НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

77-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

16 травня – 22 травня 2025 р.

записів із таблиці в сервісі Google Sheets та виведенні їх у вигляді зрозумілого графічного інтерфейсу: числових значень температури та вологості, а також часу останнього оновлення.

Для реалізації взаємодії з таблицею використовується бібліотека gspread, яка забезпечує взаємодію з Google Sheets API. Доступ до таблиці здійснюється за допомогою файлу авторизації (наприклад, credentials.json), створеного в Google Cloud Console. Завдяки цьому додаток може автономно зчитувати дані без додаткових дій з боку користувача.

Окрім відображення поточних показників, додаток може бути розширений за рахунок таких функцій:

— графічне відображення динаміки температури та вологості у вигляді графіків;

— система повідомлень при перевищенні встановлених меж (наприклад, надмірна вологість);

— експорт історичних даних у файл формату CSV або PDF;

— налаштування частоти оновлення даних.

Таким чином, поєднання Python, Kivy та сервісів Google дозволяє реалізувати зручний, адаптивний та функціональний мобільний застосунок, який значно підвищує ефективність роботи з інформацією, отриманою з мікроконтролера Arduino. При подальшому розвитку даного програмного продукту передбачається можливість створити повноцінну мережу моніторингу. Застосування такого рішення можливе у сільському господарстві (агро-датчики), розумних будинках, освітніх закладах тощо.

Література:

1. Google Workspace for developers. URL: https://developers.google.com/workspace/sheets/api/quickstart/python (дата звернення - 22.04.2025 р.).

2. Arduino Project Hub. URL: https://projecthub.arduino.cc/arcaegecengiz/using-dht11-12f621 (дата звернення - 22.04.2025 р.).

УДК 004.492.2

Ю.В. Калашнікова, асистент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

КІБЕРАТАКИ ЯК НОВИЙ ФРОНТ ВІЙНИ: ДОСВІД УКРАЇНИ У ПРОТИДІЇ КІБЕРАГРЕСІЇ РОСІЇ

В науковій роботі проаналізовано досвід України у протидії кібератакам Російської Федерації, що розпочалися з повномасштабним вторгненням у 2022 році. Розглядаються основні типи атак, досягнення України в кіберпросторі, міжнародна співпраця та роль громадян у

зміцненні кібероборони. Висвітлюються практичні рекомендації для користувачів щодо захисту своїх даних та участі у кібероборонні [1].

З початком повномасштабного вторгнення Російської Федерації в Україну у 2022 році, країна зіткнулася не лише з фізичними атаками, але й з безпрецедентним рівнем кіберагресії. Сотні атак щодня спрямовуються на урядові установи, банки, об'єкти енергетики та інфраструктури, медіа та соцмережі. Кібервійна стала повноцінним фронтом, на якому Україна не лише обороняється, а й дає гідну відсіч.

Основні типи кібератак [2]:

DDoS-атаки. Метою є перевантаження серверів та виведення з ладу державних сайтів. Прикладом є атака на портал «Дія» та сайти Міноборони та МЗС у лютому 2022 року.

Фішинг та соціальна інженерія. Здійснення масованої розсилки листів та SMS під виглядом державних повідомлень, використовуючи фейкові сайти «Дія», банків та служб допомоги.

Wiper-віруси. Застосування програмного забезпечення, що знищує дані. Прикладами є HermeticWiper, WhisperGate та CaddyWiper, застосовані перед наземним вторгненням.

Злом критичної інфраструктури. Спроби зупинки енергосистем, транспорту та зв'язку. Використання Industroyer2, як зловмисного ПЗ, яке намагалося вивести з ладу енергомережу.

Досягнення України у національному сегменті кіберпростору [3]:

ІТ-армія України. Створено ІТ-армію України, що об'єднала понад 300 000 волонтерів з усього світу та яка провела тисячі атак на російські ресурси, зокрема на банки, ЗМІ, держпортали та військові сервіси.

Зміцнення кіберзахисту держави. Система реагування на кібератаки (CERT-UA) була модернізована, впроваджено інструменти автоматичного моніторингу та виявлення загроз в реальному часі. Понад 1200 масштабних атак було відбито лише за 2023 рік. Захищено роботу порталів «Дія», податкової, митниці та військових сервісів.

Міжнародна кіберспівпраця. Компанії Microsoft, Google, Amazon, Cloudflare, Cisco надали захист інфраструктури та хмарні сервіси. НАТО та ЄС допомогли з навчанням фахівців, технікою та розвідданими про загрози.

Контрнаступ у кіберпросторі. Українські хактивісти зламали російські бази даних військових, мобілізованих, пропагандистів, злили документи Міноборони РФ, дані силовиків та ФСБ, а також здійснили саботаж ІТ-інфраструктури через атаки на їхні системи управління [4].

Аналітика та дезінформація. Побудовано системи для виявлення фейків та бот-мереж, моніторингу інформаційних атак. Організації, такі як UA Cyber Shield, Cyber Unit Technologies та OSINT-волонтери, аналізують діяльність ворога. Україна увійшла до ТОП-10 країн з найрозвиненішим кіберзахистом під час війни за даними CyberPeace Institute.

Рекомендації для користувачів [5]:

Захист даних. Використання складних паролів та двофакторної автентифікації (2FA). Заборона переходу за підозрілими посиланнями та відмова від встановлення будь-яких додатків з неперевірених джерел. Використання антивірусного програмного забезпечення та VPN, особливо при доступі до публічних Wi-Fi.

Протидія фейкам. Перевірка фактів новин перед поширенням. Перехресна перевірка інформації в офіційних джерелах: СБУ, Міноборони, Центр протидії дезінформації. Повідомлення про ботоферми чи фейки в соцмережах.

Отже, повномасштабна війна РФ проти України переконливо довела, що кіберпростір є повноцінним фронтом сучасних збройних конфліктів, де вирішуються не лише воєнні, а й політичні, економічні та суспільні питання. Україна продемонструвала унікальний приклад цифрової стійкості: в умовах постійної небезпеки вона не лише зберегла функціональність критичної інфраструктури, а й посилила свою позицію у глобальному кіберпросторі.

Ключовими чинниками цього успіху стали: ефективна координація між державними структурами, приватним IT-сектором і громадянським суспільством; підтримка міжнародних партнерів, зокрема компаній-лідерів у сфері кібербезпеки; високий рівень цифрової культури та відповідальності з боку звичайних користувачів, які долучилися до кібероборони в межах IT-армії та волонтерських ініціатив.

Література:

1. IT ARMY of Ukraine. Офіційний сайт боротьби проти ворога на IT-фронті. URL: https://itarmy.com.ua [дата звернення: 08.05.2025].

2. Європейський Союз Східного партнерства. Шахрайство, фішинг та кібератаки: як вберегти себе від зловмисників у мережі. URL: https://euneighbourseast.eu/uk/news/stories/shahrajstvo-fishyng-ta-kiberataky-yak-vberegty-sebe-vid-zlovmysnykiv-u-merezhi/ [дата звернення: 08.05.2025].

3. Смілянець Є., Білаш О., Плахотний А. Щодо кібербезпеки в умовах воєнного стану. Матеріали конференцій МЦНД, 22.12.2023; Одеса, Україна. URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/936 [дата звернення: 08.05.2025].

4. Кіберполіція України. Фішинг та фейкові акаунти: як захистити себе від інтернет-шахраїв. URL: https://cyberpolice.gov.ua/news/fishyng-ta-fejkovi-akaunty-yak-zaxystyty-sebe-vid-internet-shaxrayiv-7424/ [дата звернення: 08.05.2025].

5. Міністерство цифрової трансформації України. Кібергігієна для молоді. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth [дата звернення: 08.05.2025].