УДК 004.056
Василишин В. — ст. гр. КН-421
Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»

АНАЛІЗ КІБЕРАТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ УКРАЇНИ

Науковий керівник: старший викладач Радчик Г.І.

Василишин В.
Separate Structural Subdivision «Ternopil Professional College of Ternopil Ivan Puluj National Technical University»

ANALYSIS OF CYBERATTACKS ON CRITICAL INFRASTRUCTURE OF UKRAINE

Supervisor**:** Halyna Radchyk

Ключові слова: кібератака, кібербезпека
Keywords: cyberattack, cybersecurity

Кіберпростір став невід'ємною частиною життя кожної сучасної людини. Він сприяє вирішенню соціальних проблем, розвитку освіти, науки, культури, бізнесу і має великий потенціал для економічного зростання та інновацій. Кіберпростір відкриває нові можливості для бізнесу, такі як електронна комерція, онлайн-банкінг та дистанційна робота, надає доступ до онлайн-курсів, вебінарів та інших освітніх ресурсів.

Зі зростанням кількості підключених до Інтернету пристроїв та систем збільшується кількість потенційних вразливостей, які можуть бути використані кіберзлочинцями. У кіберпросторі розвиваються кіберзлочинність, шпигунство в політичних чи економічних цілях, атаки на критичну інфраструктуру (транспорт, енергетику, зв’язок тощо) з метою диверсій.

З початком російської агресії проти України, кіберпростір став одним з основних полів бою. РФ постійно проводить кібератаки на українську інфраструктуру, намагаючись дестабілізувати ситуацію.

В умовах війни в Україні, захист критичної інфраструктури є одним з пріоритетних завдань держави. З початку повномасштабного вторгнення збільшилась кількість кібератак, зросла відповідальність за безпеку передачі інформації. Ці атаки можуть призвести до порушення роботи життєво важливих систем, таких як енергетика, транспорт, фінанси та телекомунікації.

Інститут CyberPeace документує кібератаки на критичну інфраструктуру та цивільні об’єкти з початку російсько-агресорської війни проти України. За даними CyberPeace Institute, з січня по вересень 2022 року в Україні було зафіксовано 166 великих кібератак. Станом на 31 травня 2023 року Інститут зафіксував 1998 кібератак і операцій, здійснених 98 різними суб'єктами. За даними Держспецзв'язку, у 2024 році кількість кібератак на Україну зросла майже на 70%.

Загалом можна графічно відобразити тенденції росту кібератак на критичну інфраструктуру України. Це продемонстровано на рисунку 1.

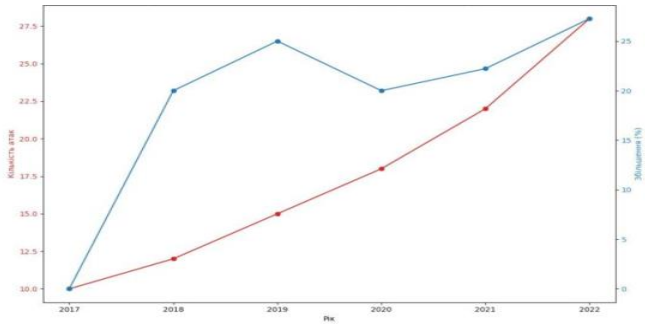

Рисунок 1 – Тенденція росту кібератак

РФ неодноразово намагалася вивести з ладу українську енергосистему за допомогою кібератак. Енергетична інфраструктура України зазнала численних атак, спрямованих на порушення електропостачання та дестабілізацію ситуації. Особливо яскравим прикладом є кібератаки 2015 та 2016 років, коли російські хакери змогли відключити електропостачання в деяких регіонах України.

12 грудня 2023 року в роботі найбільшого в Україні оператора зв'язку «Київстар» стався масштабний збій, внаслідок якого по всій країні в абонентів «Київстар» зник мобільний зв'язок та інтернет. Мережа «Київстар» стала мішенню потужної хакерської атаки, що спричинила технічний збій. В результаті цієї атаки тимчасово стали недоступні послуги зв'язку та доступу в інтернет.

Під час війни фінансова інфраструктура України постійно перебуває під прицілом кіберзлочинців. З початком повномасштабного вторгнення Росії, інтенсивність кібератак на фінансову інфраструктуру України значно зросла. Найпоширенішими типами атак є DDoS-атаки, фішинг, використання шкідливого програмного забезпечення та атаки на системи дистанційного банківського обслуговування.

РФ активно використовує дезінформаційні кібератаки як інструмент гібридної війни, особливо проти України. Російські хакерські групи та пропагандистські ресурси постійно поширюють дезінформацію з метою дестабілізації ситуації в Україні та підриву її міжнародної підтримки. Дезінформаційні кібератаки можуть призвести до дестабілізації суспільства, поширення паніки та недовіри до державних органів. Вони можуть бути використані для маніпулювання виборами, розпалювання конфліктів та підриву міжнародної безпеки.

Саме тому питання забезпечення інформаційної і кібербезпеки країни нині є надзвичайно актуальним. В Україні активно вживаються заходи для підвищення кібербезпеки критичної інфраструктури, особливо в умовах постійних кібератак. Посилюється співпраця між державними органами, приватним сектором та міжнародними партнерами. Ефективний захист критичної інфраструктури вимагає комплексного підходу, який поєднує як технічні, так і організаційні заходи, а також постійного моніторингу та адаптації до нових загроз. Прикладом цього є проєкт USAID «Кібербезпека критично важливої інфраструктури України», співпраця з Академією електронного управління Естонії (eGA). Держспецзв'язку активно співпрацює з eGA у рамках проєкту «Готовність кібербезпеки для критичної інфраструктури в Україні».

Одним із ефективних методів захисту є використання штучного інтелекту (ШІ) та машинного навчання (ML). ШІ та ML можуть аналізувати величезні обсяги даних з мереж, систем та пристроїв для виявлення незвичайних закономірностей, які можуть свідчити про кібератаку. Виявляти як відомі, так і нові, невідомі раніше загрози (zero-day attacks), які можуть пропустити традиційні системи захисту. ШІ може автоматизувати процеси реагування на кіберінциденти, такі як блокування шкідливого трафіку, ізоляція уражених систем та запуск процедур відновлення.