УДК 004.056

Стадник Р. Ю.
Слюсар Д. Ю.
Остапенко-Боженова А. В.

ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ СЬОГОДЕННЯ

Вінницький національний технічний університет

Анотація
Проаналізовано перспективи розвитку кібербезпеки в Україні в умовах сьогодення. Роль російсько-української інформаційної війни в удосконаленні системи безпеки України.
Ключові слова: кібербезпека, кібербезпека України, інформаційна війна, кібергігієна

Abstract
The prospects for the development of cybersecurity in Ukraine in today's conditions are analyzed. The role of the Russian-Ukrainian information war in improving ukraine's security system.
Keywords: cybersecurity, cybersecurity of Ukraine, Information war, Cyber Hygiene.

Вступ

На сьогоднішній день, побудова якісної системи захисту інформації є важливим аспектом у збереженні конфіденційності даних кожного громадянина України. Від початку інформаційної війни від кібератак найбільше страждають впливові медіа, фінансові інститути та державні установи [1]. Зважаючи на те, що безпечна комп'ютерна система – це ідеальна система, що забезпечує повний захист, побудувати її на практиці неможливо. Проте, будь-яку систему можна удосконалювати отримуючи результат її роботи. Тобто, забезпечення безпеки найчастіше зводиться до управління ризиками, а саме до оцінки імовірності їх виникнення та запровадження відповідних запобіжних заходів.

Результати дослідження

Кібербезпека — це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

Зважаючи на сучасні реалії, кібербезпека без сумнівів важлива для кожного, адже враховуючи ризик того, що конфіденційна інформація людини зберігається у багатьох різних організаціях, що не завжди можуть убезпечити себе від витоку даних чи злому. Як наслідок, уже в березні 2013 року представники розвідки застерегли, що кібератаки та шпигунство наразі є головною загрозою національній безпеці, що перевершує навіть тероризм.

Систему безпеки України формують: академічна кібербезпека (дослідницькі інститути, вищі навчальні заклади); державна кібербезпека (СБУ, кіберполіція, НБУ і т. д.); комерційна кібербезпека (методи та методики, технології та набутий досвід); некомерційні, волнтерські та громадські організації (Український кіберальянс, ІнформНапалм) [3].

Сьогодні, Україна має незадовільний рівень захищеності кіберпростору, про що свідчить думка експертів з різних країн світу. Підтвердженням того, що ця галузь недостатньо розвинена в Україні є мала кількість кваліфікованих працівників у цій сфері [4].

Для України питання кібербезпеки максимально загострилось у 2014 році з початком російсько-української гібридної війни, адже, окрім традиційного воєнного фронту, протистояння триває і на кібернетичному полі бою [5]. У кіберпросторі противник переслідує ті ж цілі, що й військові – завдати якомога більше шкоди інфраструктурі, причому не стільки військовій як цивільній [6]. Загалом,

сьогодні Україна успішно відбиває кібератаки, які здійснюють РФ і групи, пов'язані з військовими та правоохоронними органами росії.

Для забезпечення кібербезпеки Україна повинна використовувати такі рівні захисту своєї інформації [6]:

- запобігання — доступ до певного виду інформації та технологій надається тільки певній кількості людей, які отримали до цього доступ та мають відповідні фахові навички;
- виявлення — виявлення злочинів і зловживання на ранніх сталях, навіть якщо злочинцям вдалося обійти механізми захисту
- обмеження — зменшення розміру втрат, якщо все ж таки злочин скоєний, попри те що заходи для його запобігання і виявлення були здійснені
- відновлення — забезпечення ефективного відновлення втраченої інформації за наявності всіх документів і перевірених планів з відновлення.

Посилення кібербезпеки в Україні потребує насамперед розвитку кіберстрахування як перспективної галузі українського страхового ринку. Важливим пунктом є посилення кримінальної відповідальності за вчинення кіберзлочину, що дозволить зменшити їхню кількість, особливо це має стосуватись державних органів та об'єктів критичної інфраструктури. Також потрібно зібльшити фінансування наукових досліджень у сфері кіберзахисту, що надасть можливості удосконалення систем захисту інформації. Розширити співпрацю з міжнародними організаціями за для спільних наукових досягнень. І найголовніше, регулярно удосконалювати політику державної кібербезпеки України.

Висновки

Отже, дослідивши питання перспективи розвитку кібербезпеки України, можна зробити висновок, що питання кібербезпеки набуває критичної актуальності в Україні. Гібридна агресія РФ надала поштовх у розвитку даного напряму, що посприяло зосередженню уваги органів влади на галузі захисту інформації, а це, у свою чергу, зробило державу в перспективі більш стійкою до кібератак. Причиною більшості успішних кібератак є громадяни, які не виконують елементарні вимоги до захисту особистої інформації у мережі, через необізнаність елементарних принципів кібергігієни. Тому, потрібно дотримуватися порад фахівців з кіберзахисту [7] для зменшення витоків особистої та критичної інформації, особливо зважаючи на реалії воєнного часу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібератаки РФ [Електронний ресурс]: Кількість кібератак під час війни. - Режим доступу: Кількість кібератак під час війни зросла втричі, - Держспецзв'язку | Кабінет Міністрів України (kmu.gov.ua). – Назва з екрана.

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. // Відомості Верховної Ради (ВВР). - 2017. - № 45. - ст.403.

2. Кібербезпека : сучасні технології захисту: навч. посіб. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король; М-во освіти і науки України, Харків. нац. економ. ун-т ім. С. Кузнеця. – Львів : Новий Світ – 2000, 2019. - 680 с.

3. Кібербезпека України [Електронний ресурс] / О. Яновський // Українська правда. – 2019. – Режим доступу: Кібербезпека України: проблеми і шляхи їх вирішення (archive.org). – Назва з екрана.

4. Кібербезпека: безпекові загрози [Електронний ресурс]: Український кіберпростір. – Режим доступу: Український кіберпростір: безпекові загрози, виклики та перспективи розвитку | ADASTRA. – Назва з екрана.

6. Рівні захисту інформації [Електронний ресурс]: Кібербезпека як складова захисту держави. - Режим доступу: КІБЕРБЕЗПЕКА ЯК ВАЖЛИВА СКЛАДОВА ВСІЄЇ СИСТЕМИ ЗАХИСТУ ДЕРЖАВИ | Міністерство оборони України (mil.gov.ua). – Назва з екрана.

7. Organization for Security and Co-operation in Europe [Електронний ресурс]: Cyber Hygiene Memo. - Режим доступу: https://www.osce.org/project-coordinator-in-ukraine/504046

Стадник Ростислав Юрійович – студент групи 1КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: totalwarplayer632003@gmail.com.

Слюсар Дмитро Юрійович – студент групи 1КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: dima.slyusar.2003@gmail.com.

Остапенко-Боженова Аліна Василівна — асистент кафедри Захисту Інформації, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua.

Stadnyk Rostislav Y. – Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, , e-mail: totalwarplayer632003@gmail.com.

Sliusar Dmitro Y. – Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, , e-mail: dima.slyusar.2003@gmail.com.

Ostapenko-Bozhenova Alina V. — assistant in Information Protection department Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua.