забезпечення, програмного забезпечення та даних, зокрема й персональних, від комп'ютерних атак та інших загроз, які можуть виникнути в процесі ведення бізнесу [6].

З ростом девайсів, розумних речей, зі збільшенням трафіку, потоку даних, людина почала дедалі більше переносити в кіберсередовище бухгалтерію, управління процесами, виконання багатьох інших процесів. З'явилася необхідність захисту інформації саме в діджитал- (кібер-) середовищі.

Кібербезпека – це новий виток інформаційної безпеки, спрямований саме на діджитал-середовище, у якому ми власне й перебуваємо. КБ має на меті не тільки захист інформації, а й захист всієї системи в інформаційному полі, в IT-полі загалом [2].

Без надійного плану щодо кібербезпеки хакери та інші зловмисники можуть легко отримати доступ до вашої комп'ютерної системи та неправомірно використовувати особисту інформацію, інформацію про клієнта, бізнес-інформацію, а також персональні дані, які компанія використовує, зберігає, передає або іншим чином оброблює. Питання кібербезпеки для бізнесу є надзвичайно важливим та актуальним [6].

На жаль, як подають аналітики, Україна посідає найнижчі місця в загальних рейтингах кібербезпеки, а саме: 51 місце за рейтингом дослідницької компанії «Comparitech», 54 місце у рейтингу «Global CybersecurityIndex», а також має найнижчі позиції у Центрально-Східній Європі. У 2017 році через вірус NonPetya Україна втратила 0,5 % ВВП, що в грошовому еквіваленті – 14,914 млрд. грн. [3].

Про потребу переглянути підходи до організації системи кібербезпеки в Україні зазначав і А. Амелін, співзасновник Українського інституту майбутнього та керівник економічних програм під час дискусії «Кібербезпека. Новий підхід в Україні» у квітні 2020 р. [3]. Адже, за словами А.Амеліна, рейтинги продемонстрували, що Україна не досягла оптимальності побудови цієї системи, сучасні методи покращення кібербезпеки недостатньо ефективні й потребують форматування.

Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, сумнозвісним NotPetya та багатьма іншими інцидентами, які протягом останніх років створили Україні сумнівну репутацію одного з головних кіберполігонів [4].

Низький рівень залучення професійної спільноти, відсутність трансформаційного підходу – загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція, СБУ, Держспецзв'язок тощо) [4]. Наразі експертне співтовариство розробляє основних принципи й напрямки покращення стану кібербезпеки в Україні. Основна ідея реформи – перейти від моделі, коли держава намагається контролювати кібербезпеку, зокрема й у приватних організаціях, до саморегуляції, яка дозволить бізнесу самостійно визначати і контролювати впровадження стандартів кібербезпеки для відповідних галузей.

Роль держави у розбудові вітчизняної системи кіберзахисту потребує переосмислення. Очевидно, це має бути не функція контролю (як зараз), а скоріше фасилітації і допомоги у вирішенні проблем кібербезпеки [4].

За результатами міжнародного дослідження Ernst&Young у сфері інформаційної безпеки за 2018-2019 роки «Кібербезпека: більше, ніж захист?», близько 80% компаній розуміють, що надалі не можуть обмежуватися стандартними заходами в галузі кібербезпеки. Тому вони продовжують нарощувати базовий функціонал своїх систем захисту, переглядають підходи до вдосконалення архітектури кібербезпеки і починають впроваджувати інші сучасні інноваційні рішення щодо захисту інформації. Основними напрямами для інвестування в кібербезпеку у 2020 році були визначені:

- хмарні рішення (52%);
- аналітика кіберзагроз (38%);
- мобільні обчислення (33%) [5].

З іншого боку, надзвичайно важливим є аспект підготовки власних фахівців у сфері кібербезпеки. Безперечно слушною з цього приводу є позиція МОН України, яке наполягає на тому, аби нові освітні програми з кібербезпеки в українських вишах грунтувалися на міжнародних стандартах та були орієнтованими на здобуття практичних навичок [5]. Про це заявили учасники віртуального круглого столу «Вища освіта з кібербезпеки в Україні», який відбувся 19 листопада 2020 року за участі заступника Міністра освіти і науки України А. Селецького. Сьогодні в Україні спеціалістів із кібербезпеки готують в 51 ЗВО. В усьому світі попит на таких фахівців зростає з неймовірною швидкістю.

Дослідники Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. визначають з-поміж основних такі фактори покращення кібербезпеки в Україні: стратегічна політика кібербезпеки, прийняття відповідного законодавства, глобальне партнерство, просвітницькі програми з кібербезпеки та ін. [1]. Україна активно залучає провідні організації до підвищення ступеня обізнаності комерційних підприємств і неприбуткових організацій щодо кібербезпеки на всіх рівнях. Крім того, організовано роботу підрозділу CERT-UA – Державного центру захисту інформаційно-телекомунікаційних

систем (ДЦЗ ІТС) ДССЗЗІ, який спеціалізується на виявленні кіберінцидентів та реагуванні на них [1].

Висновки

Належний рівень кібербезпеки є необхідною умовою розвитку інформаційного суспільства. В Україні є ряд проблем щодо захисту кіберпростору, які потребуєть комплексного підходу в розв'язанні. Професійний потерціал, належний моніторинг, стратегічна політика кібербезпеки, прийняття відповідного законодавства, глобальне партнерство, просвітницькі програми з кібербезпеки – це ті фактори, що можуть уплинути позитивно на покращення рівня кібербезпеки в Україні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. Том 21, 3. 2019. С. 150-157. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBER SECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y.
2. ІНФОРМАЦІЙНА БЕЗПЕКА І КІБЕРБЕЗПЕКА – В ЧОМУ РІЗНИЦЯ? URL: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/.
3. Амелін А. Кібербезпека. Новий підхід в Україні. URL: https://uifuture.org/publications/kiberbezpechna-ukrayina-novyj-pidhid/.
4. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/.
5. Нові освітні програми з кібербезпеки в українських вишах мають базуватися на міжнародних стандартах та бути орієнтованими на здобуття практичних навичок. URL: https://mon.gov.ua/ua/news/novi-osvitni-programi-z-kiberbezpeki-v-ukrayinskih-vishah-mayut-bazuvatisya-na-mizhnarodnih-standartah-ta-buti-oriyentovanimi-na-zdobuttya-praktichnih-navichok-mon.
6. Основні види кібербезпеки в контексті захисту та обробки персональних даних. URL: https://bsoprivacygroup.com/node/41.

Даов Несрін — студентка групи 1БС-20б, Вінницький національний технічний університет, Вінниця, e-mail: veravoroniuk18@gmail.com.

Радомська Людмила Анатоліївна – кандидат філологічних наук, доцент кафедри мовознавства, Вінницький національний технічний університет, м. Вінниця, e-mail: ludarad9@gmail.com.

Daov Nesrin – student of 1БС-20b group, Vinnytsia National Technical University, Vinnytsia, email: nesrindaw@gmail.com;

Radomska Liudmyla A. – Cand. Sc. (Eng), Assistant Professor, Department of Linguistics, Vinnytsia National Technical University, Vinnytsia, e-mail: ludarad9@gmail.com.