DOI: https://doi.org/10.26642/ten-2024-2(94)-121-128
УДК 004.056

М.С. Колощук, асистент
О.Ю. Дячук, ст. викладач
О.О. Окунькова, ст. викладач
О.В. Пірог, к.т.н., доц.
Державний університет «Житомирська політехніка»

Інструменти штучного інтелекту для автоматизації тестування на проникнення

У статті розглянуто автоматизоване тестування на проникнення з використанням штучного інтелекту (ШІ), яке дозволяє значно підвищити ефективність і точність оцінки кібербезпеки. Технології на основі ШІ здатні автоматизувати багато процесів, що раніше виконувалися вручну, включно зі скануванням вразливостей, аналізом загроз та експлуатацією вразливих місць у системах. Особливу увагу приділено інструментам на базі ШІ, таким як DeepExploit, Sn1per та Cortex XSOAR, які демонструють суттєві переваги перед традиційними методами тестування на проникнення. У статті також розглянуто основні виклики впровадження ШІ у тестування на проникнення, зокрема труднощі навчання моделей та проблему помилкових спрацьовувань. Досліджуються майбутні тенденції у сфері використання ШІ для забезпечення кібербезпеки, такі як автономні системи тестування та інтеграція з квантовими обчисленнями.

Ключові слова: *штучний інтелект; тестування на проникнення; автоматизація кібербезпеки; вразливості; машинне навчання; кіберзагрози; оцінка безпеки; етичний хакінг; DeepExploit; Sn1per; Cortex XSOAR; автоматизація тестування.*

Постановка проблеми. Сучасні методи тестування на проникнення стикаються зі зростаючими викликами через ускладнення мереж і збільшення частоти кіберзагроз. Традиційні підходи вимагають значних людських ресурсів і часу, що може призводити до помилок та затримок у виявленні вразливостей. У той же час швидкі зміни в кібербезпеці, зокрема вразливості нульового дня та розширені постійні загрози, вимагають більш гнучких та ефективних рішень.

Актуальність теми. З розвитком цифрових технологій і збільшенням обсягу інформаційних систем значно зростає кількість кіберзагроз та їх складність. Традиційні підходи до тестування на проникнення стають менш ефективними через ручну природу виконання, що призводить до затримок у виявленні вразливостей та пропуску критичних загроз. У відповідь на ці виклики штучний інтелект пропонує нові можливості для автоматизації та покращення тестування на проникнення. Інструменти на основі ШІ дозволяють швидше реагувати на кіберзагрози, підвищуючи точність і масштабованість процесів безпеки. Це робить тему дослідження надзвичайно важливою в контексті сучасних потреб кібербезпеки, адже від ефективного виявлення та усунення вразливостей залежить стійкість організацій до атак.

Аналіз останніх досліджень та публікацій. Тема автоматизованого тестування на проникнення з використанням штучного інтелекту (ШІ) привертає значну увагу дослідників та практиків у сфері кібербезпеки. Аналіз останніх досліджень та публікацій виявляє кілька ключових напрямів та важливих результатів, що підтримують та розширюють розуміння цієї проблематики.

Дослідження О.Г. Корченко та співавторів [1] підкреслює важливість інтеграції ШІ в системи виявлення вторгнень (IDS). Автори пропонують використання нейронних мереж для аналізу мережевого трафіку та виявлення аномалій, що може бути адаптовано для автоматизованого тестування на проникнення. Це дослідження демонструє потенціал ШІ у підвищенні ефективності виявлення складних атак.

Робота В.А. Лахно та колег [2] фокусується на застосуванні машинного навчання для підвищення ефективності систем захисту інформації. Автори пропонують модель, яка використовує алгоритми машинного навчання для аналізу та класифікації кібератак, що може бути корисним під час розробки інструментів автоматизованого тестування на проникнення.

Дослідження Ю.І. Грицюк та П.Ю. Грицюк [3] розглядає методи та засоби виявлення вразливостей програмного забезпечення. Автори аналізують різні підходи до автоматизованого тестування, враховуючи статичний та динамічний аналіз коду, що є важливим аспектом при розробці ШІ-інструментів для оцінки вразливостей.

Праця О.К. Юдіна та співавторів [4] присвячена аналізу сучасних методів виявлення вразливостей в інформаційних системах. Дослідники пропонують комплексний підхід до оцінки безпеки, який включає використання автоматизованих інструментів та експертних систем, що може бути розширено за допомогою технологій ШІ.

Дослідження С.Г. Семенова та колег [5] розглядає застосування нейронних мереж для виявлення та запобігання кібератакам. Автори пропонують архітектуру системи захисту, яка використовує глибоке

навчання для аналізу поведінки користувачів та виявлення аномалій, що може бути адаптовано для створення більш ефективних інструментів тестування на проникнення.

У роботі [6] увага фокусується на використанні технологій великих даних та ШІ для підвищення ефективності систем кіберзахисту. Дослідники пропонують модель, яка інтегрує різні джерела даних та використовує алгоритми машинного навчання для прогнозування та виявлення загроз, що є важливим аспектом під час розробки передових інструментів тестування на проникнення.

Аналіз останніх досліджень та публікацій демонструє зростаючий інтерес до використання ШІ в галузі кібербезпеки, зокрема в контексті автоматизованого тестування на проникнення. Дослідження підтверджують потенціал ШІ у підвищенні ефективності виявлення вразливостей та оцінки безпеки систем. Вони також вказують на необхідність інтеграції різних підходів, враховуючи машинне навчання, аналіз великих даних та експертні системи, для створення комплексних рішень.

Ці дослідження розширюють розуміння проблематики, демонструючи можливості ШІ у подоланні обмежень традиційних методів тестування на проникнення та підкреслюючи важливість адаптивних, самонавчальних систем для протидії еволюціонуючим кіберзагрозам.

Мета статті – дослідити можливості використання інструментів на основі штучного інтелекту для автоматизації тестування на проникнення, виявлення вразливостей, а також визначити їх переваги та обмеження порівняно з традиційними методами.

Викладення основного матеріалу. Тестування на проникнення, або етичний хакінг, є основою сучасної кібербезпеки. Воно враховує симуляцію атак на системи, мережі або додатки з метою виявлення вразливостей, які зловмисники можуть використати. Традиційне тестування на проникнення було важливим інструментом для захисту цифрових активів, але його обмеження стають дедалі більш вираженими у міру зростання складності систем і частоти кіберзагроз. Ручне проведення тестування на проникнення часто призводить до неефективності, затримок і потенційних пропусків, що можуть поставити безпеку під загрозу. Крім того, швидкі зміни в ландшафті кібербезпеки, що характеризуються вразливостями нульового дня та розширеними постійними загрозами, потребують більш гнучких і масштабованих рішень.

Саме тут вступає в дію штучний інтелект (ШІ). Інтеграція ШІ в тестування на проникнення дозволяє організаціям автоматизувати багато процесів, які раніше виконувалися людьми, покращуючи швидкість і точність. Алгоритми ШІ здатні обробляти величезні набори даних, виявляти патерни і знаходити вразливості набагато швидше, ніж будь-яка людина. Більше того, ШІ може адаптуватися до еволюційних загроз у режимі реального часу, забезпечуючи постійний захист у динамічних середовищах.

Тестування на проникнення з використанням ШІ використовує машинне навчання (ML), обробку природної мови (NLP) та інші просунуті алгоритми для підвищення ефективності оцінки безпеки [11].

Інструменти та технології на основі ШІ

Інструменти на основі штучного інтелекту для тестування на проникнення набули великої популярності останніми роками. Вони застосовують різні ШІ-технології для автоматизації процесів оцінки вразливостей та виявлення експлойтів. Одні з найвідоміших інструментів і технологій, що базуються на ШІ, в цій сфері:

1. DeepExploit. Цей інструмент на базі штучного інтелекту автоматизує процес пошуку вразливостей і їх використання. DeepExploit інтегрується з Metasploit, популярною платформою для тестування на проникнення, і дозволяє автономно сканувати та експлуатувати вразливі місця. Використовуючи методи глибокого навчання з підкріпленням, DeepExploit постійно вдосконалюється і вибирає вразливості для експлуатації, замість застосування грубої сили. Це підвищує ефективність тестування та зменшує вплив на систему [16];
2. Sn1per. Автоматизований інструмент для розвідки та сканування вразливостей, який широко застосовується для тестування безпеки як з наступальною, так і з захисною метою. Хоча Sn1per не повністю заснований на штучному інтелекті, його інтеграція з технологіями машинного навчання дозволяє пріоритизувати виявлені вразливості за рівнем ризику, що особливо корисно для швидкої ідентифікації найбільш критичних загроз [17];
3. Cortex XSOAR. Ця платформа (колишній Demisto) забезпечує оркестрацію, автоматизацію безпеки та реагування (SOAR), використовуючи ШІ для автоматизації завдань у сфері кібербезпеки, включно з тестуванням на проникнення. Завдяки можливостям ШІ, Cortex XSOAR автоматизує сканування, експлуатацію та усунення вразливостей, а інтеграція з іншими інструментами забезпечує комплексний підхід до безпеки [15].

Ці інструменти на основі ШІ надають істотні переваги порівняно з традиційними методами тестування на проникнення, зокрема в швидкості, масштабах та точності. Традиційне тестування на проникнення, хоч і ефективне, часто зіштовхується з труднощами через зростаючу складність сучасних мереж, велику кількість потенційних вразливостей і час, необхідний для проведення повної оцінки.

Переваги автоматизованого тестування на проникнення з використанням ШІ

Автоматизація тестування на проникнення за допомогою ШІ революціонізує сферу кібербезпеки, пропонуючи значні переваги організаціям усіх масштабів. Ця технологія підвищує ефективність, точність та адаптивність оцінки безпеки, відповідаючи на сучасні цифрові виклики. ШІ не лише автоматизує рутинні завдання, але й надає глибокі аналітичні та прогностичні можливості. Застосування машинного навчання та аналізу даних дозволяє виявляти приховані вразливості та передбачати загрози, що особливо цінно в умовах постійно змінюваного ландшафту кіберзагроз. Інтеграція ШІ в процеси тестування забезпечує комплексний підхід до безпеки, що надзвичайно важливо для організацій зі складною IT-інфраструктурою.

Ключові переваги, які пропонує ця передова технологія, охоплюють декілька важливих аспектів. Насамперед, інструменти на основі ШІ значно підвищують точність тестування, мінімізуючи ймовірність людських помилок. Завдяки алгоритмам машинного навчання ШІ здатний аналізувати складні системи та виявляти вразливості, які могли б залишитися непоміченими при ручному тестуванні.

Швидкість оцінки – ще одна суттєва перевага. На відміну від традиційного тестування, яке може тривати тижнями, ШІ-системи здатні провести сканування за години чи навіть хвилини. Ця оперативність критично важлива в середовищах, де нові загрози виникають постійно.

Масштабованість ШІ-інструментів дозволяє ефективно обробляти великі мережі та складні системи. Організації можуть автоматизувати рутинні перевірки, звільняючи людські ресурси для більш складних завдань та симуляцій атак.

Особливо цінною є здатність ШІ прогнозувати майбутні вразливості. Аналізуючи історичні дані, моделі ШІ виявляють патерни, які можуть вказувати на потенційні слабкі місця ще до їх виникнення, що дозволяє вжити превентивних заходів.

Економічна ефективність – ще один вагомий аргумент на користь автоматизації. Зниження витрат на персонал при одночасному збільшенні частоти перевірок робить регулярні оцінки безпеки доступними для організацій будь-якого розміру, враховуючи малий та середній бізнес [18–19].

Нарешті, адаптивність ШІ дозволяє системам постійно вдосконалюватися, вивчаючи нові техніки атак та вразливості. Це безперервне навчання забезпечує організаціям перевагу над зловмисниками, дозволяючи швидко реагувати на нові загрози та залишатися на крок попереду в постійно змінюваному ландшафті кібербезпеки.

Виклики та обмеження

Тестування на проникнення на основі ШІ має великі переваги, однак воно також стикається з низкою викликів і обмежень, які необхідно враховувати для ефективного використання цієї технології. Один з основних викликів полягає в складності навчання та підтримки моделей ШІ. Для створення дійсно ефективних інструментів потрібна глибока експертиза як у сфері кібербезпеки, так і в машинному навчанні. Дані, що використовуються для навчання моделей ШІ, мають охоплювати широкий спектр атак і конфігурацій систем, а моделі потребують постійного оновлення у зв'язку з появою нових технік атак. Це вимагає значних ресурсів, що може бути проблемою для організацій з обмеженими можливостями. Крім того, помилкові позитивні та негативні спрацьовування залишаються серйозним викликом. Хоча ШІ може зменшити кількість помилкових результатів порівняно з ручними методами, все ж є ризик пропуску вразливостей або помилкового визначення нешкідливих дій як загроз. Ще однією проблемою є упередженість алгоритмів ШІ, яка може виникати через недостатньо репрезентативні навчальні дані. Якщо дані не відображають весь спектр можливих вразливостей, ШІ може працювати неефективно в середовищах, що відрізняються від тих, на яких він був навчений. Більше того, моделі ШІ самі можуть стати об'єктом атак, коли зловмисники намагаються маніпулювати вхідними даними для обману моделі. Це ставить нові вимоги щодо забезпечення безпеки самих моделей. Нарешті, зростання використання ШІ у кібербезпеці порушує важливі юридичні та етичні питання. Організації мають дотримуватися правових норм, таких як GDPR, і враховувати етичні аспекти, щоб інструменти не порушували конфіденційність або не завдавали ненавмисної шкоди користувачам.

1. Упередження моделі. Моделі ШІ настільки хороші, наскільки хороші дані, на яких вони навчені. Якщо навчальні дані є упередженими або неповними, ШІ може не виявити певні типи вразливостей. Це може призвести як до переоцінки, так і до недооцінки ризиків безпеки системи.
2. Помилкові спрацьовування та пропуски. Інструменти на основі ШІ іноді можуть генерувати помилкові позитивні (коли безпечну активність вважають шкідливою) або помилкові негативні спрацьовування (коли справжню вразливість не виявлено). Помилкові позитиви можуть призвести до непотрібної тривоги, тоді як помилкові негативи можуть залишити системи відкритими для справжніх загроз.
3. Еволюційний ландшафт загроз. Хоча інструменти ШІ можуть до певної міри адаптуватися, швидкий розвиток кіберзагроз вимагає постійних оновлень і перенавчання моделей. Зловмисники постійно розробляють нові методи для обходу заходів безпеки, і інструменти ШІ мають встигати за цими змінами.

4. Складність і потреби в ресурсах. Розробка, навчання та підтримка інструментів на основі ШІ вимагають значної експертизи та обчислювальних ресурсів. Крім того, інтеграція цих інструментів у наявні інфраструктури кібербезпеки може бути складною, потребуючи координації між різними командами та системами.

5. Регуляторні та етичні питання. Використання ШІ в кібербезпеці викликає занепокоєння щодо конфіденційності, захисту даних та етичного використання. Організації мають забезпечити, щоб інструменти тестування на проникнення з використанням ШІ відповідали нормативним стандартам і не порушували випадково конфіденційність даних або закони про захист даних.

Майбутні тенденції

Майбутні тенденції у тестуванні на проникнення з використанням ШІ обіцяють революційні зміни у сфері кібербезпеки. У найближчі роки очікується, що штучний інтелект стане невід'ємною частиною арсеналу фахівців з безпеки, трансформуючи способи виявлення вразливостей, реагування на загрози та захисту інформаційних систем. Ці інновації не лише вдосконалять традиційні методи оцінки безпеки, але й відкриють нові можливості для захисту цифрових активів в умовах постійно еволюціонуючого ландшафту кіберзагроз. Розвиток ШІ в цій галузі стимулюється зростаючою складністю атак, збільшенням обсягів даних, що потребують аналізу, та необхідністю швидкого реагування на нові типи загроз. Впровадження ШІ у тестування на проникнення обіцяє підвищити ефективність, точність та масштабованість процесів безпеки, дозволяючи організаціям краще захищатися від кіберзагроз. Розглянемо детальніше ключові напрями, які, ймовірно, визначатимуть майбутнє тестування на проникнення з використанням ШІ та їх потенційний вплив на галузь кібербезпеки в цілому [18].

Таблиця 1

Основні тенденції розвитку автоматизованого тестування на проникнення з ШІ

Тенденція	Опис
Тестувальники, доповнені ШІ	Замість повної заміни людей, ШІ розширюватиме їхні можливості. ШІ виконуватиме рутинні завдання, як-от сканування вразливостей та експлуатація, дозволяючи людям зосередитися на складніших завданнях, таких як атаки соціальної інженерії та багатоступеневі експлойти
Повністю автономне тестування на проникнення	Автономні системи тестування зможуть самостійно проводити тестування від початку до кінця без втручання людини, враховуючи розвідку, сканування, експлуатацію вразливостей і звітування. Вони будуть адаптуватися до нових загроз завдяки постійному навчанню на реальних інцидентах
ШІ для виявлення вразливостей нульового дня	ШІ зможе аналізувати патерни поведінки в програмному коді та мережевому трафіку, виявляючи аномалії, що можуть вказувати на нові, невідомі вразливості нульового дня, надаючи додатковий рівень захисту
ШІ у пошуку загроз та реагуванні на інциденти	ШІ відіграватиме важливу роль у проактивному пошуку загроз і реагуванні на інциденти, автоматизуючи збір і аналіз даних, що дозволить організаціям швидше локалізувати й усувати загрози
Інтеграція з квантовими обчисленнями	Інтеграція ШІ з квантовими обчисленнями значно підвищить ефективність та швидкість тестування на проникнення, дозволяючи виконувати криптографічні атаки й оцінку вразливостей на безпрецедентних швидкостях
ШІ для забезпечення безпеки Інтернету речей (IoT)	Зі збільшенням кількості IoT-пристроїв ШІ буде критично важливим для забезпечення їх безпеки, дозволяючи в реальному часі аналізувати величезні масиви даних з багатьох пристроїв та виявляти вразливості у масштабних мережах
Федеративне навчання для тестування на проникнення	Федеративне навчання дозволить навчати моделі ШІ в децентралізованих середовищах без передачі конфіденційних даних назовні, зберігаючи приватність та підвищуючи ефективність тестування
Етичне використання ШІ у кібербезпеці	Етичні аспекти використання ШІ ставатимуть дедалі важливішими для уникнення негативних наслідків, таких як збої систем або порушення конфіденційності, і сприятимуть розвитку прозорих, справедливих і пояснюваних практик ШІ

Практичні рекомендації щодо впровадження тестування на проникнення на основі ШІ у фінансовому секторі

Для того щоб повністю використати переваги тестування на проникнення на основі ШІ у фінансовому секторі, організаціям необхідно стратегічно підійти до його впровадження. Фінансові установи стикаються з унікальним набором викликів у сфері безпеки через складність своїх систем та чутливість даних, якими вони управляють. Ці організації обробляють великі обсяги транзакцій, інформацію про клієнтів та широкі фінансові мережі, які є привабливими цілями для кібератак. Традиційні методи тестування на проникнення часто є недостатніми для покриття цієї складності, що залишає вразливості неусуненими. Тестування на проникнення на основі ШІ пропонує автоматизоване, масштабоване та високопродуктивне рішення, здатне аналізувати ці складні системи більш точно та ефективно.

Завдяки впровадженню рішень на основі ШІ, таких як DeepExploit або подібні фреймворки, фінансові установи можуть забезпечити безперервні та реальні оцінки вразливостей, виявляючи потенційні ризики до того, як вони будуть використані. Критичні області, такі як платіжні шлюзи, клієнтські платформи та мережі банкоматів, потребують постійного моніторингу, оскільки вони часто є мішенями для хакерів. Штучний інтелект дозволяє цим фінансовим установам оптимізувати свої процеси безпеки, використовуючи машинне навчання для прогнозування потенційних векторів атак і зменшення ризику фінансового шахрайства. Крім того, інструменти тестування на проникнення на основі ШІ можуть підвищити точність виявлення вразливостей, зменшуючи кількість хибних спрацювань і забезпечуючи, щоб команди безпеки зосереджувалися на реальних загрозах. Ця можливість є надзвичайно важливою для банків, фінтех-компаній та інших фінансових підприємств, які мають захищатися від постійно змінюваних кіберзагроз.

Інтеграція таких рішень на основі ШІ з існуючими рамками кібербезпеки також дозволяє фінансовим установам оптимізувати реагування на інциденти та покращити загальне управління безпекою.

1. Впровадження оцінки вразливостей на основі ШІ:

a. Зосередженість на системах із високим рівнем ризику. Фінансовим установам, враховуючи банки та фінтех-компанії, варто застосовувати інструменти для тестування на проникнення на основі ШІ для захисту критичних систем, таких як платіжні шлюзи, платформи онлайн-банкінгу та мережі банкоматів. Інструменти, такі як DeepExploit, можуть постійно оцінювати ці важливі області, зменшуючи ризик виникнення невидимих загроз;

b. Виявлення загроз у реальному часі. Завдяки впровадженню рішень на основі ШІ для безперервного моніторингу установи можуть випереджати нові загрози. Безперервне сканування вразливостей у режимі реального часу виявляє вразливості нульового дня та захищає критичну інфраструктуру від невідомих раніше векторів атак;

c. Виявлення шахрайства за допомогою машинного навчання. Моделі ШІ, оснащені некерованим машинним навчанням, можуть виявляти незвичну поведінку транзакцій та шахрайські дії, надаючи фінансовим установам додатковий рівень захисту від фінансових шахрайств.

2. Інтеграція з існуючими платформами кібербезпеки:

a. Інтеграція з платформами SIEM та SOAR. Інструменти тестування на проникнення на основі ШІ мають бути інтегровані з існуючими платформами SIEM (система управління подіями та інформацією безпеки) і SOAR (оркестрація, автоматизація та реагування на безпеку) для забезпечення ефективного виявлення інцидентів та реагування на них. Автоматизуючи процеси реагування на інциденти та встановлення патчів для вразливостей, фінансові установи можуть значно скоротити час реагування та покращити загальне управління безпекою;

b. Забезпечення відповідності нормативним вимогам. Інструменти на основі ШІ можуть допомогти фінансовим організаціям дотримуватися нормативних стандартів, таких як PCI DSS (Стандарт безпеки даних індустрії платіжних карток) і GDPR (Загальний регламент захисту даних). Автоматизовані системи на основі ШІ здатні виявляти вразливості, які становлять ризик для відповідності вимогам, створювати звіти та полегшувати процеси аудиту.

3. Рішення для підвищення безпеки:

a. Самонавчальні системи ШІ. Розробка самонавчальних систем ШІ, які адаптуються до поведінки зловмисників у реальному часі. Шляхом постійної симуляції складних загроз ШІ може випереджати кіберзлочинців і з часом покращувати захисні механізми;

b. Блокчейн для аудиту. Інтеграція технології блокчейн для створення незмінних записів тестів на проникнення. Блокчейн може забезпечити прозорість та відповідальність під час аудиту кібербезпеки, надаючи фінансовим установам надійну платформу для зберігання журналів безпеки та результатів тестів;

c. Виявлення внутрішніх загроз. Моделі ШІ можуть відстежувати поведінку працівників, щоб виявити незвичайні патерни, які можуть свідчити про потенційні внутрішні загрози. Аналізуючи внутрішні дані в режимі реального часу, фінансові організації можуть знизити ризики, пов’язані з внутрішніми порушеннями безпеки.

Тестування на проникнення на основі ШІ зміцнює кібербезпеку фінансового сектора завдяки підвищенню точності, скороченню часу реагування та поліпшенню масштабованості. Інтегруючи рішення на основі ШІ з існуючими системами та використовуючи інноваційні технології, такі як блокчейн і самонавчальні моделі, фінансові установи можуть випереджати нові загрози та одночасно забезпечувати відповідність нормативним вимогам.

Висновки та перспективи подальших досліджень. Тестування на проникнення з використанням ШІ є значним кроком вперед у постійній боротьбі за захист цифрових інфраструктур. Автоматизація оцінки вразливостей і використання машинного навчання для виявлення та експлуатації слабких місць дозволяють інструментам на основі ШІ забезпечити безпрецедентну швидкість, точність та масштабованість. Ці інструменти вже доводять свою цінність у різних галузях, від фінансів до охорони здоров'я, де складні системи та високі вимоги до безпеки роблять традиційні методи недостатніми.

Однак виклики залишаються. Питання, пов'язані з упередженістю моделей, помилковими спрацьовуваннями та складністю підтримки інструментів на основі ШІ, підкреслюють необхідність постійного вдосконалення та контролю. У міру розвитку ШІ наступне покоління інструментів для тестування на проникнення, ймовірно, стане ще більш досконалим, здатним до повністю автономного тестування та адаптації до нових загроз у режимі реального часу.

У перспективі інтеграція ШІ з іншими технологіями, такими як квантові обчислення та федеративне навчання, ймовірно, сприятиме подальшим інноваціям у сфері кібербезпеки. У міру того, як організації продовжують впроваджувати рішення на основі ШІ, тестування на проникнення стане не лише більш ефективним, але й більш доступним для організацій будь-якого розміру.

Майбутнє тестування на проникнення з використанням ШІ виглядає перспективним, і в міру розвитку технологій ШІ, безсумнівно, стане незамінним інструментом для захисту дедалі більшого цифрового ландшафту від усе складніших кіберзагроз.

Список використаної літератури:

1. Сучасні системи виявлення вторгнень: аналіз та застосування / *О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук та ін.* – Київ : НАУ, 2022. – 250 с.
2. *Лахно В.А.* Інтелектуальні системи кібербезпеки: проблеми та перспективи / *В.А. Лахно, О.С. Петров, О.М. Гуцан* // Системи обробки інформації. – 2021. – № 2 (165). – С. 115–124.
3. *Грицюк Ю.І.* Особливості використання сучасних методів і засобів виявлення вразливостей програмного забезпечення / *Ю.І. Грицюк, П.Ю. Грицюк* // Науковий вісник НЛТУ України. – 2023. – Т. 33, № 1. – С. 136–149.
4. *Юдін О.К.* Аналіз сучасних методів виявлення вразливостей інформаційних систем / *О.К. Юдін, С.С. Бучик, А.В. Чунарьова* // Наукоємні технології. – 2022. – № 3 (55). – С. 277–286.
5. *Семенов С.Г.* Застосування нейронних мереж в системах виявлення вторгнень / *С.Г. Семенов, В.В. Давидов, С.Ю. Гавриленко* // Системи управління, навігації та зв'язку. – 2021. – № 2 (64). – С. 64–68.
6. *Бурячок В.Л.* Використання технологій Big Data та штучного інтелекту в системах кіберзахисту / *В.Л. Бурячок, С В. Толюпа, В.В. Семко* // Сучасний захист інформації. – 2022. – № 1 (49). – С. 6–12.
7. Огляд рішень безпеки / H-X Technology. – 2023 [Електронний ресурс]. – Режим доступу : https://www.h-x.technology/ua/security-solutions-full-review-ua.
8. Тестування на проникнення або етичний хакінг / ESKA Global. – 2023 [Електронний ресурс]. – Режим доступу : https://eska.global/blog/testuvannya-na-proniknennya-abo-etichnij-haking.
9. *Слюсар В.І.* Штучний інтелект як основа перспективних мереж зв'язку та базовий елемент цифрової економіки / *В.І. Слюсар.* – 2022 [Електронний ресурс]. – Режим доступу : https://www.slyusar.kiev.ua/AI_2022-1-1_ua.pdf.
10. Що таке хакінг? Типи хакерів. Вступ до кіберзлочинності / HackYourMom. – 2023 [Електронний ресурс]. – Режим доступу : https://hackyourmom.com/osvita/shho-take-haking-typy-hakeriv-vstup-do-kiberzlochynnosti/.
11. Що таке машинне навчання? / De Novo. – 2023 [Електронний ресурс]. – Режим доступу : https://denovo.ua/resources/what-is-machine-learning.
12. AI in Pen Testing / Cyber Smart Consulting. – 2023 [Electronic resource]. – Access mode : https://cybersmartconsulting.com/ai-in-pen-testing/.
13. What does 2024 have in store for the world of cybersecurity? / World Economic Forum. – 2024 [Electronic resource]. – Access mode : https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/.
14. *Stallings W.* Network Security Essentials: Applications and Standards / *W.Stallings*. – 4th ed. – Prentice Hall, 2011 [Electronic resource]. – Access mode : https://books.google.com.ua/books?id=pfdBiJNfWdMC&lpg=PR3&hl=uk&pg=PR34#v=onepage&q&f=false.
15. Palo Alto Networks / Cortex XSOAR. – 2023 [Electronic resource]. – Access mode : https://www.paloaltonetworks.com/cortex/cortex-xsoar.
16. DeepExploit / The DreamPort. – 2023 [Electronic resource]. – Access mode : https://github.com/TheDreamPort/deep_exploit?tab=readme-ov-file.
17. Automated Pentest Framework / Sn1per Security. – 2023 [Electronic resource]. – Access mode : https://sn1persecurity.com/wordpress/.
18. How does AI reduce human error? / KODEXO LABS [Electronic resource]. – Access mode : https://kodexolabs.com/how-does-ai-reduce-human-error.

19. AI in Threat Detection: Challenges and Benefits / PALO ALTO NETWORKS [Electronic resource]. – Access mode : https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection#challenges.

References:

1. Korchenko, O.H., Hnatiuk, S.O., Kazmirchuk, S.V. et al. (2022), *Suchasni systemy vyiavlennia vtorhnen: analiz ta zastosuvannia*, «NAU», Kyiv, 250 p.
2. Lakhno, V.A., Petrov, O.S. and Hutsan, O.M. (2021), «Intelektualni systemy kiberbezpeky: problemy ta perspektyvy», *Systemy obrobky informatsii*, No. 2 (165), pp. 115–124.
3. Hrytsiuk, Yu.I. and Hrytsiuk, P.Iu. (2023), «Osoblyvosti vykorystannia suchasnykh metodiv i zasobiv vyiavlennia vrazlyvostei prohramnoho zabezpechennia», *Naukovyi visnyk NLTU Ukrainy*, Vol. 33, No. 1, pp. 136–149.
4. Yudin, O.K., Buchyk, S.S. and Chunarova, A.V. (2022), «Analiz suchasnykh metodiv vyiavlennia vrazlyvostei informatsiinykh system», *Naukoiemni tekhnolohii*, No. 3 (55), pp. 277–286.
5. Semenov, S.H., Davydov, V.V. and Havrylenko, S.Yu. (2021), «Zastosuvannia neironnykh merezh v systemakh vyiavlennia vtorhnen», *Systemy upravlinnia, navihatsii ta zviazku*, No. 2 (64), pp. 64–68.
6. Buriachok, V.L., Toliupa, S.V. and Semko, V.V. (2022), «Vykorystannia tekhnolohii Big Data ta shtuchnoho intelektu v systemakh kiberzakhystu», *Suchasnyi zakhyst informatsii*, No. 1 (49), pp. 6–12.
7. «Ohliad rishen bezpeky» (2023), *H-X Technology*, [Online], available at: https://www.h-x.technology/ua/security-solutions-full-review-ua
8. «Testuvannia na pronyknennia abo etychnyi khakinh» (2023), *ESKA Global*, [Online], available at: https://eska.global/blog/testuvannya-na-proniknennya-abo-etichnij-haking
9. Sliusar, V.I. (2022), «Shtuchnyi intelekt yak osnova perspektyvnykh merezh zviazku ta bazovyi element tsyfrovoi ekonomiky», [Online], available at: https://www.slyusar.kiev.ua/AI_2022-1-1_ua.pdf
10. «Shcho take khakinh? Typy khakeriv. Vstup do kiberzlochynnosti» (2023), *HackYourMom*, [Online], available at: https://hackyourmom.com/osvita/shho-take-haking-typy-hakeriv-vstup-do-kiberzlochynnosti/
11. «Shcho take mashynne navchannia?» (2023), *De Novo*, [Online], available at: https://denovo.ua/resources/what-is-machine-learning
12. «Cyber Smart Consulting. AI in Pen Testing» (2023), *Cyber Smart Consulting*, [Online], available at: https://cybersmartconsulting.com/ai-in-pen-testing/
13. «What does 2024 have in store for the world of cybersecurity?» (2024), *World Economic Forum*, [Online], available at: https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/
14. Stallings, W. (2011), *Network Security Essentials: Applications and Standards*, 4th ed., Prentice Hall, [Online], available at: https://books.google.com.ua/books?id=pfdBiJNfWdMC&lpg=PR3&hl=uk&pg=PR34#v=onepage&q&f=false
15. «Cortex XSOAR» (2023), *Palo Alto Networks*, [Online], available at: https://www.paloaltonetworks.com/cortex/cortex-xsoar
16. «The DreamPort» (2023), *DeepExploit*, [Online], available at: https://github.com/TheDreamPort/deep_exploit?tab=readme-ov-file
17. «Automated Pentest Framework» (2023), *Sn1per Security*, [Online], available at: https://sn1persecurity.com/wordpress/
18. «How does AI reduce human error?», *KODEXO LABS*, [Online], available at: https://kodexolabs.com/how-does-ai-reduce-human-error
19. «AI in Threat Detection: Challenges and Benefits», *PALO ALTO NETWORKS*, [Online], available at: https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection#challenges

Колощук Марія Сергіївна – асистент кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0009-0001-5825-2054.

Наукові інтереси:

– комп'ютерні мережі;
– кібербезпека;
– архітектура комп'ютера.

Дячук Ольга Юріївна – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0000-0002-6996-4700.

Наукові інтереси:

– комп'ютерні мережі;
– кібербезпека;
– архітектура комп'ютера.

Окунькова Оксана Олексіївна – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0009-0004-0093-0694.

Наукові інтереси:

– інформаційні та комп'ютерні технології в освіті.

Пірог Олександр Вікторович – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0009-0001-6111-9676.

Наукові інтереси:

- стандарти та нормативно-правове забезпечення кібербезпеки та захисту інформації;
- безпека вебзастосунків та вебресурсів;
- комплексні системи захисту інформації.

Koloshchuk M.S., Dyachuk O.Yu., Okunkova O.O., Piroh O.V.

Artificial intelligence tools for automating penetration testing

The article discusses automated penetration testing using artificial intelligence (AI), which significantly enhances the efficiency and accuracy of cybersecurity assessments. AI-based technologies are capable of automating many processes that were previously performed manually, including vulnerability scanning, threat analysis, and exploitation of system weaknesses. Special attention is given to AI-based tools such as DeepExploit, Sn1per, and Cortex XSOAR, which demonstrate substantial advantages over traditional penetration testing methods. The article also addresses the main challenges of implementing AI in penetration testing, including the difficulties of training models and the issue of false positives. The future trends in the use of AI for cybersecurity, such as autonomous testing systems and integration with quantum computing, are explored as well.

Keywords: artificial intelligence; penetration testing; cybersecurity automation; vulnerabilities; machine learning; cyber threats; security assessment; ethical hacking; DeepExploit; Sn1per; Cortex XSOAR; test automation.

Стаття надійшла до редакції 24.09.2024.