Костерчук К.
здобувач вищої освіти обліково-фінансового факультету
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Розвиток кіберзахисту в Україні

У сучасних умовах існує проблема кіберзахисту як фінансової сфери України, так і державних інформаційних хостів. Раніше цій сфері діяльності в нашій країні майже не приділялося уваги, так як кіберзагроз не виникало. У 2006 р. в Україні було прийнято Конвенцію про кіберзлочинність №994-575 від 01.07.2006 року [1]. А після подій у 2017 році, коли вірус Petya.A заполонив усі хости державних установ, банків, податкової, поліції та ін., виникло питання про посилення кіберзахисту в державі та оновлення законодавчої бази. Було прийнято рішення про підписання Закону України «Про основні засади забезпечення кібербезпеки України» № 2469-VIII від 21.06.2018 року [2], який став рушійною силою для створення центру ліквідації кіберзагроз CERT-UA - Computer Emergency Response Team of Ukraine що функціонує в рамках Держспецзв'язку [3].

CERT-UA являється основним і єдиним органом в Україні, який слідкує за кіберсистемою та виявляє кіберзагрози до їх настання. Запроваджено правила щодо захисту та імунітету хостів перед кібератаками.

Основні правила кібергігієни [3]:

1. Використання ліцензійних/легалізованих операційних систем, інших програмних продуктів, своєчасне й систематичне їх оновлення.
2. Користування антивірусним програмним забезпеченням з технологією евристичного аналізу.
3. Використання програмного міжмережевого екрану (брандмауеру) та штатних засобів захисту від шкідливого програмного забезпечення.
4. Здійснення регулярного резервного копіювання даних, збереження резервних копій на зовнішніх носіях інформації (SDD, HDD тощо) та налаштування функції «відновлення системи».
5. Заборона підключення флешек та зовнішніх дисків, CD та DVD тощо у комп'ютер, якщо відсутня довіра їх джерелу.
6. При підключенні пристроїв забезпечення їх автоматичної перевірки на наявність шкідливого програмного забезпечення.
7. Відключення автоматичного запуску змінних носіїв інформації.
8. Уникнення використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях), тощо.

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» № 2469-VIII від 21.06.2018 року, було встановлено принципи забезпечення кібербезпеки [2]:

1) верховенство права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватна взаємодія, широка співпраця з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проєктів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетність запобіжних заходів;

7) невідворотність покарання за вчинення кіберзлочинів;

8) пріоритетний розвиток та підтримка вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідація зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Отже, Україна перебуває на шляху становлення міцної системи кіберзахисту країни, в той час коли розвинуті країни світу мають 5-рівневу систему захисту та вдосконалюють її з кожним роком все більше.

Список використаних джерел:

1. Конвенція про кіберзлочинність №994-575 від 01.07.2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 13.11.2019).
2. Про основні засади забезпечення кібербезпеки України: Закон України № 2469-VIII від 21.06.2018 р. URL: https://zakon.rada.gov.ua/laws/main/2163-19 (дата звернення: 13.11.2019).
3. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua (дата звернення: 13.11.2019).

Науковий керівник: **Бурковська А. В.,** *канд. екон. наук, доцент, доцент кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, м. Миколаїв, Україна*