датчика, який дає зрозуміти, що в разі хакерської атаки відхилення часу буде не в межах допустимості, яке сповістить про некоректність роботи системи.

ВИСНОВОК

В ході проведення тестування на захищеність даних в системі Інтернету речей нерідко буває ситуація, коли важливі дані або викрадають, або спеціально змінюють для заподіяння шкоди. Через що людство втрачає велику кількість інформації, а також страждають фінансові капітали.

Було обраховано кількість затрати часу на виконання одного циклу роботи програми та однієї тисячі циклів керування. Також було визначено допустиме максимальне відхилення та недопустиме відхилення, що буде значити, що хтось втрутився в роботу нашої системи. Це дає змогу оцінити якість і швидкість роботи PID-контролера. Адже, він є ключовою частиною в роботі всієї системи, що в комплексі з RSM дає потужну захист системи.

Список використаних джерел

1. *Cornelia Győrödi, Robert Győrödi, Roxana Sotoc, "A Comparative Study of Relational and Non-Relational Database Models in a Web- Based Application" in International Journal of Advanced Computer Science and Applications, vol. 6, No. 11, pp78-82, 2015, DOI: 10.14569/IJACSA.2015.061111.*
2. *J. Siegel and S. Sarma, "A Cognitive Protection System for the Internet of Things," in IEEE Security & Privacy, vol. 17, no. 3, pp. 40-48, May-June 2019, doi: 10.1109/MSEC.2018.2884860.*
3. *Howard Shrobe, Dimitrios Serpanos, Muhammad Taimoor Khan, "ARMET: Behavior-Based Secure and Resilient Industrial Control Systems" in Proceedings of the IEEE, PP(99):1-15, doi: 10.1109/JPROC.2017.2725642.*
4. *A. Salisu, Aminu Bugaje, A. Z. Loko, "IOT BASED HOUSEHOLD ELECTRICITY ENERGY MONITORING AND CONTROL" in FUDMA Journal of Sciences, Vol. 4 No. 4, December, 2020, pp 77 – 84, doi: 10.33003/fjs-2020-0404-466.*
5. *Muhammad Taimoor Khan, Dimitrios Serpanos, Howard Shrobe, "Sound and Complete Runtime Security Monitor for Application Software" in arXiv, pp 1-3, 17 Jan 2016, doi: 10.48550/ arXiv:1601.04263v1.*

УДК 316.485.26:316.776.23](477)(043.2)

Мазур Ю.О., здобувачка 4 курсу спеціальності 125 «Кібербезпека»
Крижановський В. Г., д.т.н., професор, професор кафедри інформаційних технологій

ПРАВИЛА ІНФОРМАЦІЙНОЇ ГІГІЄНИ ПІД ЧАС ВІЙНИ

Донецький національний університет імені Василя Стуса, м. Вінниця

У період коли наша країна перебуває у стані повномасштабної війни з Російською Федерацією, а бажання країни агресора посіяти паніку та знизити моральних дух суспільства зростає, варто підняти тему інформаційної гігієни. Інформаційна гігієна – це фільтрація потоку отримуваної інформації, що допомагає не засмічувати голову фейками, протистояти шахрайству та не робити непотрібних помилок у момент паніки. Головною функцією інформаційної гігієни є захист національного інформаційного простору від втручання і впливів інформаційної політики іноземних країн, від нав'язування громадянам інших, нетипових моделей поведінки (політичної, суспільної, ідеологічної) [2].

За статистикою в 2020 році 54% користувачів у Facebook поширювали базову інформаційну гігієну. Зважаючи на те, що 2020 рік признаний роком пандемії, то найчастіше фейки поширювались саме на тему коронавірусу. Загалом цих 54 % розділились наступним чином [3]:

- 34% користувачів публікували маніпулятивні заголовки та публікації
- 29% користувачів публікували посилання на сайти-сміттярки
- 13% користувачів публікували фейки
- 10% користувачів проходили тести, які викрадали дані.

Якщо ж брати минулий 2021 рік, то відсоток користувачів, що порушують інформаційну гігієну зріс до 73%, з яких [4]:

- 61% користувачів публікували матеріали з сайтів-сміттярок
- 39% користувачів публікували матеріали, що містять маніпулятивну інформацію
- 26% користувачів публікували фейки
- 25% користувачів публікували результати тестів, ігор, опитувань чи проходили тести.

Точних даних за 2022 рік не опубліковано, але ми можемо зробити припущення, що відсоткова кількість користувачів, що порушують інформаційну гігієну не зменшився. Навпаки, з початком повномасштабного вторгнення розповсюдження фейкової інформації збільшилось, адже з'явилась дуже велика пропаганда, почалась велика інформаційна війна та, звичайно, зросла кількість атак на різні державні установи, що у свою чергу потягло за собою здійснення кібератаки для розповсюдження фейкової інформації.

Зважаючи на те що на сьогоднішній день фейки поширюються зі швидкість звуку, варто вміти їх розпізнавати. Нижче наведено 9 найпоширеніших ознак фейкових новин [5].

1. Яскрава емоційна забарвленість. Надавати емоційного забарвлення події – не робота журналіста. Вони навряд чи будуть використовувати такі слова як «Шок!», «Сенсація!» та інші.
2. Емоційний заголовок не відповідає змістові статті. Чим емоційніший заголовок, тим більша вірогідність що ви перейдете за цим посиланням, тобто збільшите кількість переглядів та заробіток пропагандиста.
3. Ненадійні інформатори. Якщо в статті відсутнє посилання на першоджерело, краще не довіряйте цій новині
4. Думка, оцінка, припущення не дорівнює фактові. Не потрібно довіряти припущенням, таким чином ви тішите себе ілюзіями, які потім не збуваються. Таким чином падає моральний дух населення
5. Розповсюдження стереотипів та навішування ярликів – один із методів пропаганди
6. Теорія змови. Якщо стаття чи пост написані у стилі «Масони домовились з інопланетянами..» – то не варто довіряти та взагалі продовжувати читати дану новину
7. Упереджене і однобоке висвітлення події. Якщо в статті йдеться про висвітлювання, наприклад сварки, то варто звернути увагу на те, аби там фігурували коментарі двох сторін
8. Помилки в публікаціях. Звертайте увагу на помилки у словах, недостовірних фото та відео (наприклад перевірте чи існують такі фото взагалі)
9. Недостовірні дата публікації та час. Звертайте увагу на те чи вказано дату публікації, чи достовірні новини на теперішній момент, чи це переопубліковані дані.

Аби убезпечити себе та не потрапити на гачок пропагандистів Міністерство культури та інформаційної політики України розробили 10 порад яких варто дотримуватись [6]:

1. Не поширюйте дезінформацію. Зберігайте самоконтроль і не поширюйте інформацію емоційного характеру в соціальних мережах.
2. Наша країна захищає та продовжує боротись за свою територію. Якщо ви чуєте протилежне – це неправда.
3. Не вірте та не поширюйте інформацію із сумнівних джерел. Лише інформація з офіційних сторінок та каналів державних органів та Суспільного мовлення
4. Жодним чином не поширюйте інформацію про переміщення українських військ.
5. Повідомлення про нібито обстріли мирного населення українськими військами – неправда. Ворог хоче підірвати вашу довіру до власних захисників.

6. Агресор поширює різні чутки не лише про бійців, а й про військово-політичне керівництво. Довіряти ворогу не можна.
7. Інформація на приватних акаунтах може не відповідати дійсності. Не діліться нею.
8. Агресор поширюватиме наклепи та «зраду» через свої офіційні чи підконтрольні канали. Перевіряйте патріотичні на вигляд, але сумнівні повідомлення та заклики.
9. Зберігайте єдність та підтримуйте одне одного
10. Якщо перервався Інтернет-зв'язок або сторінки державних органів були зламані, звертайтесь до Суспільного мовлення. Якщо не працює телебачення – вмикайте абонентську радіоточку.

На останок варто наголосити, що наш мозок потребує перепочинку. Тому не варто забувати хоча б два-три рази на день давати своєму фізичному та емоційному станові відпочивати від новин. І саме головне, не поширюйте фейки, не довіряйте сумнівним джерелам таким чином ви допомагаєте здолати ворога на інфораційному полі бою.

Список використаних джерел

1. *Халамендик В.Б. Інформаційна гігієна к фактор збереження психічного здоров'я людини. Гуманітарний вісник Запорізької державної інженерної академії. Київ, 2016. 9 с.*
2. *54% українців не дотримуються інформаційної гігієни в Facebook – дослідження. URL: https://cutt.ly/dN5oqGv (дата звернення:08.11.2022)*
3. *Інформаційна гігієна, або як Facebook став джерелом №1 брехні для українців. URL: https://cutt.ly/dN5odWf (дата звернення:08.11.2022)*
4. *Інформаційна гігієна або як розпізнати неправдиві новини в інтернеті? Видавництво «Простір», Львів, 2019. 7 с.*
5. *У разі надзвичайної ситуації або війни. Міністерство культури та інформаційної політики України. Київ, 2022. 14 с.*

УДК 004.056:[164:658.8](043.2)

Македонський Б. О., здобувач 4 курсу спеціальності 125 «Кібербезпека»
Потапова Н. А., к.е.н., доцент, доцент кафедри інформаційних технологій

ПРОБЛЕМА КІБЕРБЕЗПЕКИ У СФЕРІ ЛОГІСТИКИ

Донецький національний університет імені Василя Стуса, м. Вінниця

З розвитком інформаційних технологій розвиваються і методи кібератак на компанії в тому числі і логістичні. Не всі хакери мають на меті отримати користь або матеріальні ресурси в результаті інциденту, багато з них проводять атаки з