Красько Ірина Андріївна
Здобувач ступеня вищої освіти НАВС

Науковий керівник:
Буренко Олег Володимирович
викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, підполковник поліції

ЗАГРОЗИ ВІД КІБЕРАТАК В УМОВАХ ВОЄННОГО СТАНУ

В умовах правового режиму воєнного стану кібератаки можуть відчутно вплинути на функціонування суспільства та стати загрозою національній безпеці.

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 – відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. Цей Закон визначає правові та організаційні основи забезпечення національних інтересів України у кіберпросторі, основні цілі державної політики у сфері кібербезпеки [1].

В умовах воєнного стану необхідно визначити форми та методи забезпечення інформаційної безпеки громадян з метою захисту суспільства не лише від деструктивного інформаційного впливу держав-агресорів та численних терористичних організацій, причетних до дестабілізації ситуації в нашій країні, а й від інших негативних інформаційних чинників, що дезорганізують національний інформаційний простір. Використання інформаційних технологій та механізмів для здійснення ворожих актів агресії проти громадян, незаконне використання інформаційних ресурсів інших країн, протиправна діяльність в інформаційному просторі, спрямована на дестабілізацію суспільства, використання інформаційної інфраструктури для поширення інформації, що розпалює міжетнічну та міжплемінну ворожнечу, ідей та теорій, що розпалюють ненависть, дискримінацію та насильство, використання інформації маніпулювання інформацією та багато інших загроз інформаційній безпеці створюють ризики [2, с. 23].

Основні загрози від кібератак в умовах воєнного стану:

1. *Втрати інформації*: кібератаки можуть призвести до викрадення або знищення конфіденційної інформації, наприклад, військових оперативних планів, даних про розробку зброї, даних державних установ та посадових осіб. Це може завдати шкоди національній безпеці та обороноздатності країни [3].

2. *Шантаж*: зловмисники можуть використовувати викрадену інформацію для шантажу державних установ, військових або цивільних осіб з метою отримання переваг або впливу на їхню поведінку.

3. *Пошкодження критичної інфраструктури*: кібератаки можуть спрямовуватися на критичну інфраструктуру, таку як енергетичні мережі, телекомунікаційні системи, системи водопостачання та інші. Пошкодження таких систем може призвести до серйозних наслідків для національної безпеки.

4. *Вплив на військові операції*: кібератаки можуть впливати на військові операції, зокрема на системи зв'язку, навігації та управління (атаки на системи зв'язку можуть зробити неможливим зв'язок між різними частинами армії, а атаки на системи навігації можуть спричинити неконтрольоване рухання техніки [4]).

Одна з найбільших кібератак на банківську сферу відбулася в липні 2017 року. Кіберзлочинці використовували шкідливий код під назвою «NotPetya», який поширювався через оновлення для бухгалтерського програмного забезпечення M.E. Doc, що використовується в Україні. Банки також використовували це програмне забезпечення і таким чином стали жертвами кібератаки. NotPetya використовував вразливість в операційній системі Windows, що дозволяло зловмисникам шифрувати комп'ютерні диски та вимагати від жертв викуп у біткоїнах. Крім того, вірус блокував доступ до систем банку, що призвело до значних фінансових втрат. В результаті цієї кібератаки кілька українських банків були змушені припинити роботу і призупинити обслуговування клієнтів.

Крім того, було пошкоджено низку комп'ютерів, що призвело до втрати даних та значних витрат на відновлення комп'ютерної інфраструктури.

Враховуючи вищевикладене слід зазначити, що Україна має необхідний потенціал для нарощування потенціалу у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам. Інструменти та технології кіберзахисту необхідно вдосконалювати, щоб зменшити ризик кібератак та забезпечити інформаційну безпеку. Тому необхідно вживати заходів для забезпечення високого рівня інформаційної безпеки та запобігання можливим кібератаки.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Вінниця: ХНУВС, 2023. – 176 с.

3. Інформаційно-аналітичний дайджест Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»: Кібербезпека в інформаційному суспільстві., №9 (вересень)

4. Інструменти інфомедійної безпеки в умовах воєнного стану URL:https://dspace.znu.edu.ua/jspui/bitstream/12345/12339/1/Vizniuk%202023.pdf.