УДК 004.056

Яропуд В.О студент
Зелінська О.В., к.т.н., доцент,
доцент
кафедри інформаційних технологій

КОМП'ЮТЕРНА БЕЗПЕКА ПІД ЧАС ВІЙНИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Комп’ютерна безпека, захищає комп’ютерні системи та інформацію від шкоди, крадіжки та несанкціонованого використання. Комп’ютерне обладнання зазвичай захищене подібними пристроями, які використовуються для захисту інших цінних або чутливих пристроїв, таких як серійні номери, двері та замки, а також сигналізація. З іншого боку, захист даних і доступ до системи досягається за допомогою інших тактик, деякі з яких є більш складними [1].

Заходи безпеки, пов’язані з комп’ютерною інформацією та доступом, спрямовані на чотири основні загрози:

- викрадення даних, таких як військова таємниця з державних комп’ютерів;
- вандалізм, включаючи знищення даних комп'ютерним вірусом;
- шахрайство, наприклад, що працівники банку спрямовують кошти на власні рахунки;
- порушення конфіденційності, наприклад, незаконний доступ до захищених особистих фінансових або медичних даних із великої бази даних.

Основним засобом захисту комп’ютерної системи від крадіжки, вандалізму, порушення конфіденційності та інших видів безвідповідальної поведінки є електронне відстеження та реєстрація доступу та діяльності різних користувачів комп’ютерної системи. Це зазвичай робиться шляхом призначення фізичного паролю для кожної особи, яка має доступ до системи [2].

У відповідь на війну росії в Україні Anonymous оголосили війну російському уряду.

27 лютого зловмисники «закрили» сайт уряду чечні. 2 лютого деякі ЗМІ, а також банківські веб-сайти піддалися атакам і в результаті було показано українські пісні і гімн України, які транслювали на російському телебаченні.

У відповідь проросійський зловмисник Killnet заявив, що теж провели успішну кібератаку на їх сайт, але цього сайту ніколи не існувало. Anonymous також захопили державний телеканал Wink і Ivy Steam і показали відео вибухів в містах України. База даних міністерства оборони росії були надані у мережу, а також і номери телефонів, і електронні адреси, і імена його співробітників [4].

У ніч з 13 на 14 січня було здійснено хакерську атаку на низку урядових сайтів, зокрема МЗС, МОН та інші.

Зловмисники на головних сторінках цих сайтів розмістили повідомлення провокаційного характеру. Роботу більшої частини атакованих державних ресурсів вже відновлено. Контент сайтів при цьому залишився без змін, і витоку

персональних даних не відбулося. Інші сайти відновлять роботу найближчим часом.

Основною ідеєю було цією кібератаки було викрадення даних через застосунок «Дія», але портал відключено, як і низку інших урядових сайтів. Це необхідно для локалізації проблеми та запобігання поширення атаки на інші ресурси.

У кінці ця кібератака не досягла своєї цілі і наші данні у повній безпеці. Іншими словами цей злочин не досяг своєї мети [3].

Які ж існують механізми кібератаки. Почнемо з основ «кібергігієни», простих і розумних способів захисту себе в Інтернеті. Ось 4 речі, які можна зробити:

• Застосуйте багатофакторну аутефікацію у своїх облікових записах і зменшіть ймовірність злому на 99%.

• Оновіть програмне забезпечення. Фактично, увімкніть автоматичне оновлення.

• Подумайте, перш ніж клацати. Більше 90% успішних кібератак починаються з фішингового листа.

• Використовуйте надійні паролі, а в ідеалі – менеджер паролів для створення та зберігання унікальних паролів [5].

Список літератури:

1 Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О. О. Комп'ютерна безпека. Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея»

2 Інформація про комп'ютерну безпеку URL: https://www.britannica.com/technology/computer-security

3 Кібератака на «Дію» URL: https://suspilne.media/197708-kiberataki-na-ministerstva-mincifri-povidomilo-so-zastosunok-dia-prodovzue-pracuvati/

4 Про вдалі кібератаки URL:https://bit.ly/3xApjQL

5 Які відбитись від кібератак URL: https://zmina.info/articles/yak-zahystytysya-vid-kiberatak-porady-dlya-zahyshhenogo-lystuvannya-obhodu-czenzury-j-czyfrovoyi-bezpeky/