4. Якщо випадково з листа ви завантажили файл, то ні в якому разі неможна його відкривати і потрібно звернутись до фахівців;
5. Не варто переходити за підозрілими адресами. Вони можуть містити віруси та "спливаючі" вікна, які автоматично завантажують шкідливі програми на комп'ютер.

Список використаних джерел

1. *Махницький О.В. Використання соціальної інженерії для крадіжки особистих даних, 6 с.*
2. *Т. В. Нескородєва, В. Ю. Грущенко Детектування фішингових посилань Матеріали наукової конференції (2019–2020 рр.). URL:* ***https://jpvs.donnu.edu.ua/article/view/10424/***
3. *Фішинг. URL: https://cutt.ly/fN9jPpX (дата звернення: 06.11.2022)*
4. *Перелік когнітивних упереджень. URL: https://cutt.ly/qN1AAcJ (дата звернення: 06.11.2022)*

УДК 004.056.5:343.97](477)

Єрмак Д.М., здобувач вищої освіти
Зелінська О.В., доцент,
доцент кафедри інформаційних технологій

ЗАХОДИ УКРАЇНИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НАЦІОНАЛЬНОЇ ІНФОСФЕРИ ТА ПРОТИДІЇ ПРОЯВАМ КІБЕРЗЛОЧИННОСТІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи: Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки».

Сьогодні фахівці з кіберзахисту від ДССЗЗІ, СБ та МВС України стикаються у своїй роботі з численними труднощами, не маючи змоги самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі. Через це їм доводиться дедалі активніше шукати шляхи співробітництва з аналогічними організаціями світового співтовариства, використовуючи для цього всі наявні можливості й механізми, які є в розпорядженні кожної з країн [1].

Відчутний поштовх до активізації зусиль у цьому напрямку дало ухвалення організацією НАТО програмного документа під назвою «Рамки для співробітництва у питаннях кібернетичного захисту між НАТО та державами 1партнерами», який було розповсюджено у Штаб-квартирі Альянсу 2 квітня 2009 року. У документі наголошується, що головний елемент політики НАТО у сфері кіберзахисту полягає в тому, що держави — члени Альянсу несуть пряму відповідальність за захист власних національних комунікацій та інформаційних систем. Альянс, у свою чергу, повинен бути здатний надати підтримку своїм партнерам, які зазнали кібератак міжнаціонального значення. Цим документом передбачено, зокрема, що головні цілі співпраці НАТО з державами-партнерами у сфері кіберзахисту полягають у підвищенні здатності НАТО та держав-партнерів у сфері захисту критичних комунікаційних та інформаційних інфраструктур проти кібератак, наданні допомоги у відновленні нормального функціонування відповідної інфраструктури після кібератак, а також у створенні основ для вжиття заходів із підтримки потерпілих від кібератак. Відповідно до головних положень згаданого документа країни-партнери закликаються до невідкладної гармонізації національного законодавства у сфері кібернетичної безпеки з відповідними міжнародними нормами, такими як Конвенція Ради Європи з питань кіберзлочинності, із неодмінним дотриманням таких головних принципів [2].

1. Співпраця між НАТО та країною-партнером має бути взаємовигідною в такому сенсі: Альянс може надати країні-партнерові інформацію та підтримку у сфері кібербезпеки, якщо ця країна неухильно виконує умови взаємодії.

2. НАТО може надати країні-партнерові як експертну допомогу, так і свої технічні можливості для захисту від кібернетичних атак.

3. Країни-партнери можуть звертатися з пропозиціями щодо співпраці у сфері кіберзахисту та отримання підтримки з боку НАТО, якщо зазнають кібератак національного масштабу.

4. Альянс і партнери мають уникати дублювання зусиль, що докладаються в рамках інших міжнародних організацій, залучених до захисту ІС від кібератак.

5. Наявність угоди про безпеку між НАТО та країною-партнером має визначати обсяги допомоги та інформаційного обміну. Проте інформацію стосовно захисту критичної інфраструктури національних комунікаційних та інформаційних систем буде позначено та передано належним чином лише в разі потреби ознайомлення з нею [2].

Згідно зі сказаним основні напрямки подальшого співробітництва України з НАТО у сфері кіберзахисту, а отже, і створення загальнодержавної системи кібернетичної безпеки мають бути такі:

1. Формування культури та проведення інформаційно-пропагандистської кампанії про значущість проблематики кібербезпеки держави.

2. Створення механізму моніторингу кібернетичних втручань і загроз, а також своєчасного ухвалення рішень щодо реагування на їх прояви.

3. Забезпечення безпеки державних інформаційних ресурсів.

4. Підвищення надійності критичної кіберінфраструктури.

5. Підтримка вітчизняних виробників програмно-апаратного забезпечення.

6. Підвищення компетентності фахівців різних сфер діяльності у питаннях кібербезпеки.

7. Вироблення і реалізація єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ-інфраструктури від деструктивного кібернетичного впливу

8. Удосконалення національного нормативно-правового та понятійно-термінологічного апарату кібербезпеки.

9. Організація міжнародного співробітництва у сфері кібербезпеки.

Відповідну роботу слід проводити поетапно.

Отже, провідні держави світу дедалі більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом становить проблему забезпечення кібербезпеки кожної країни [3-5].

Список використаних джерел

1. *Конспект лекцій з дисципліни «Методика та техніка кібербезпеки» URL:* ***https://kn-it.info/wp-content/uploads/2020/10/Konspekt_MTKYS-41.pdf***
2. Інформаційна та кібербезпека: соціотехнічний аспект *URL: https://dut.edu.ua/uploads/p_303_79299367.pdf*
3. *Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.*
4. *В.В. Денисюк, О.В. Зелінська, Важливість кібербезпеки в сучасному світі. Комп'ютерні технології обробки даних: матеріали ІІ Всеукраїнської науково-практичної конференції, м. Вінниця: ДонНУ, 10 грудня 2021. – 130-132 с.*
5. *Н.В. Рогожук, Т.В. Січко, Передача даних небезпечним каналом зв'язку, з використанням шифрування відкритим ключем. Прикладні інформаційні технології: матеріали Всеукраїнської науково-практичної конференції для студентів, аспірантів та молодих вчених, м. Вінниця: ДонНУ, 29 квітня 2020. – 88-90 с.*

УДК 004.4

Жеребцов О.М., здобувач СО «Магістр»
спеціальності 122 «Комп'ютерні науки»
Нескородєва Т.В., д.т.н., доцент, зав.
кафедри інформаційних технологій

ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ ДАНИХ ІНТЕРНЕТ-МАГАЗИНУ МУЗИЧНИХ ІНСТРУМЕНТІВ