КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.789
УДК 004.056

Притула Андрій Вікторович
аспірант кафедри захисту інформації
ТОВ «ValueTek»
ORCID ID: 0009-0006-9632-0712
andrik.pritula@gmail.com

Куперштейн Леонід Михайлович
к.т.н., доцент кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

АНАЛІЗ ПІДХОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ З ПІДКРІПЛЕННЯМ

Анотація. Тестування на проникнення (ТнП) є важливим методом для забезпечення цифрової безпеки, який дозволяє оцінити наявність вразливостей у системах та мережах через симуляції атак. Завдяки швидкому розвитку технологій і зростанню цифрових загроз, постає потреба в удосконаленні методів тестування, зокрема через впровадження машинного навчання (МН) та алгоритмів навчання з підкріпленням (НзП). У статті розглядаються сучасні підходи до автоматизації тестування на проникнення з використанням машинного навчання та навчання з підкріпленням, які дозволяють значно підвищити ефективність і точність процесу. Тестування на проникнення включає кілька етапів, таких як збір інформації про цільову систему, сканування, аналіз загроз і вразливостей, експлуатація, формування звіту. Традиційні методи часто вимагають витрат значних людських ресурсів і часу для виконання цих процесів. Впровадження штучного інтелекту (ШІ) та МН дозволяє автоматизувати ці етапи, що призводить до значного скорочення часу і підвищення результативності тестування. Зокрема, підхід на основі НзП демонструє високий потенціал для адаптації до змін у середовищі тестування, що дозволяє системам самостійно вдосконалювати свої стратегії з часом, опираючись на досвід. У статті розглянуто різні підходи, зокрема використання методів глибокого навчання та безмодельного НзП для автоматизації тестування на проникнення. Проаналізовано переваги та обмеження кожного з підходів, зокрема важливість адаптивності до змін середовища, високої точності виявлення вразливостей, а також складнощі, що виникають при інтеграції та налаштуванні інструментів, особливо для великих та складних мереж. Також розглянуто можливі виклики, пов'язані з використанням значних обчислювальних потужностей та необхідністю моделювання специфічних умов. У результаті дослідження виділено найбільш актуальні підходи до автоматизації тестування на проникнення з використанням методів навчання з підкріпленням, які мають значний потенціал для підвищення ефективності та адаптивності процесів тестування. Перспективи подальших досліджень зосереджуються на розширенні можливостей моделей НзП для застосування в складних і великих мережах, а також на інтеграції з іншими платформами кібербезпеки для створення більш комплексних та ефективних систем автоматизованого тестування.

Ключові слова: тестування на проникнення; машинне навчання; навчання з підкріпленням; автоматизація; кібербезпека; вразливості; загрози; штучний інтелект.

ВСТУП

Сучасні компанії конкурують, використовуючи технології для підтримки продуктів, які вони виробляють, а люди завдяки технологіям можуть зберігати дані, шукати інформацію, здійснювати безготівкові платежі, купувати онлайн та багато іншого. Однак така зручність робить важливим безпечне зберігання даних в

технологічних рішеннях, що використовуються різними структурами. Компанії та організації повинні забезпечити, щоб технології, які будуть використовуватися громадськістю та бізнесом, були безпечними. Це формує одну із ключових цілей кібербезпеки — забезпечення захищеності [**Error! Reference source not found.**].

Стрімкий розвиток технологій із застосуванням штучного інтелекту ставить перед кібербезпекою вимоги формувати нові типи захисту, пришвидшувати пошуки ефективних рішень, підвищувати ефективність безпеки. І в той же час сучасні доробки у сфері машинного навчання дозволяють компаніям успішно формувати стратегії кіберзахисту.

У сучасному світі кіберзагрози стають дедалі складнішими і ризики безпеки сервісів та даних вагомішими, тому тестування на проникнення стає критично важливим як один із передових підходів перевірки захищеності систем. Проте традиційні методи тестування на проникнення можуть бути трудомісткими та не завжди відповідати параметрам ефективності в умовах швидкого розвитку технологій. Інтеграція машинного навчання, зокрема навчання з підкріпленням, відкриває нові горизонти для автоматизації та підвищення ефективності тестування на проникнення.

Постановка проблеми. Тестування на проникнення є методом оцінки безпеки в системі, шляхом виконання або імітації реальної кібератаки [**Error! Reference source not found.**]. Однак тестування на проникнення має кілька недоліків, основними серед яких є необхідність специфічних навичок для його проведення і час для виконання. Наразі гостро постає питання формування достатнього рівня кібербезпеки, оскільки різноманітність інформаційних систем, складність атак та множинність потенційних векторів проникнення суттєво ускладнюють ручне тестування. У зв’язку з цим актуальним стає завдання автоматизації процесів тестування на проникнення шляхом використання алгоритмів машинного навчання, зокрема навчання із підкріпленням, які здатні ефективно адаптуватись до змін середовища та швидко і точно визначати вразливості, що можуть бути пропущені людським фактором.

Аналіз останніх досліджень і публікацій. Використання машинного навчання у тестуванні на проникнення стало предметом численних досліджень протягом останніх років.

Д. Лі, Л. Кусвандана, С. Ахмад та Д. Сухартоно зазначають, що термін «тестування на проникнення» використовується для процесу, який допомагає підтримувати безпеку технологій [**Error! Reference source not found.**]. Тестування на проникнення складається з двох основних термінів: «проникнення», що означає проникати або прориватися, і «тестування», що означає експеримент. Тому тестування на проникнення є діяльністю, яка симулює проникнення або порушення існуючого захисту мережі, хоста, сервісу. Це потрібно, щоб існувала можливість заздалегідь виявити слабкі місця та як їх усунути, перш ніж вони будуть виявлені та використані зловмисниками. Технологічні розробки призвели до появи технології під назвою «машинне навчання». Машинне навчання є відгалуженням штучного інтелекту, яке направлене на забезпечення можливості навчання деякого алгоритму на основі наданих даних вирішувати складні інтелектуальні задачі [**Error! Reference source not found.**]. Основою машинного навчання є аналіз даних за допомогою алгоритмів, які виявляють різноманітні шаблони у цих даних. Це дає змогу створити систему, яка здатна «навчатися» на основі накопиченого досвіду та самостійно приймати оптимальні рішення або виконувати дії. Таким чином, машинне навчання сприяє автоматизації процесів, що повторюються і мають стабільні шаблони, значно підвищуючи ефективність і точність таких операцій [**Error! Reference source not found.**]. З. Ху, Р. Беуран, та Ю. Тан зазначають, шо наразі тестування на проникнення виконується здебільшого вручну та значною мірою залежить від досвіду етичних

хакерів, які його виконують, так звані «пентестери» [**Error! Reference source not found.**]. Р. С. Джагамоган, С. А. Ісмаїл, Н. Х. Хасан та Х. Абас зазначають, що режим машинного навчання здатний виявити більше типів вразливостей [**Error! Reference source not found.**]. А. Толкачова та М. Посувайло відзначають, що останні дослідження підкреслюють значний потенціал автоматизації процесів тестування на проникнення за допомогою глибокого навчання з підкріпленням. Розробка автоматизованих систем тестування обіцяє значно підвищити точність, швидкість і ефективність виявлення та усунення вразливостей безпеки [**Error! Reference source not found.**].

М. Ганем і Т. Чен відзначають, що на практиці, інтеграція машинного навчання в будь-яку систему тестування на проникнення принаймні зменшить повторювані людські помилки, спричинені втомою, упущеннями та тиском [**Error! Reference source not found.**]. Це також покращить продуктивність системи під час виконання різних тестів. Автоматизація на основі МН дозволить знизити завантаження мережі та час простою, скоротивши кількість тестів, виконуючи лише релевантні тести поза робочими або офісними годинами, таким чином уникаючи будь-яких проблем із доступністю активів. Втім, на думку авторів, у МН-орієнтованій системі тестування на проникнення виникнуть три основні проблеми. По-перше, це набуття та узагальнення досвіду — використання знань, отриманих під час навчання, для оптимального майбутнього використання в подібних ситуаціях. По-друге, важливим стає питання адаптації до дуже конкретного контексту навчання (достатньо вузького напрямку), що включає послідовне прийняття рішень з винагородою (як автоматизованих, так і у контексті з винагородою від експертів). По-третє, компроміс між дослідженням та використанням спрямований на забезпечення найкращих можливих результатів при раціональному використанні ресурсів. Крім того, навчання такої системи вимагатиме, щоб модуль навчання був відкритий і міг безпосередньо взаємодіяти з експертом для вирішення складних ситуацій, пропонуючи вказівки та рекомендації, які можуть бути прийняті або відхилені експертом [**Error! Reference source not found.**].

При цьому доцільно відзначити, що систему кібербезпеки часто класифікують на два типи: керовану експертами або автоматизовану систему, що використовує неконтрольоване машинне навчання. Системи, керовані експертами, такі як AVs, FWs, IDPSs та SIEMs [**Error! Reference source not found.**], спираються на внесок експертів з безпеки і зазвичай приводять до високих рівнів помилок, доки не використовувалися техніки навчання з підкріпленням (НзП). Це дало змогу розробити більш точні та ефективні навчальні системи, які забезпечують автономне або напівавтономне прийняття рішень, що точно відображає реальний контекст кібербезпеки та, зокрема, сферу наступальної безпеки (тобто проактивної реакції на випередження), таку як оцінка вразливостей і контекст тестування на проникнення. Основні причини вибору НзП для тестування на проникнення включають три важливі аспекти:

- ефективність автономного навчання та покращення завдяки постійній взаємодії з навколишнім середовищем; навчання, засноване на винагородах, та існуючі гнучкі схеми винагород, які можуть бути відкладені, щоб дозволити агенту НзП максимізувати довгострокову мету;
  - різноманітність середовища НзП, яке допомагає захоплювати всі основні характеристики тестування на проникнення, включаючи невизначеність і складність;
  - здатність НзП адаптуватися до змін середовища, що дозволяє системам покращувати стратегії тестування на проникнення в умовах нових або

непередбачуваних загроз, зменшуючи залежність від попередніх знань або вручну розроблених правил.

НзП дозволяє агенту навчатися на власній поведінці в середовищі, досліджуючи його та вчитися, як діяти на основі винагород, отриманих від виконаних дій [**Error! Reference source not found.**]. Ця політика прийняття рішень може бути засвоєна один раз і назавжди або бути покращена чи адаптована при досягненні кращих результатів. При правильному моделюванні проблеми, деякі алгоритми НзП можуть збігатися до глобального оптимуму, який є ідеальною поведінкою, що максимізує загальну винагороду. Схема навчання НзП виключає необхідність значного втручання від людини, яка є експертом у цій галузі [**Error! Reference source not found.**]. Крім того, реалізація НзП означатиме, що менше часу виділяється на навчання та налаштування, як це зазвичай буває з машинним навчанням і експертними системами.

Мета статті. Метою статті є аналіз підходів автоматизації процесу тестування на проникнення за допомогою алгоритмів машинного навчання, зокрема МН з підкріпленням.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Тестування на проникнення є надзвичайно важливим для цифрової та інформаційної безпеки у світі, де технологічний розвиток рухається швидкими темпами. Це легальний метод імітації кібератак, який довів свою ефективність у виявленні вразливостей та експлойтів, що можуть загрожувати мережі або системі [**Error! Reference source not found.**]. Тестування на проникнення є ефективним способом симулювати реальні атаки на систему, допомагаючи виявляти матрицю вразливостей, проблеми з патчами та надавати дуже дієві результати у межах досліджуваної системи. Воно також може допомогти усувати слабкі місця безпеки, перевіряти відповідність політиці безпеки організації, підвищувати обізнаність співробітників щодо безпеки та здатність організації ідентифікувати та реагувати на інциденти безпеки, що є надзвичайно важливими для підтримки інформаційної безпеки у межах цифрових взаємодій [**Error! Reference source not found.**].

Збільшення цифровізації всіх сфер життя супроводжується ризиками для персональних даних, виробничих процесів та управлінських рішень, внаслідок чого кібербезпека стає критично важливою для компаній, що формує потребу у тестуванні на проникнення, яке за своєю сутністю є імітацією хакерських атак для виявлення вразливостей у системах безпеки. Як правило, у таких тестуваннях ефективність підвищується через використання двох етапів: оцінки вразливостей і тестування на проникнення. Оцінка вразливостей визначає ризики, тоді як тестування досліджує, як їх можна використати. З огляду на це цілями тестування на проникнення є підвищення безпеки систем, виявлення слабких місць, підтвердження безпеки. В ідеалі результати тестування включають не лише список проблем, але й пропозиції з їх усунення. Автоматизація тестування на проникнення та доступ до різноманітних інструментів сприяють зростанню ринку послуг кібербезпеки [**Error! Reference source not found.**], [**Error! Reference source not found.**].

Використання штучного інтелекту та машинного навчання здатне позитивно впливати на різні етапи тестування на проникнення (табл. 1).

Таблиця 1

Вплив ШІ та МН на тестування на проникнення на різних етапах

Етап тестування на проникнення	Традиційний підхід	Вплив ШІ та МН
1	2	3
Розвідка та збір даних	Збір інформації про цільову систему вручну, що займає багато часу.	Автоматизація процесу збору даних, підвищення швидкості та точності.
Сканування	Ручне сканування для виявлення вразливостей, що може бути неефективним.	Швидше та точніше сканування з використанням алгоритмів ШІ та МН, зменшення людських помилок.
Аналіз загроз	Складний процес аналізу загроз вручну з обмеженими ресурсами.	Когнітивні здібності ШІ та МН покращують розуміння даних та виявлення підозрілої активності.
Аналіз вразливостей	Важко керувати ризиками через складність та швидкість появи нових загроз.	Моделі МН допомагають пріоретизувати заходи з відновлення та планувати цикли виправлення.
Використання вразливостей	Ручне використання вразливостей може бути складним та повільним.	ШІ та МН прискорюють процес використання вразливостей, підвищуючи ефективність тестування.

Таким чином, потенціал інтеграції ШІ та МН полягає у можливостях підвищення ефективності та точності тестування на проникнення, зменшуючи залежність від людського фактору та прискорюючи процеси, що дозволяє суттєво економити час на тестування.

Д. Лі, Л. Кусвандана, С. Ахмад та Д. Сухартоно запропонували підхід до автоматизації тестування на проникнення, використовуючи алгоритми машинного навчання, зокрема навчання з підкріпленням. Для цього дослідники розробили інструмент на мові Python із інтеграцією НзП-алгоритмів, які здатні виявляти вразливості, що можуть бути пропущені людськими тестувальниками, адаптуватися до змін у середовищі та покращувати свої результати на основі накопиченого досвіду. Для навчання авторами використано фреймворк MITRE ATT&CK, що забезпечує базу для атак та експлуатацій для безпосереднього тестування. Після розробки інструменту авторами запропоновано провести серію тестових запусків на різних мережевих цілях із різними конфігураціями та середовищами, а результати таких тестів порівняти з результатами, отриманими за допомогою традиційних інструментів (наприклад, Nmap), щоб оцінити ефективність використання машинного навчання в автоматизованому тестуванні на проникнення [**Error! Reference source not found.**].

А. Толкачова та М.-М. Посувайло на етапі підготовки тесту залучати штучний інтелект для автоматичного створення реалістичної топології мережі, включаючи розробку дерева можливих атак. Автори зазначають, що інтегровані з МН системи тестування на проникнення можуть служити ефективним інструментом навчання для фахівців з кібербезпеки, так як дозволяють симулювати атаки в контрольованому навчальному середовищі, пропонуючи користувачам аналіз різних стратегій і методів вторгнення, а також бути засобом навчання виявленню реальних атак і проактивної розробки способів реагування на них. Такий підхід сприяє глибокому розумінню потенційних загроз і розвиває навички ефективного захисту від них, в той час як використання машинного навчання може допомогти вирішити проблему високої кількості помилкових тривог, яка є поширеною проблемою в традиційних системах безпеки. Глибоке навчання з підкріпленням дає можливість створювати більш адаптивні тестові системи, які можуть навчатися самостійно та адаптуватися до мінливих моделей загроз. Такі системи стають не тільки ефективнішими, але й здатними працювати з меншою кількістю помилок, знижуючи навантаження на людей. Це дозволяє їм виявляти

вразливості, які люди пропустили, забезпечуючи глибший і комплексний аналіз безпеки. Цей підхід має потенціал для революції в індустрії кібербезпеки, пропонуючи нові стратегії захисту IT-систем і створюючи більш надійні мережеві структури [**Error! Reference source not found.**].

М. Ганем та Т. Чен запропонували підхід до автоматизації тестування на проникнення за допомогою НзП. Вони розробили інтелектуальну автоматизовану систему тестування на проникнення IAPTS, яка використовує НзП для моделювання тестування на проникнення як процесу прийняття рішень у частково спостережуваному середовищі Маркова (partially observable Markov decision process, POMDP). Ця система інтегрується з існуючими фреймворками тестування на проникнення, дозволяючи їм накопичувати інформацію, навчатися на досвіді та відтворювати тести в майбутніх подібних випадках. Розроблена у такий спосіб IAPTS спрямована на зменшення витрат людських ресурсів, підвищення ефективності, надійності та частоти тестування, використовуючи різні алгоритми POMDP, що дозволяє адаптуватися до різних контекстів та враховувати обмеження ресурсів, таких як час, пам’ять та обчислювальні потужності. Результати досліджень показують, що використання НзП може покращити процеси тестування на проникнення, перевершуючи можливості людських експертів у трьох ключових аспектах — точність, надійність та охоплення тестування [**Error! Reference source not found.**].

Відповідно до досліджень М. Ганем, Т. Чен та Е. Непомуцено, у великих мережах тестування на проникнення стає повторюваним, складним і вимагає значних ресурсів, незважаючи на використання автоматизованих інструментів. Тому актуалізується доцільність застосування НзП, щоб зробити тестування на проникнення більш розумним, цілеспрямованим і ефективним. Запропонований розробниками підхід під назвою Intelligent Automated Penetration Testing Framework (IAPTF) використовує НзП на основі моделі автоматизації прийняття послідовних рішень. Завдання тестування на проникнення розглядаються як частково спостережуваний марківський процес прийняття рішень, який вирішується за допомогою зовнішнього POMDP-розв’язувача з використанням різних алгоритмів для визначення найбільш ефективних варіантів. Основною проблемою, з якою зіткнулися, було розв’язання великих POMDP, що виникають у великих мережах. Це було подолано шляхом представлення мереж ієрархічно як групи кластерів і обробки кожного кластера окремо. Цей підхід перевірено шляхом моделювання мереж різного розміру. Результати показують, що IAPTF з моделюванням ієрархічної мережі перевершує попередні підходи, а також продуктивність людини з точки зору часу, кількості перевірених векторів і точності, і перевага зростає разом із розміром мережі. Ще однією перевагою IAPTF є легкість повторення для повторного тестування подібних мереж. Результати свідчать про те, що IAPTF є багатообіцяючим підходом для розвантаження роботи та, зрештою, заміни тестування вручну [**Error! Reference source not found.**].

Дж. Шварц та Х. Курняваті зазначили, що сучасні підходи до автоматизованого ТнП спираються на планування на основі моделі, однак ландшафт кібербезпеки швидко змінюється, що ускладнює підтримку актуальних моделей експлойтів. У своєму проєкті автори досліджували застосування безмодельного НзП для автоматизованого ТнП. Безмодельний НзП має ключову перевагу перед плануванням на основі моделі, оскільки не вимагає моделі середовища, натомість вивчає найкращу політику через взаємодію з середовищем. Автори вперше розробили та створили швидкий симулятор із низьким обчислювальним ресурсом для навчання та тестування автономних агентів ТнП, представивши тестування як марківський процес прийняття рішень із відомою конфігурацією мережі як станами, доступними скануваннями та експлойтами як діями,

а винагорода визначається цінністю обчислювальних систем у мережі. Потім було використано цей симулятор, щоб дослідити застосування безмодельного НзП для ТнП. Автори протестували стандартний алгоритм Q-навчання, використовуючи табличні алгоритми та нейронні мережі, і виявили, що в змодельованому середовищі обидва підходи змогли знайти оптимальні шляхи атаки для різних топологій і розмірів мережі, не маючи моделі поведінки дій. Однак реалізовані алгоритми були практичними лише для менших мереж і кількості дій. Потрібна подальша робота над розробкою масштабованих алгоритмів НзП і тестуванням цих алгоритмів у великих середовищах із високою точністю [**Error! Reference source not found.**].

З. Ху, Р. Беуран та Ю. Тан представили автоматизовану структуру тестування на проникнення, яка використовує глибоке навчання з підкріпленням для автоматизації процесу тестування на проникнення [**Error! Reference source not found.**]. Автори запропонували використовувати цей фреймворк головним чином як компонент навчальної діяльності з кібербезпеки, щоб забезпечити кероване навчання навчанню атакам, використовуючи його для пропонування можливих стратегій. Додаючи підтримку для фактичних інструментів тестування на проникнення, фреймворк також можна використовувати в навчанні захисту, автоматично відтворюючи атаки в навчальному середовищі. Запропонований авторами підхід до автоматизованого тестування на проникнення складається з двох етапів. Спочатку автори використали пошукову систему Shodan [**Error! Reference source not found.**] для збору відповідних даних сервера, щоб побудувати реалістичну топологію мережі, а також використовували багатоетапний аналіз вразливостей на кількох хостах, щоб створити дерево атак для цієї топології. Традиційні алгоритми пошуку використовувалися для пошуку всіх можливих шляхів атаки в цьому дереві та для побудови матричного представлення для алгоритмів глибокого навчання з підкріпленням. На другому етапі автори запропонували використовувати метод Deep Q-Learning Network (DQN) [**Error! Reference source not found.**], щоб виявити найбільш простий у використанні шлях атаки з можливих. Цей підхід було оцінено шляхом створення тисяч вхідних сценаріїв, і DQN вдалося знайти оптимальний шлях із точністю 0,86, а також запропонувати дійсні рішення в інших випадках .

У своїй роботі Ф. М. Зеннаро та Л. Ердіоді дослідили застосування алгоритмів НзП для автоматизації процесів тестування на проникнення, використовуючи спрощені задачі у форматі змагань «Capture the Flag» (CTF) [**Error! Reference source not found.**]. Автори моделювали CTF-завдання як задачі НзП, де агент повинен виявити структуру проблеми та знайти оптимальні стратегії для досягнення мети. Вони підкреслили важливість балансу між алгоритмами безмодельного навчання та використанням апріорних знань для підвищення ефективності навчання агентів. Зокрема, було показано, що впровадження попередніх знань може звузити простір пошуку та прискорити процес навчання, що є критичним для успішного застосування НзП у тестуванні на проникнення. Дослідження авторів продемонструвало потенціал використання НзП для автоматизації етичного хакінгу, водночас підкреслюючи необхідність ретельного підходу до інтеграції різних методів навчання та знань для досягнення оптимальних результатів.

Р. Маеда та М. Мімура запропонували автоматизувати етапи експлуатації та пост-експлуатації в процесі тестування на проникнення, поєднуючи глибоке навчання з підкріпленням та інструмент PowerShell Empire [**Error! Reference source not found.**]. У їхньому підході агенти НзП обирають модулі PowerShell, використовуючи їхні внутрішні функції як стани та дії. Автори порівняли ефективність трьох моделей НзП:

A2C, Q-Learning та SARSA, і виявили, що модель A2C є найефективнішою. Навчений агент зміг отримати права адміністратора системи на контролері домену, демонструючи потенціал цього підходу для автоматизації складних завдань у тестуванні на проникнення.

Дослідники Нгуєн Тхань Конг та Нгуєн В'єт Хунг запропонували метод автоматизації тестування на проникнення, який поєднує алгоритми навчання з підкріпленням із реальним тестовим середовищем, створивши модель, оптимізовану за допомогою розміченого набору даних, та інтегрувавши її з інструментами виявлення вторгнень і атаки для оцінки продуктивності системи [**Error! Reference source not found.**]. Результати показали, що ця система може бути ефективно застосована для тестування систем різного масштабу, знижуючи витрати на тестування та забезпечуючи регулярну перевірку безпеки. Однак автори відзначили і обмеження, пов'язані з процесом сканування мережі та обмеженою кількістю інтегрованих інструментів.

У табл. 2 узагальнимо розглянуті підходи до тестування на проникнення із використанням НзП, виділивши їх переваги та недоліки.

Таблиця 2

Переваги та недоліки підходів тестування на проникнення із використанням НзП

Коротка характеристика підходу	Переваги	Недоліки
Використання НзП для автоматизації тестування на проникнення через інтеграцію з фреймворком MITRE ATT&CK. Підхід включає розробку інструменту на Python для виявлення вразливостей, адаптацію до змін середовища.	Підвищення точності виявлення вразливостей, адаптивність до змін середовища.	Можливе підвищення складності в розробці та інтеграції інструментів.
Використання ШІ для автоматичного створення топології мережі та дерева атак. Підхід підтримує навчання та розвиток навичок у кібербезпеці.	Висока адаптивність, зниження помилкових тривог, покращення навчання захисту.	Потребує значних ресурсів для навчання та обчислень.
Розробка Інтелектуальної Автоматизованої Системи Тестування на Проникнення (IAPTS) з використанням НзП для моделювання PT як POMDP.	Зменшення витрат людських ресурсів, покращення точності та надійності тестування.	Складність вирішення POMDP для великих мереж.
Використання безмодельного НзП для автоматизованого пентестування, що не вимагає моделі середовища, навчання через взаємодію з середовищем.	Без потреби у моделі середовища, можливість тестування без попередніх знань про мережу.	Обмеженість застосування на великих мережах та складних топологіях
Використання глибокого підсилювального навчання для автоматизації тестування на проникнення, включаючи два етапи: збір даних для побудови топології та використання DQN для виявлення атак.	Висока точність знаходження оптимальних шляхів атаки, адаптивність до різних сценаріїв.	Потребує значних обчислювальних потужностей для реалізації
Моделювання задач тестування на проникнення у форматі CTF з використанням НзП, акцент на баланс між безмодельним навчанням та апріорними знаннями.	Можливість навчання стратегій в умовах обмеженої інформації, адаптивність до нових ситуацій.	Залежність від спрощених задач CTF, що не завжди відображає реальні умови
Підхід Intelligent Automated Penetration Testing Framework (IAPTF), який використовує методи НзП для автоматизації тестування на проникнення в великих мережах. IAPTF розглядає завдання тестування на проникнення	Зменшення навантаження, масштабованість, легкість повторення, покращена точність	Складність налаштування і початкової адаптації, необхідність в значних обчислювальних ресурсах, залежність від даних,

як частково спостережуваний марківський процес прийняття рішень (POMDP).		необхідність моделювання специфічних умов
Ієрархічне навчання з підкріпленням (Hierarchical НзП) для великих і складних мереж	Покращена масштабованість та ефектив-ність для великих середовищ, зниження складності обчислень	Складність в налаштуванні і необхідність ієрархічного моделювання
Безмодельне навчання з підкріпленням (Model-Free НзП)	Підвищена гнучкість, не вимагає попередніх знань про середовище, адаптивність до нових загроз	Проблеми зі складними та великими середовищами, обмеження в плануванні на великих мережах
Глибоке навчання для автоматизації тестування на проникнення (Deep НзП)	Висока точність виявлення вразливостей, можливість вибору оптимальних стратегій	Високі вимоги до обчислювальних ресурсів, складність налаштування моделей

Загалом, на сьогоднішній день, розробляється кілька підходів до автоматизації тестування на проникнення з використанням НзП, і кожен з них має певні переваги та обмеження. Зокрема можна виділити такі основні перспективні напрямки:

1) інтеграція з існуючими інструментами та середовищами, наприклад MITRE ATT&CK, CIS Controls, Cyber Kill Chain [**Error! Reference source not found.**], [**Error! Reference source not found.**]. Перевагами даного підходу є те, що інтеграція з відомими фреймворками, такими як MITRE ATT&CK, дозволяє автоматизованим системам НзП виявляти вразливості, які можуть бути пропущені тестувальниками, і адаптуватися до змін у середовищі. У перспективі це дозволяє знижувати навантаження на фахівців з кібербезпеки, даючи можливість на основі накопиченого досвіду покращувати результати тестування на проникнення;
2) моделювання атак за допомогою дерева можливих атак та навчання в контрольованих середовищах. До переваг даного підходу доцільно віднести те, що цей підхід дозволяє створювати реалістичні топології мережі, що використовується для симуляції атак, що у перспективі дає змогу фахівцям з кібербезпеки навчатися різних стратегій вторгнення та реагування. Цей підхід є перспективним, оскільки завдяки застосуванню машинного навчання з глибоким підкріпленням, здатний значно знизити кількість помилок і збільшити точність тестувань;
3) моделювання процесів тестування як частково спостережуваних марківських процесів (POMDP). Цей підхід має переваги у тому, що використання POMDP дозволяє системам адаптуватися до різних контекстів та обмежень, таких як час та обчислювальні потужності, а також планувати та виконувати складні атаки. І в перспективі цей підхід може значно підвищити точність тестування на проникнення, а також зменшити витрати на людські ресурси;
4) безмодельне навчання з підкріпленням (Model-free НзП). Безмодельне НзП має суттєву перевагу, оскільки не вимагає складних моделей середовища і може адаптуватися до швидко змінюваних умов кіберпростору. У перспективі це дозволяє створювати системи, які самостійно вивчають оптимальні стратегії атаки без необхідності мати попереднє знання про середовище, що робить їх більш гнучкими і адаптивними до нових типів загроз;

5) використання багатоступеневого навчання з підкріпленням (DQN та інші методи). До переваг застосування даного підходу доцільно віднести той факт, що цей підхід дозволяє виявляти оптимальні шляхи атаки і адаптуватися до змін у топології мережі. Дослідження показують високу точність виявлення вразливостей. Оскільки методи DQN можуть досягати високих результатів у малих та середніх мережах, вони мають великий потенціал для застосування в реальних умовах за рахунок подальшого розвитку та масштабування.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Застосування методів МН відкриває нові можливості для автоматизації та підвищення ефективності тестування на проникнення. Основні підходи до тестування на проникнення з використанням навчання з підкріпленням передбачають автоматизацію процесу тестування. Використання НзП дозволяє створювати автоматизовані системи, здатні самостійно навчатися та адаптуватися до змінних загроз, що підвищує ефективність виявлення вразливостей. При цьому перспективними є підходи, що використовують багатоступеневе навчання з підкріпленням та моделювання процесів як частково спостережуваних марківських процесів, так як вони надають можливість автоматизувати тестування на проникнення, зменшити кількість помилкових сповіщень і підвищити точність, при цьому дозволяючи адаптуватися до змін у середовищі. Безмодельне навчання і інтеграція з існуючими фреймворками також мають великий потенціал, дозволяючи розробляти адаптивні, гнучкі системи, які можуть працювати в умовах високої динаміки кіберзагроз.

Подальші дослідження в галузі автоматизації тестування на проникнення з використанням методів НзП повинні бути зосереджені на кількох ключових напрямках, а саме: масштабуванні та оптимізації методів НзП для великих мереж, покращення характеристик адаптивності моделей; дослідження можливостей та напрямів інтеграції з існуючими платформами кібербезпеки; зниження кількості помилкових тривог тощо. В загальному, подальші дослідження повинні бути спрямовані на підвищення ефективності, масштабованості та адаптивності систем автоматизованого тестування на проникнення з використанням навчання з підкріпленням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Cybersecurity – is (n. d.)*. FoxmindEd. https://foxminded.ua/kiberbezpeka-tse/
2. Clintswood, Lie, D. G., Kuswandana, L., Nadia, Achmad, S., & Suhartono, D. (2023). The usage of machine learning on penetration testing automation. *In 2023 3rd international conference on electronic and electrical engineering and intelligent system (ICE3IS)*. IEEE. https://doi.org/10.1109/ice3is59323.2023.10335188
3. Hu, Z., Beuran, R., & Tan, Y. (2020). Automated penetration testing using deep reinforcement learning. *In 2020 IEEE european symposium on security and privacy workshops (euros&pw)*. IEEE. https://doi.org/10.1109/eurospw51379.2020.00010
4. Jagamogan, R. S., Ismail, S. A., Hassan, N. H., & Abas, H. (2022). Penetration testing procedure using machine learning. У *2022 4th international conference on smart sensors and application (ICSSA)*. IEEE. https://doi.org/10.1109/icssa54161.2022.9870951
5. Tolkachova, A., Posuvailo, M-M. (2024). Penetration testing using deep reinforcement learning. *Cybersecurity: education, science, technology*, 17–30. https://doi.org/10.28925/2663-4023.2024.23.1730

6. Ghanem, M. C., & Chen, T. M. (2018). Reinforcement learning for intelligent penetration testing. *In 2018 second world conference on smart trends in systems, security and sustainability (worlds4)*. IEEE. https://doi.org/10.1109/worlds4.2018.8611595
7. Ghanem, M. C., & Chen, T. M. (2019). Reinforcement learning for efficient network penetration testing. *Information, 11(1), 6.* https://doi.org/10.3390/info11010006
8. Prytula, A. V., & Kupershtein, L. M., (2024). Application of reinforcement learning methods in penetration testing: Effectiveness, challenges and prospects. *In Proceedings of the Fourth Scientific and Technical Conference*, 78–79.
9. Skybun, O. (2022). Penetration Testing: purpose and objectives. *Grail of Science, (22),* 161–163. https://doi.org/10.36074/grail-of-science.25.11.2022.28
10. Prytula, A. V., & Kupershtein, L. M., (2024). Application of artificial intelligence for penetration testing. *LIII All-Ukrainian Scientific and Technical Conference of the Faculty of Information Technologies and Computer Engineering. Vinnytsia National Technical University*.
11. Joseph, T. (2023). Influence of AI and Machine Learning on Pen Testing. *QASource Blog*. https://blog.qasource.com/the-influence-of-ai-and-machine-learning-on-pen-testing
12. Ghanem, M. C., Chen, T. M., & Nepomuceno, E. G. (2022). Hierarchical reinforcement learning for efficient and effective automated penetration testing of large networks. *Journal of Intelligent Information Systems*. https://doi.org/10.1007/s10844-022-00738-0
13. Schwartz, J., & Kurniawati, H. (2019, May 15). *Autonomous penetration testing using reinforcement learning*. arXiv.org. https://arxiv.org/abs/1905.05965
14. *Search engine for the internet of everything.* (n. d.). Shodan Search Engine. https://www.shodan.io/
15. Dhumne, S. (2023). *Deep Q-Network (DQN).* Medium. https://medium.com/@shruti.dhumne/deep-q-network-dqn-90e1a8799871
16. Zennaro, F., & Erd´odi, L. (2021). *Modeling Penetration Testing with Reinforcement Learning Using Capture-the-Flag Challenges: Trade-offs between Model-free Learning and A Priori Knowledge*. arXiv.org. https://arxiv.org/pdf/2005.12632
17. Maeda, R., & Mimura, M. (2021). Automating post-exploitation with deep reinforcement learning. *Computers & Security*, *100*, *102108*. https://doi.org/10.1016/j .cose.2020.102108
18. Hùng, N. V., & Công, N. T. (2023). Applying reinforcement learning in automated penetration testing. *Journal of Science and Technology on Information Security*, *3(17),* 61–77. https://doi.org/10.54654/isj.v3i17.876
19. Kupershtein, L. M., Prytula, A. V., & Malinovskyi, V. I. (2024). Analysis of web application penetration testing technologies. *Scientific papers of Vinnytsia National Technical University*, (2). https://doi.org/10.31649/2307-5376-2024-2-45-53

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Andrii Prytula
PhD student of Information Protection Department
LLC "ValueTek"
ORCID ID: 0009-0006-9632-0712
andrik.pritula@gmail.com

Leonid Kupershtein
PhD, Associate Professor of Information Protection Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

ANALYSIS OF PENETRATION TESTING APPROACHES USING REINFORCEMENT LEARNING

Abstract. Penetration testing (PT) is an important method for ensuring digital security, which allows to assess the presence of vulnerabilities in systems and networks through attack simulations. Due to the rapid development of technologies and the growth of digital threats, there is a need to improve testing methods, in particular through the implementation of machine learning (ML) and reinforcement learning (RL) algorithms. The article discusses modern approaches to automating penetration testing using machine learning and reinforcement learning, which can significantly increase the efficiency and accuracy of the process. Penetration testing includes several stages, such as collecting information about the target system, scanning, analyzing threats and vulnerabilities, exploitation, generating a report, etc. Traditional methods often require significant human resources and time. The implementation of artificial intelligence (AI) and ML allows to automate these stages, which leads to a significant reduction in time and increased testing efficiency. In particular, the NLP-based approach demonstrates high potential for adapting to changes in the testing environment, allowing systems to independently improve their strategies over time, based on experience. The article reviews various approaches, including the use of deep learning and model-free NLP methods for penetration testing automation. The advantages and limitations of each approach are analyzed, including the importance of adaptability to environmental changes, high accuracy of vulnerability detection, and the difficulties that arise when integrating and configuring tools, especially for large and complex networks. Possible challenges associated with the use of significant computing power and the need to model specific conditions are also considered. As a result of the study, the most relevant approaches to penetration testing automation using reinforcement learning methods have been identified, which have significant potential for increasing the efficiency and adaptability of testing processes. Future research prospects focus on expanding the capabilities of NFP models for application in complex and large networks, as well as on integration with other cybersecurity platforms to create more comprehensive and efficient automated testing systems.

Keywords: penetration testing; machine learning; reinforcement learning; automation; cybersecurity; vulnerabilities; threats; artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Cybersecurity – is (n. d.).* FoxmindEd. https://foxminded.ua/kiberbezpeka-tse/
2. Clintswood, Lie, D. G., Kuswandana, L., Nadia, Achmad, S., & Suhartono, D. (2023). The usage of machine learning on penetration testing automation. *In 2023 3rd international conference on electronic and electrical engineering and intelligent system (ICE3IS)*. IEEE. https://doi.org/10.1109/ice3is59323.2023.10335188
3. Hu, Z., Beuran, R., & Tan, Y. (2020). Automated penetration testing using deep reinforcement learning. *In 2020 IEEE european symposium on security and privacy workshops (euros&pw)*. IEEE. https://doi.org/10.1109/eurospw51379.2020.00010

4. Jagamogan, R. S., Ismail, S. A., Hassan, N. H., & Abas, H. (2022). Penetration testing procedure using machine learning. У *2022 4th international conference on smart sensors and application (ICSSA)*. IEEE. https://doi.org/10.1109/icssa54161.2022.9870951
5. Tolkachova, A., Posuvailo, M-M. (2024). Penetration testing using deep reinforcement learning. *Cybersecurity: education, science, technology*, 17–30. https://doi.org/10.28925/2663-4023.2024.23.1730
6. Ghanem, M. C., & Chen, T. M. (2018). Reinforcement learning for intelligent penetration testing. *In 2018 second world conference on smart trends in systems, security and sustainability (worlds4)*. IEEE. https://doi.org/10.1109/worlds4.2018.8611595
7. Ghanem, M. C., & Chen, T. M. (2019). Reinforcement learning for efficient network penetration testing. *Information, 11(1), 6.* https://doi.org/10.3390/info11010006
8. Prytula, A. V., & Kupershtein, L. M., (2024). Application of reinforcement learning methods in penetration testing: Effectiveness, challenges and prospects. *In Proceedings of the Fourth Scientific and Technical Conference*, 78–79.
9. Skybun, O. (2022). Penetration Testing: purpose and objectives. *Grail of Science, (22),* 161–163. https://doi.org/10.36074/grail-of-science.25.11.2022.28
10. Prytula, A. V., & Kupershtein, L. M., (2024). Application of artificial intelligence for penetration testing. *LIII All-Ukrainian Scientific and Technical Conference of the Faculty of Information Technologies and Computer Engineering. Vinnytsia National Technical University*.
11. Joseph, T. (2023). Influence of AI and Machine Learning on Pen Testing. *QASource Blog*. https://blog.qasource.com/the-influence-of-ai-and-machine-learning-on-pen-testing
12. Ghanem, M. C., Chen, T. M., & Nepomuceno, E. G. (2022). Hierarchical reinforcement learning for efficient and effective automated penetration testing of large networks. *Journal of Intelligent Information Systems*. https://doi.org/10.1007/s10844-022-00738-0
13. Schwartz, J., & Kurniawati, H. (2019, May 15). *Autonomous penetration testing using reinforcement learning*. arXiv.org. https://arxiv.org/abs/1905.05965
14. *Search engine for the internet of everything.* (n. d.). Shodan Search Engine. https://www.shodan.io/
15. Dhumne, S. (2023). *Deep Q-Network (DQN).* Medium. https://medium.com/@shruti.dhumne/deep-q-network-dqn-90e1a8799871
16. Zennaro, F., & Erd´odi, L. (2021). *Modeling Penetration Testing with Reinforcement Learning Using Capture-the-Flag Challenges: Trade-offs between Model-free Learning and A Priori Knowledge*. arXiv.org. https://arxiv.org/pdf/2005.12632
17. Maeda, R., & Mimura, M. (2021). Automating post-exploitation with deep reinforcement learning. *Computers & Security*, *100*, *102108*. https://doi.org/10.1016/j .cose.2020.102108
18. Hùng, N. V., & Công, N. T. (2023). Applying reinforcement learning in automated penetration testing. *Journal of Science and Technology on Information Security*, *3(17)*, 61–77. https://doi.org/10.54654/isj.v3i17.876
19. Kupershtein, L. M., Prytula, A. V., & Malinovskyi, V. I. (2024). Analysis of web application penetration testing technologies. *Scientific papers of Vinnytsia National Technical University*, (2). https://doi.org/10.31649/2307-5376-2024-2-45-53