УДК 004.056:004.85

Є. А. Садовник

ЗАГРОЗА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ТРАДИЦІЙНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ: АНАЛІЗ ВРАЗЛИВОСТЕЙ НА ПРИКЛАДІ НЕЙРОМЕРЕЖІ PASSGAN

Вінницький національний технічний університет

Анотація. *У роботі досліджено зміну підходів до зламу паролів під впливом генеративно-змагальних мереж (GAN) на прикладі ШІ-інструменту PassGAN. Проаналізовано механізми, за допомогою яких алгоритми вивчають статистичні закономірності та поведінкові звички користувачів, перетворюючи злам зі звичайного перебору на ймовірнісне прогнозування. Запропоновано нові методи захисту корпоративних і персональних даних в умовах еволюції кіберзагроз.*

Ключові слова: штучний інтелект, кібербезпека, PassGAN, злам паролів, генеративно-змагальні мережі, автентифікація.

Abstract. *This paper examines how generative adversarial networks (GANs) are changing password-cracking approaches, using the AI tool PassGAN as an example. It analyzes the mechanisms by which algorithms learn statistical patterns and user behavior, transforming password cracking from a brute-force attack into a probabilistic prediction. New methods for protecting corporate and personal data in the context of evolving cyber threats are proposed.*

Keywords: artificial intelligence, cybersecurity, PassGAN, password cracking, generative adversarial networks, authentication.

Вступ

Звична автентифікація за допомогою паролів поступово втрачає свою надійність в умовах стрімкого розвитку технологічних загроз. В епоху швидкого розвитку штучного інтелекту (ШІ) та машинного навчання, злам облікових даних стає значно простішим і швидшим порівняно з використанням звичайних методів. Раніше зловмисники здебільшого покладалися на інструменти на кшталт John the Ripper або Hashcat, які оперують визначеними людиною правилами для перебору та генерування здогадок. Проте сьогодні їм на зміну приходять інструменти, що працюють на основі генеративно-змагальних мереж (GAN) [1]. Найяскравішим прикладом такої еволюції є нейромережа PassGAN, яка ефективно підбирає паролі, аналізуючи поведінкові особливості користувачів. Метою цієї роботи є аналіз загроз, які несе застосування генеративного ШІ для традиційної автентифікації, а також визначення ефективних методів захисту інформації.

Результати дослідження

PassGAN працює завдяки двом нейромережам, які постійно взаємодіють між собою: генератору та дискримінатору. Генератор створює нові варіанти паролів, тоді як дискримінатор оцінює їхню реалістичність на основі вивчених баз даних із реальними витоками паролів [1]. Це дає змогу системі безперервно самонавчатися та генерувати точні комбінації без жодного втручання людини. Завдяки такій високій автономності та ефективності, швидкість роботи подібних алгоритмів створює критичну загрозу для корпоративних і персональних даних. Згідно з дослідженнями, нейромережа здатна зламати 51% типових паролів менш ніж за одну хвилину. Протягом однієї години цей показник досягає 65%, за добу – 71%, а через місяць безперервної роботи PassGAN успішно підбирає до 81% паролів із досліджуваної вибірки [2]. Більше того, додатково встановлено, що навіть 7-символьний пароль, який містить комбінацію великих та малих літер, цифр і спецсимволів, піддається зламу всього за шість хвилин [3].

Особлива небезпека PassGAN полягає в тому, що алгоритм досягає таких результатів не шляхом сліпого повного перебору (brute-force), а через глибоке розуміння поведінки користувача. Нейромережа навчається на мільйонах реальних паролів і швидко засвоює такі поведінкові звички, як написання першої літери з великої, додавання цифр або знаку оклику в кінці, заміна літер на візуально схожі символи (наприклад, «а» на «@», а «е» на «3»), а також часте використання дат народжень чи імен [4]. Таким чином, алгоритм зосереджується виключно на тих комбінаціях, що відповідають типовим людським звичкам, нагадуючи досвідченого зламника, який аналізує відомі вразливості. Ефективність такого аналізу була підтверджена тестуванням на масиві з понад 15 мільйонів паролів, яке наочно продемонструвало, що звичні паролі вже не здатні забезпечити надійний захист [5]. Ситуацію критично ускладнює й людський фактор: близько 62% співробітників повторно використовують одні й ті самі паролі або їхні незначні варіації для різних сервісів, що робить корпоративні мережі більш вразливішими до атак [1].

Для протидії таким загрозам експерти пропонують змінити підходи до захисту. Зокрема, рекомендується переходити до використання складних паролів довжиною понад 15 символів, які повністю позбавлені очевидних слів чи патернів на кшталт «1234» [5]. Крім того, необхідно регулярно оновлювати облікові дані та суворо уникати їхнього повторного використання на різних ресурсах. Важливим елементом сучасної безпеки також є застосування офлайн-менеджерів паролів для надійного збереження даних та обов'язкове впровадження багатофакторної автентифікації (MFA) для забезпечення додаткового рівня захисту [1; 3; 4].

Висновки

Розвиток штучного інтелекту, зокрема нейромережі PassGAN, повністю змінює напрямок кіберзагроз, перетворюючи процес зламу паролів із завдання грубої сили на процес ймовірнісного прогнозування та розпізнавання поведінкових патернів. Здатність ШІ автоматично навчатися на поведінкових звичках користувачів робить традиційні методи автентифікації застарілими та небезпечними. Для збереження конфіденційності як користувачам, так і бізнесу необхідно впроваджувати комплексну стратегію захисту, що включає використання унікальних багатосимвольних паролів, парольних менеджерів та систем багатофакторної автентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How cracking passwords can be easier in the age of AI/ML. *Okta*. URL: https://www.okta.com/en-au/blog/product-innovation/how-cracking-passwords-can-be-easier-in-the-age-of-aiml/ (date of access: 13.05.2026).
2. Report 2962. *AI Incident Database*. URL: https://incidentdatabase.ai/reports/2962/ (date of access: 13.05.2026).
3. AI Cracks Passwords in Less than a Minute: Securing Against the Threat. *Atlancube*. URL: https://www.atlancube.com/blogs/blog/ai-cracks-passwords-in-less-than-a-minute-securing-against-the-threat (date of access: 13.05.2026).
4. PassGAN: How AI Cracks Passwords in Seconds. *Safe Password Generator*. URL: https://safepasswordgenerator.net/blog/passgan-ai-password-cracking/ (date of access: 13.05.2026).
5. AI Roundup: Guessing passwords, conjuring images out of peoples' minds, and… writing fortune cookies? *The Hustle*. URL: https://thehustle.co/ai-roundup-guessing-passwords-conjuring-images-out-of-peoples-minds-and-writing-fortune-cookies (date of access: 13.05.2026).

Садовник Євгеній Анатолійович – студент групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: sadovnikevgenii@gmail.com

Науковий Керівник: ***Радченко Євгеній Валентинович*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: eradchenko@vntu.edu.ua

Sadovnyk Yevhenii A. – student of 1BS-24b group, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: sadovnikevgenii@gmail.com

Supervisor: ***Yevhenii Radchenko V.*** – Assistant professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: eradchenko@vntu.edu.ua