УДК 004.056.53:004.8:[334.716-021.412.1:355.45
DOI: 10.31673/2409-7292.2025.031896

Савченко В.А, Хавер А.В.

ОЦІНКА ВПЛИВУ ПРОГРАМНИХ ІНСТРУМЕНТІВ НА ОСНОВІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА РЕСУРСНУ ЕФЕКТИВНІСТЬ ЩОДО ПРОВЕДЕННЯ ДЕСТРУКТИВНИХ КІБЕРОПЕРАЦІЙ ПО ВІДНОШЕННЮ ДО ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Розвиток технологій штучного інтелекту безпосередньо виступив каталізатором розвитку для суб'єктів кіберпростору. Сучасні програмні інструменти, які використовують можливості технологій штучного інтелекту активно використовуються як з боку "етичних хакерів" (фахівців кібербезпеки), зокрема в засобах кіберзахисту антивірусних програм, EDR/XDR, SIEM, CTI-платформах, так і з боку суб'єктів кіберзагрози (хакерів). За оцінками компанії з кібербезпеки "Crowdstrike" суб'єкти кіберзагрози, зазвичай, найчастіше використовують програмні інструменти на основі технологій ШІ у двох випадках: для швидкого написання програмного коду ШПЗ/payload/скрипту та для підготовки текстово-візуальних компонентів фішингу. Крім того, фахівцями з кібербезпеки фіксуються численні модульні AI-платформи для написання шкідливого коду, проведення соціальної інженерії, вибору і реалізації процедур MITRE, Darknet – розвідки та реверс-інжинірингу та інш. Використання таких програмних засобів дозволяє суб'єктам кіберзагрози значно скоротити фінансові, часові та людські ресурси для проведення, у тому числі деструктивних кібератак в рамках кібероперацій проти об'єктів критичної інфраструктури. Завдяки впровадженню та адаптації таких доступних програмних рішень зловмисники можуть обійтися без участі окремих вузькопрофільних технічних фахівців, досконалого знання мов програмування та істотно скоротити час життєвого циклу кібероперації в декілька разів, що підвищує масовість таких заходів. У перспективі цей процес створює нові виклики для систем кіберзахисту держав з урахуванням зростаючого впливу інтелектуальних технологій, які стають все більш функціонально збагаченими і все більш доступними.

Ключові слова: штучний інтелект (ШІ), програмні інструменти на основі технології ШІ, кібероперація, кібератака, спеціалізоване технологічне троянське програмне забезпечення, об'єкт критичної інфраструктури, Stuxnet.

Вступ

Найбільш небезпечними загрозами для функціонування об'єктів критичної інфраструктури держави з кіберпростору є деструктивні кібератаки суб'єктами кіберзагрози, які спонсоруються іноземними державами. Причому деструктивні кібератаки на комунікаційну систему підприємства, зазвичай, є менш критичними для відновлення ніж аналогічні кібератаки на технологічну систему підприємства. Варто зауважити, що кібератака на технологічну систему потребує значних затрат ресурсів з боку зацікавленої сторони (фінансових, часових, людських) та з високою ймовірністю може бути здійснена у рамках проведення кібероперації.

Проте, сучасні загальнодоступні та пропрієтарні програмні інструменти на основі технологій штучного інтелекту дозволяють суб'єктам кіберзагрози значною мірою скоротити часові та людські ресурсні витрати на реалізацію такої кібероперації. Численні технічні звіти провідних компаній з кібербезпеки свідчать про активне використання таких інструментів з боку суб'єктів кіберзагроз. Цей факт, в свою чергу, збільшує актуальність загроз щодо численності та інтенсивності проведення деструктивних кібератак на об'єкти критичної інфраструктури.

Аналіз останніх досліджень

Аналіз останніх наукових досліджень і публікацій (за результатами аналізу публікацій на платформах "Scopys" та "Web of Science") щодо використання програмних інструментів на основі технологій штучного інтелекту для дій в кіберпросторі показав здебільшого зосередження авторів на темі кібербезпеки та підвищення рівня кіберстійкості за допомогою таких засобів (кіберзахисту інформаційно-комунікаційних систем, близько 90% робіт). Окремі наукові дослідження іноземних авторів були присв'ячені використанню програмних інструментів на основі технологій штучного інтелекту суб'єктами кіберзагроз [1-2]. Зокрема в вищезазначених роботах розглядалася тематика використання чат-ботів на основі технологій штучного інтелекту для проведення кібератак та використання технологій штучного інтелекту для генерації шкідливого коду в рамках

автоматизованої кібератаки. Проте, розглянуті автором роботи не розкривали дослідження використання програмних інструментів на основі технологій штучного інтелекту в рамках проведення деструктивних кібероперацій та не оцінювали їх ефективність у цьому процесі.

Мета дослідження

Проведення оцінки ресурсної ефективності залучення програмних інструментів на основі технології ШІ при реалізації деструктивних кібероперацій на об'єкти критичної інфраструктури.

Основними завданнями дослідження є:

- проаналізувати алгоритм деструктивної кібероперації;
- розглянути основні класи програмних інструментів на основі технологій ШІ та їх спеціалізацію в контексті реалізації алгоритму деструктивної кібероперації;
- порівняти ефективність щодо скорочення часових та людських ресурсів у процесі проведення деструктивної кібероперації з використанням програмних інструментів на основі технологій ШІ та без їх використання (на прикладі кібероперації "Stuxnet").

Основна частина

Деструктивні кібератаки на об'єкти критичної інфраструктури (далі – ОКІ) здійснюються з метою порушення функціонування об'єктів критичної інформаційної інфраструктури такого ОКІ, а саме комунікаційної (ІТ/корпоративна) чи/та технологічної (ОТ/промислова) систем. Кінцева цільова система ураження ОКІ обирається суб'єктом кіберзагрози враховуючи множину можливих ефективних векторів здійснення кібератаки. Така кібератака, яка має на меті деструктивні кібердії по відношенню до ОКІ, з високою ймовірністю здійснюється суб'єктами кіберзагрози, які спонсоруються зацікавленою державою (-ми) в рамках проведення військової кібероперації. Важливо зазначити, що такі терміни як "кібероперація" та "кібератака" в сучасних публікаціях публіцистичного, художнього та навіть наукового характеру часто використовують як синоніми, якими вони не є. Термін "кібероперація" є ширшим поняттям, стосується переважно військової сфери та за своїм характером може включати як одну так і декілька кібератак (в подальшому контексті дослідження розглядається варіант коли в рамках кібероперації здійснюється одна кібератака), в тому числі на ОКІ держави-противника для досягнення мети і завдань військового характеру з використанням кіберзброї. Згідно "Tallin manual 2.0 on the international law applicable to cyber operations" термін кібероперація визначається як "застосування кіберзасобів з метою досягнення поставлених завдань у межах або за допомогою кіберпростору" [3]. Кібератака ж може використовуватися на певних етапах кібероперації як основний механізм досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [4].

У разі, якщо суб'єктом кіберзагрози здійснюється деструктивна кібератака на технологічну систему ОКІ то одним із його завдань є отримання доступу до її основних інформаційних підсистем – Basic process control system (далі – BPCS) та Safety instrumented system (далі – SIS). BPCS – це інформаційна підсистема технологічної системи ОКІ, яка призначена для здійснення моніторингу за станом технологічного процесу та управлінні ним. SIS – це інформаційна підсистема технологічної системи ОКІ, яка призначена для забезпечення безпеки експлуатації технологічного об'єкта, контролю аварійних процедур і у разі виникнення аномалій, приведення технологічного процесу до безпечного стану.

Для ураження SIS суб'єктом кіберзагрози майже напевно буде використано спеціалізоване технологічне троянське програмне забезпечення (далі – СТТПЗ). Автор пропонує наступну дефініцію терміну "СТТПЗ" –це вид кіберзброї, що маскується від засобів виявлення та/або імітує легітимне програмне забезпечення, може мати функції віддаленого управління та призначене для застосування в конкретній технологічній мережі/конкретних типах технологічних мереж (з

урахуванням технологічних особливостей будови інформаційних систем) з метою здійснення кібершпигунства чи/та деструктивного кібервпливу.

Автор пропонує розглянути алгоритм проведення деструктивної кібероперації по відношенню до ОКІ, а саме його технологічної складової (далі – алгоритм деструктивної кібероперації), в який, в частині безпосередньо проведення кібератаки за основу покладено “Cyber kill chain” (проте внесено певні модифікації на його окремих етапах). Безпосередньо “Cyber kill chain” – це фреймворк, розроблений у 2011 році оборонно-промисловою компанією США “Lockheed Martin” [5]. Він відображає лінійну прогресію етапів кібератаки та описує наступні 7 етапів її проведення: “розвідка”, “озброєння”, “доставка”, “експлуатація”, “встановлення”, “підвищення привілеїв”, “дія над цільовою системою”.

Запропонований алгоритм деструктивної кібероперації складається з наступних 12 етапів: “планування”, “розвідка”, “озброєння”, “написання тестового зразка СТТПЗ та його тестування”, “доставка”, “етап експлуатації привілеїв”, “підтримання скритності і маскування”, “підготовка до дій над об'єктом”, “дія над об'єктом”, “замітання слідів”, “завершення”, “аналіз результатів”. На думку автора такий етап як “написання тестового зразка СТТПЗ та його тестування” є невід’ємною складовою кібероперацій, які мають на меті в тому числі (крім втручання в роботу BPCS) здійснювати втручання в функціонування SIS (тобто нести деструктивний а не кібершпигунський характер).

2. Програмні інструменти на основі технологій ШІ (далі – ПІОТ ШІ), зазвичай, ґрунтовно використовуються суб'єктами кіберзагрози в рамках реалізації алгоритму деструктивної кібероперації на етапах від “планування” до “аналізу результатів” включно. Концептуальна класифікація таких ПІОТ ШІ базується на основі функціональних ознак та типів ШІ-технології, що використовується та є наступною:

- машинне навчання (далі – ML);
- глибоке навчання (далі – DL);
- навчання з підкріпленням (далі – RL);
- нейромовні моделі (NLP, зокрема, її класу LLM (далі – LLM));
- еволюційні алгоритми (далі – Genetic AI);
- гібридні системи ШІ [6].

Зокрема, ML характеризується використанням алгоритмів класифікації, кластеризації, дерева рішень, регресії. Одним із шляхів використання з боку суб'єктів кіберзагрози цієї технології є вибір найбільш вдалого вектору початкового доступу в цільову систему, найбільш вразливої цільової системи (вузла) в підсистемах BPCS та/або SIS [7].

DL характеризується використанням нейронних мереж, аналізу складних даних, генерацією поведінкових шаблонів, для виявлення складних закономірностей у даних (навіть у так званих “сирих” даних). Як один з варіантів використання DL суб’єктами кіберзагрози в рамках алгоритму проведення деструктивної кібероперації — створення моделі симуляції поведінки технологічного процесу за допомогою глибокої нейронної мережі, яка в подальшому може використовуватися для імітації нормальних даних на Human machine interface для введення в оману інженера/оператора інформаційної підсистеми BPCS чи SIS.

RL характеризується адаптивним прийняттям рішень у динамічному середовищі. Наприклад, може використовуватися для побудови маршруту “бічного переміщення” при виборі подальшого вектору кібератаки на цільову систему BPCS – SCADA.

LLM, перш за все характеризуються генерацією текстів в тому числі написанням скриптів та/або коду СТТПЗ, руткітів та інш. (наприклад, “LAMEHUG”) [8].

Genetic AI характеризується використанням алгоритмів, які базуються на імітації принципів природнього добору (мутації, кросовери, відбір найкращих зразків, для знаходження оптимальних рішень в умовах складного пошуку). Такі алгоритми можуть бути використані суб'єктами кіберзагрози для *автоматизованої генерації численних варіантів шкідливого коду* (в тому числі модифікації існуючих готових СТТПЗ) для створення оптимальної обфускації та вдосконалення

зразків, які найкраще будуть маскуватися від антивірусного програмного забезпечення, уникати виявлення в конкретних системах EDR та/або HIDS. Такими загальнодоступними ПІОТ ШІ, зокрема, є “GAMMA (Genetic Algorithm for Malware Mutation & Analysis)”, “GA Wrapper” та Python бібліотека “DEAP”.

Гібридні системи ШІ характеризуються симбіозом підкласів технологій ШІ, наприклад ML+DL+LLM або RL+LLM для багатофункціональних агентів. Практичними прикладами таких автономних агентів є “AutoGPT”, “LLMRecon”, “Red-Team Agents”. Найчастіше саме такі багатофункціональні інструменти використовуються суб'єктами кіберзагрози під час проведення сучасних деструктивних кібероперацій на ОКІ.

Розглянемо використання вищезазначених ПІОТ ШІ по відношенню до етапів алгоритму деструктивної кібератаки.

На етапі “планування” ПІОТ ШІ може використовуватися обмежено, ймовірно, обходячись засобами LLM (наприклад, у випадку відсутності певної технічної інформації/ певного технічного фахівця).

Зазвичай, ПІОТ ШІ більш активно використовуються починаючи з 2-го етапу - “розвідка”. На цьому етапі найбільшу ефективність показують LLM-агенти з OSINT-модулями. Наприклад, агент “AutoGPT” чи “LLMRecon” з підключеними модулями GoogleSearch, GitHubSearch, Whois, ShodanAPI та інш., що допомагають знайти всі відкриті та доступні з мережі Інтернет ресурси ОКІ тим або іншим чином пов'язані технологічною системою, BPCS та/або SIS. Результатом даного етапу буде автоматизоване формування початкового звіту про технологічну систему цільового ОКІ та її складові для подальшого аналізу та доповнення [5].

На етапі 3 - “озброєння” суб’єктами кіберзагрози використовуються дані зібрані на попередньому етапі. Найбільшу ефективність на даному етапі продемонструють гібридні системи ШІ, наприклад з функціоналом LLM+RL+ML, які будуть адаптивно працювати з TTP базами знань (MITRE ATT&CK, ICS-ATT&CK) та розвідувальними даними здобутими на етапі “розвідки”. Результатом етапу “озброєння” є індивідуалізований профіль атаки, який може включати: ланцюг технік за MITRE ATT&CK та/або ICS ATT&CK; опис основних вимог до функціоналу СТТПЗ та основних і запасних способів його доставки; алгоритм реалізації бічного переміщення до цільової системи; способи уникнення виявлення зловмисної активності та обходу основних елементів кіберзахисту; алгоритм розгортання і реалізації командно-контрольної інфраструктури та інш. Тобто, по суті цей етап дозволяє сформулювати своєрідний “технічний паспорт” кібератаки.

На етапі “написання тестового зразка СТТПЗ та його тестування” ПІОТ ШІ є найбільш ефективними та ресурсоекомомними засобами. Даний етап передбачає роботу програмістів з текстом коду окремих модулів зразка СТТПЗ, тому в даному випадку найбільшу ефективність показують рішення на базі LLM (наприклад, комбінація таких моделей як “Claude 3 Opus”, “Phind v2”, “Code Llama 70B”, “WizardCoder”). Тестові зразки СТТПЗ (скриптів, бібліотек, руткітів і інш.) можуть тестуватися завдяки ML на ймовірність виявлення конкретними засобами кіберзахисту.

“Доставка” СТТПЗ і відповідно використання ПІОТ ШІ на для подальшого використання в BPCS та SIS буде мати відмінності. Для BPCS даний етап може бути реалізовано завдяки прямому доступу в цільову систему через вихід у мережу Інтернет. Ймовірність того, що в BPCS буде успішно реалізовано, наприклад, тактику “перехоплення ланцюжка поставок” вища аніж того, що буде успішно здійснено фішингове надсилання і активація СТТПЗ. Враховуючи цей факт серед ПІОТ ШІ для BPCS на етапі доставки ефективнішим буде використання LLM (щонайменше для моделювання сценаріїв перехоплення ланцюжка поставок та інш.). Для SIS цей етап, з високою долею ймовірності, буде реалізовано через з’ємний носій, для чого може бути використаний такий функціонал ПІОТ ШІ як кастомізація носія, реалізація стелс-логіки (затримка запуску, запуск по події, запуск за ознакою, наприклад ім'ям хосту), вибір оптимального сценарію активації, вибір вектору запуску, створення селективної активації (зразок СТТПЗ буде виконуватися лише на конкретній цільовій системі (комп'ютері)) та реалізації механізмів антифорензики. Наприклад, кастомізація носія може бути виконана LLM; стелс-логіка реалізована завдяки LLM з Embedded

Logic Generator; вибір оптимального сценарію активації передбачає використання RL; вибір вектору запуску, селективна активація, антифорензика – LLM.

“Етап експлуатації привілеїв” також буде відмінним щодо використання ПІОТ ШІ для BPCS та SIS відповідно. При віддаленій взаємодії суб'єкта кіберзагрози з BPCS (коли з цільової системи є доступ до мережі Інтернет) ПІОТ ШІ можуть використовуватися суб'єктом кіберзагрози “на гарячу”, наприклад, для узгодження своїх дій через використання LLM. У разі якщо BPCS ізольована то як і у випадку з SIS ПІОТ ШІ будуть застосовані на етапі “написання тестового зразка СТТПЗ та його тестування”. Вищезазначене стосується і таких етапів операції як “підтримання скритності і маскування”, “підготовки до деструктивних дій”, “дія над об'єктом” та “замітання слідів”.

3. Для проведення порівняння ефективності щодо скорочення часових та людських ресурсів з використанням програмних інструментів на основі технологій ШІ та без їх використання, на прикладі кібероперації “Stuxnet” автор пропонує скористатися PERT-аналізом (Program Evaluation and Review Technique) [9]. Кібератака СТТПЗ “Stuxnet” була спрямована на інформаційну підсистему SIS (основна ціль), проте як точку входу в цільову систему використовувала інженерну станцію BPCS. СТТПЗ “Stuxnet” змінювало логіку в PLC Siemens S7-315 і S7-417, які використовувались у захисних сценаріях (SIS), наприклад, керували швидкістю центрифуг, щоб запобігти аварії.

PERT-аналіз – це мережевий метод управління проєктами, що належить до математичного розділу теорії ймовірностей, який дозволяє оцінити очікувану тривалість виконання задач, враховуючи невизначеність у їх тривалості. Такий підхід особливо доречний при використанні у складних проєктах, де кожен етап може мати значну варіативність затрат часових та людських ресурсів (що й відповідає реалізації алгоритму деструктивної кібероперації). Кожна задача згідно зазначеного методу має три ймовірні сценарії розвитку: “оптимістичний”, “реалістичний/найбільш ймовірний” та “песимістичний”. Метод використовує формулу зваженого середнього, де кожному сценарію присвоюється коефіцієнт. “оптимістичний” сценарій має коефіцієнт – 1, “реалістичний” – 4, “песимістичний” – 1. Згідно методу PERT-аналізу найбільший коефіцієнт зумовлений практичним досвідом, найменшою залежністю від ризиків та має вагу вдвічі більшу за суму “оптимістичного” та “песимістичного” сценаріїв (відповідно 66% вірогідності на противагу 17% вірогідності для оптимістичного та песимістичного сценаріїв). Відтак, загальна вага коефіцієнтів в чисельнику складає – 6 і для розрахунку середньозваженого значення цей показник використано в знаменнику як стале значення.

Формула (1) PERT-аналізу для вирішення вищеописаного завдання зображена нижче:

$$T_{PERT} = \frac{О+4Р+П}{6}, \quad (1)$$

де О – кількісне значення оптимістичного коефіцієнта; Р – кількісне значення реалістичного коефіцієнта; П – кількісне значення песимістичного коефіцієнта.

В подальшому дослідженні запропоновано пов'язати можливі сценарії реалізації алгоритму деструктивної кібероперації (оптимістичний, реалістичний, песимістичний) із рівнем критичності об'єкта критичної інфраструктури (ОКІ), виходячи з припущення, що вищий рівень критичності ОКІ, зазвичай відповідає більш розвиненій системі кіберзахисту та вищому рівню кіберстійкості, а отже – потребує більших затрат щодо часових і людських ресурсів з боку суб'єкта кіберзагрози для проведення успішної кібератаки.

Згідно з вищезазначеним, оптимістичний сценарій, що передбачає мінімальні ресурсні витрати, є найбільш імовірним у випадку атаки на найменш критичні ОКІ – об’єкти які можуть мати низький рівень кіберзахисту або застарілу інфраструктуру. Реалістичний же сценарій корелює з ОКІ середнього класу критичності, з помірним рівнем безпеки, де існують чіткі вимоги до наявності базових заходів контролю та моніторингу. Песимістичний сценарій, найбільш ймовірний у випадку

цілеспрямованої атаки на критичні об’єкти, важливість сталого функціонування яких має вплив державного масштабу. В інформаційній інфраструктурі таких об'єктів, зазвичай впроваджено глибокоешелоновану оборону (стратегія “Defense in depth”), ізоляцію критичних сегментів та контроль доступу високого рівня з багатофакторною автентифікацією користувачів.

Надалі, в рамках дослідження будемо враховувати, що всі розрахунки щодо часових та людських затрат буде зазначено для підготовки до деструктивної кібератаки одночасно на інформаційну інфраструктуру BPCS та SIS (тобто сумарно). Так як саме вплив на обидві вищезазначені інформаційні підсистеми дозволяє здійснити деструктивний кібервплив на функціонування ОКІ. Проте, окремі етапи реалізації алгоритму деструктивної кібероперації з використанням ПІОТ ШІ можливі лише для інформаційної підсистеми BPCS так як інформаційна підсистема SIS, зазвичай, є ретельно ізольованою, незалежно від класу критичності цільового ОКІ [10].

Для подальшого вирішення завдання дослідження необхідно виокремити кожен етап алгоритму деструктивної кібероперації та оцінити за кожним сценарієм PERT-аналізу час необхідний для виконання кожного з етапів алгоритму проведення деструктивної кібератаки на ОКІ та кількісний показник людського ресурсу, необхідний для його успішної реалізації, якщо б суб'єкти кіберзагрози використовували ПІОТ ШІ (табл. 1).

Таблиця 1

PERT-аналіз часових і людських ресурсів в рамках виконання алгоритму реалізації деструктивної кібероперації на технологічну систему ОКІ

№з/п	Етапи деструктивної кібероперації	Оптимістичний сценарій (робочих днів/людського ресурсу)	Найбільш ймовірний/реалістичний сценарій (робочих днів/людського ресурсу)	Песимістичний сценарій (робочих днів/людського ресурсу)	PERT-оцінка (робочих днів/людського ресурсу усереднене значення)
1.	Планування	6	10	20	11
		5	7	10	7
2.	Розвідка	50	80	120	82
		3	7	10	7
3.	Озброєння	10	15	30	17
		3	5	7	5
4.	Написання тестового зразка СТТПЗ та його тестування	70	90	150	97
		6	8	10	8
5.	Доставка	30	65	90	63
		3	4	5	4

6.	Етап експлуатації привілеїв (лише для BPCS при наявності доступу до зовнішньої мережі)	0,5	1	3	1,25
		1	1	1	1
7.	Підтримання скритності і маскування (лише для BPCS при наявності доступу до зовнішньої мережі)	1	2	4	2
		1	1	1	1
8.	Підготовка до деструктивних дій над цільовою системою (лише для BPCS при наявності доступу до зовнішньої мережі та залежить від специфіки завдання)	1	14	30	14,5
		1	1	1	1
9.	Дія над об'єктом (лише для BPCS)	0,2	0,5	1	0,5
		1	1	1	1
10.	Замітання слідів (лише для BPCS)	Використання засобів ПІОТ ШІ не вплине на ресурсні витрати	Використання засобів ПІОТ ШІ не вплине на ресурсні витрати	Використання засобів ПІОТ ШІ не вплине на часові витрати	–
11.	Завершення	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	–
12.	Аналіз результатів	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	Використання засобів ПІОТ ШІ не вплине на часові/людські витрати	–

Кількість людського ресурсу в Таблиці 1 зазначена виходячи з функціональних ролей фахівців. Наприклад, на етапі алгоритму деструктивної кібероперації “Планування” за оптимістичного сценарію (на думку автора) залучається 5 фахівців. На практиці це відповідає 3-4 особам керівного складу та 2-1 фахівцю-практику за напрямком знання технологічних систем (знанням Industrial control system). За реалістичного сценарію збільшиться кількість професійних фахівців-практиків

(додадуться представники напрямків OSINT та розробки/ОТ-аналітик/ спеціаліст HUMINT). За песимістичного сценарію, що визначається 10-ма особами, буде залучена менша кількість представників керівного складу і збільшено участь технічних спеціалістів, які за своїми професійними якостями не здатні в повній мірі реалізувати бачення стратегічних аспектів проведення операції.

Кількість часового ресурсу в Таблиці 1 зазначена виходячи з мінімальних термінів проведення етапу на кожен сценарій. Наприклад, на етапі алгоритму деструктивної кібероперації “Планування” за оптимістичного сценарію буде затрачено 6 робочих днів. Така тривалість пов'язана з кількістю підпунктів даного етапу, наявним досвідом, можливістю швидко виконати всі заходи планування та передбачає: визначення цілей операції; оцінка категорії критичності ОКІ та його потенційно вразливих місць; вибір векторів кібератаки; вибір типу кібератаки; визначення необхідності застосування вразливостей нульового дня; аналіз наявного практичного досвіду у реалізації обраних підходів, доступних інструментів та ресурсів; формування часових рамок проведення операції; делегування завдань; формування планувального документу з описом стратегії та тактики проведення операції.

Таким чином, обрахуємо загальну PERT-оцінку часових та людських ресурсів для виконання деструктивної кібероперації на ОКІ.

Оптимістичний сценарій проведення операції з використанням ПІОТ ШІ передбачає:

людських затрат (за умови , що кожен окремий фахівець працює над одним напрямком робіт, а етапи з 6 по 11 виконує один спеціаліст) – 21;

часові затрати (за умови, що пункти 9-11 виконуються суб'єктом кіберзагрози максимально швидко) – 118,7 робочих днів (з урахуванням стандартного “робочого” місяця з двома вихідними днями щотижня та тим фактом, що кожен етап операції проводиться послідовно — наступний після попереднього (а не паралельно) за оптимістичного сценарію виконання операції займе близько 5 місяців).

Реалістичний сценарій проведення деструктивної кібероперації з використанням ПІОТ ШІ передбачає:

- людських затрат (за умови , що кожен окремий фахівець працює над одним напрямком робіт, а етапи з 6 по 11 виконує один спеціаліст) – 32;

- часові затрати (за умови, що пункти 9-11 виконуються суб'єктом кіберзагрози максимально швидко) – 277,5 робочих днів (з урахуванням стандартного “робочого” місяця з двома вихідними днями щотижня та тим фактом, що кожен етап операції проводиться послідовно — наступний після попереднього (а не паралельно) за реалістичного сценарію виконання операції займе близько 12 місяців (1 року).

Песимістичний сценарій проведення деструктивної кібероперації з використанням ПІОТ ШІ передбачає:

- людських затрат (за умови , що кожен окремий фахівець працює над одним напрямком робіт, а етапи з 6 по 12 виконує один спеціаліст) – 43;

- часові затрати (за умови, що пункти 9-12 виконуються суб'єктом кіберзагрози максимально швидко) – 448 робочих днів (з урахуванням стандартного “робочого” місяця з двома вихідними днями щотижня та тим фактом, що кожен етап операції проводиться послідовно – наступний після попереднього (а не паралельно) за реалістичного сценарію виконання операції займе близько 22, 4 місяці, тобто 1 рік і 10 місяців.

Усереднена PERT-оцінка щодо використання часових та людських ресурсів під час проведення деструктивної кібероперації з використанням ПІОТ ШІ передбачає:

- людських затрат (за умови , що кожен окремий фахівець працює над одним напрямком робіт, а етапи з 6 по 12 виконує один спеціаліст) – 32;

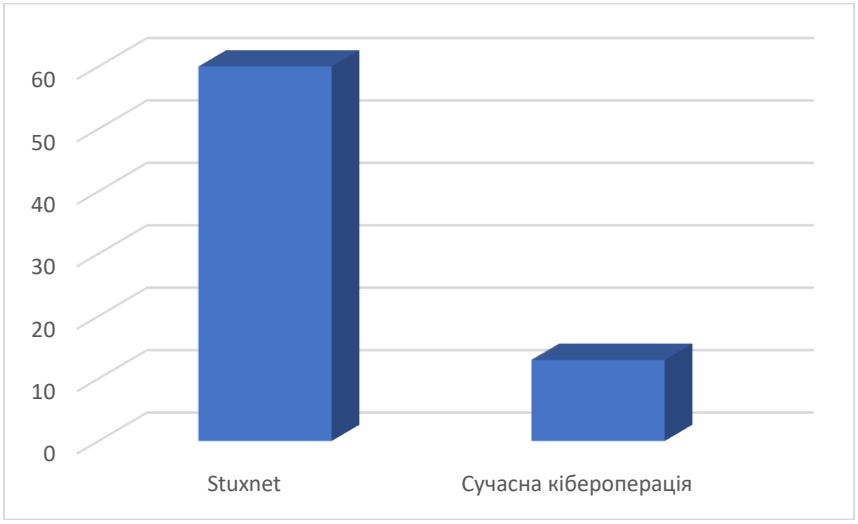
- часові затрати (за умови, що пункти 9-12 виконуються суб'єктом кіберзагрози максимально швидко) – 288, 25 робочих днів (з урахуванням стандартного “робочого” місяця з двома вихідними днями щотижня та тим фактом, що кожен етап операції проводиться послідовно – наступний після

попереднього (а не паралельно) за усередненого сценарію виконання операції займе близько 13 місяців, тобто 1 рік і 1 місяць.

Порівняємо результати щодо використання часових та людських ресурсів у ході проведення операції “Stuxnet” та потенційної сучасної деструктивної кібероперації до проведення якої задіяно програмні інструменти на основі технології ШІ за результатами PERT-оцінки [11] з Таблиці 1 (Діаграма 1-2).

Аналізуючи наявні в відкритих джерелах відомості щодо проведення найбільш безпрецедентної деструктивної кібероперації “Stuxnet” можна наближено визначити такі вихідні дані, що під час цієї кібероперації сумарна кількість часових затрат для реалізації усіх етапів алгоритму деструктивної кібероперації становила близько 5-ти років, а людських ресурсів згідно експертних оцінок до програмної реалізації СТТПЗ було задіяно близько 50 осіб (включаючи розробників шкідливого ПЗ, OSINT-аналітиків, реверс-інженерів, фахівців з мережевої інфраструктури, QA-інженерів, фахівців із промислових систем (ICS/SCADA), персонал експериментального лабораторного середовища та інш). Зокрема, зазначена інформація щодо часових і кількісних показників кібероперації “Stuxnet” зазначена в публікації технічного журналу IEEE “Spectrum” з посиланням на книгу Kim Zetter “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon” (2014 р.) [12].

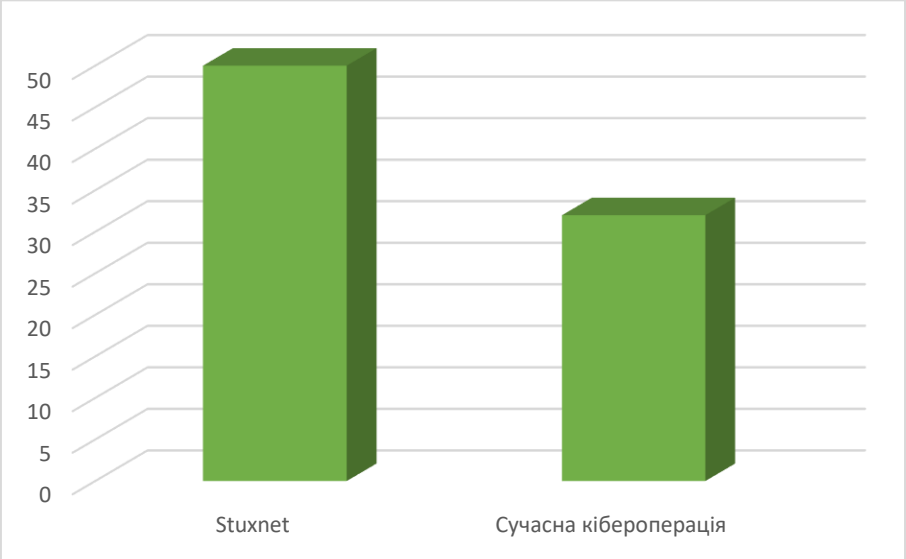
Так як у ході дослідження неможливо отримати дані щодо часових затрат на проведення кожного етапу (фази) кібероперації “Stuxnet” можна порівняти виключно кінцеві показники ресурсних затрат (часових та людських ресурсів) за PERT-оцінкою з результатів за Таблицею 1.



Діаграма 1. Результати порівняння часових ресурсів необхідних для реалізації повного алгоритму деструктивної кібеорперації “Stuxnet” та потенційної сучасної деструктивної кібероперації до проведення якої задіяно ПІОТ ШІ

Порівнюючи затрати по часових ресурсах відповідно до аналізу Діаграми 1 можна вважати, що сучасні деструктивні кібероперації, які проводяться з використанням ПІОТ ШІ дозволяють значно скоротити витрати часового ресурсу на їх реалізацію. У конкретному прикладі ПІОТ ШІ дозволяють заощадити в 5 разів більше часу (тобто подібна кібероперація до “Stuxnet” могла би бути реалізована до 5 разів швидше).

Порівнюючи затрати людського ресурсу відповідно до аналізу Діаграми 2 можна вважати, що сучасні деструктивні кібероперації, які проводяться з використанням ПІОТ ШІ дозволяють скоротити витрати людського ресурсу на їх реалізацію. У конкретному прикладі ПІОТ ШІ дозволяють заощадити в 1,5 рази більше часу (тобто подібна кібероперація до “Stuxnet” могла би бути реалізована залучивши в 1,5 разів менше виконавців).



Діаграма 2. Результати порівняння людських ресурсів необхідних для реалізації повного алгоритму деструктивної кібеорперації "Stuxnet" та потенційної сучасної деструктивної кібероперації до проведення якої задіяно ПІОТ ШІ

Висновки

Таким чином, узагальнюючи результати даного дослідження можна підсумувати наступне:

- всі сценарії реалізації деструктивних кібероперацій можна описати єдиним алгоритмом, який за виключенням самої кібератаки буде містити етапи планування, розвідки та оцінки результатів;

- сучасні кібероперації можуть проводитися з набагато меншими ресурсними витратами ніж це було раніше, завдяки використанню різноманітних класів ПІОТ ШІ;

- використання в процесі проведення деструктивних кібероперацій ПІОТ ШІ значно дозволяє скоротити часові витрати та частково скоротити людські витрати (переважно в частині широкопрофільних. фахівців за рахунок автоматизації задач OSINT, аналізу вразливостей і частково – реверс-інжинірингу, тестування. Водночас, наприклад фахівці з ICS/SCADA і лабораторного моделювання залишаються критично необхідними, оскільки їх експертність наразі складно замінити навіть найсучаснішими інструментами ШІ).

Отже, програмні засоби на основі технологій штучного інтелекту є високоефективним інструментом під час реалізації деструктивних кібероперацій на об'єкти критичної інфраструктури.

Перелік посилань

1. Kiran Maraju, Rashu, Tejaswi Sagi "Hackers Weaponry: Leveraging AI Chatbots for Cyber Attacks"// Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media (pp.385-398), February 2024;

2. Calvin NMN Nobles Offensive Artificial Intelligence in Cybersecurity: Techniques, Challenges, and Ethical Considerations // Real-World Solutions for Diversity, Strategic Change, and Organizational Development (pp.348-363), June 2023;

3. Michael N. Schmitt, Liis Vihul "Tallin manual 2.0 on the international law applicable to cyber operations", Cambridge university press, 2017, p. 564;

4. ЗУ "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text;

5. Kareem K., Naik N., Jenkins P., Grace P., Song JP., "Understanding the Defence of Operational Technology Systems: A Comparison of Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework, and Diamond Model", Contributions presented at the international conference on computing, communication, cybersecurity and AI, 2024;

6. Maathuis C. "Human-Centred AI in Military Cyber Operations", International Conference on Cyber Warfare and Security, 2024;

7. Donald G. Dunn, Eric Cosman "Cybersecurity Fundamentals Are Not Just for Industrial Control Systems: Guidance and Direction Are Available", IEEE, 2024;

8. Кібератаки UAC-0001 на сектор безпеки та оборони із застосуванням програмного засобу LAMEHUG, що використовує LLM (велику мовну модель) [Електронний ресурс] режим доступу доступу :https: // cert.gov.ua / article/6284730;

9. Kour, R , Karim, R, Dersin, P “Modelling cybersecurity strategies with game theory and cyber kill chain”, International journal of system assurance engineering and management, 2025;

10. F. Charmet, H. C. Tanuwidjaja, S. Ayoubi, P.-F. Gimenez, Y. Han, H. Jmila, G. Blanc, T. Takahashi, and Z. Zhang, “Explainable artificial intelligence for cybersecurity: a literature survey,” Annals of Telecommunications - annales des tel´ ecommunications ´ , vol. 77, no. 11-12, pp. 789–812, Dec. 2022. [Online]. Available: https: //hal.science/hal-03965590;

11. Gustavo Bergantinos and Juan Vidal-Puga “A value for PERT problems” [Електронний ресурс] режим доступу: https://www.worldscientific.com/doi/epdf/10.1142/S0219198909002418;

12. .K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown, 2014.

Надійшла 09.08.2025