УДК 004.89

Марія МИКОЛИШИН

Західноукраїнський національний університет

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ

Вступ. Сучасні мобільні пристрої відіграють важливу роль у житті кожного користувача, адже саме вони зберігають величезну кількість приватної інформації, від особистих фотографій до банківських даних та ділової інформації. Кількість мобільних додатків, які використовують люди, стрімко зростає, так само, як і ризики, пов'язані з їх використанням.

Впровадження штучного інтелекту у забезпечення безпеки різноманітних мобільних додатків дозволяє значно підвищити захист користувацьких даних та знизити вразливість перед кібератаками, що і визначає актуальність даної роботи.

Мета: аналіз методів використання штучного інтелекту для підвищення безпеки мобільних додатків, виявлення ключових переваг застосування ШІ у цій галузі та наведення практичних прикладів інтеграції технологій ШІ у мобільні платформи.

1. Прогнозування кіберзагроз за допомогою штучного інтелекту

Штучний інтелект (ШІ) відкриває нові можливості для передбачення і прогнозування кіберзагроз, що є надзвичайно важливим для безпеки мобільних додатків. Технології машинного навчання та аналізу даних дозволяють системам безпеки мобільних додатків автоматично виявляти аномалії та потенційно небезпечні патерни, навіть ще до того, як вони можуть призвести до серйозних загроз.

Використовуючи алгоритми, ШІ може обробляти величезні обсяги інформації про попередні атаки, виявляти схожі моделі і створювати прогнози для майбутніх загроз, що дозволяє мобільним додаткам ефективно реагувати на можливі атаки в реальному часі.

Одним із основних аспектів є можливість ШІ ідентифікувати відхилення від звичайної поведінки користувачів або аномалії в мережевому трафіку. Наприклад, система може зафіксувати спроби входу з нових локацій, нестандартну активність або надмірну кількість транзакцій, що можуть свідчити про спробу злому або шахрайства.

Такий підхід дозволяє не тільки виявляти загрози, але й здійснювати превентивні заходи, знижуючи можливі збитки і зменшуючи час, необхідний для реагування на інциденти безпеки. У поєднанні з іншими методами, такими як аналіз великих даних, прогнозування на основі історичних атак забезпечує значно кращу захист мобільних додатків від кіберзагроз.

Використання ШІ для прогнозування кіберзагроз (рисунок 1) є особливо корисним в умовах, коли традиційні методи безпеки, як-от статичні алгоритми виявлення загроз, можуть бути недостатньо ефективними для боротьби з новими, раніше невідомими атаками.

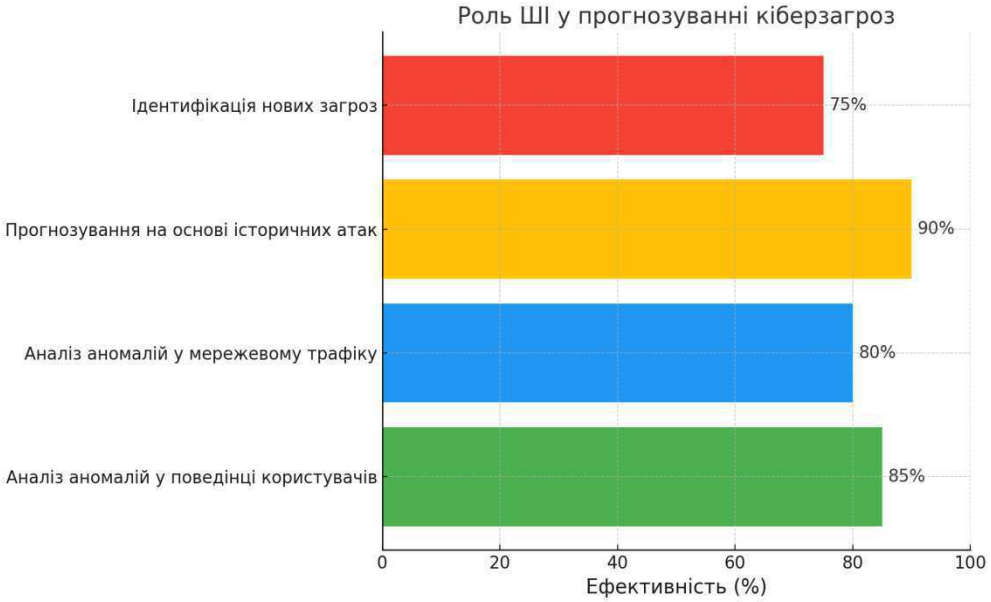

Рисунок 1 - Роль ШІ у прогнозуванні кіберзагроз

Оскільки атаки на мобільні додатки постійно змінюються і адаптуються до нових умов, прогнозування і проактивний підхід дозволяють швидко реагувати на нові види кіберзагроз, до того як вони завдадуть шкоди [1].

2. Машинне навчання для посилення шифрування і захисту даних мобільних додатків

ШІ та машинне навчання активно використовуються для вдосконалення методів шифрування і захисту даних у мобільних додатках, що є критично важливим для безпеки користувачів. Сучасні мобільні додатки зберігають величезні обсяги особистих даних, включаючи фінансову інформацію, особисті документи та конфіденційну переписку, що робить їх привабливою ціллю для кіберзлочинців. Машинне навчання дозволяє створювати більш складні і адаптивні методи шифрування, що можуть швидко реагувати на нові загрози та вдосконалюватися з часом, вивчаючи поведінку кіберзлочинців і виявляючи їхні нові стратегії.

Однією з важливих переваг використання машинного навчання для шифрування є здатність адаптувати системи шифрування до нових типів атак, таких як атаки через квантові обчислення або спроби злому через слабкі паролі. Наприклад, алгоритми ШІ можуть бути використані для виявлення та посилення вразливостей в алгоритмах шифрування на основі змінних умов, таких як місце розташування користувача або поведінка його пристрою. Це дозволяє значно підвищити рівень захисту даних, роблячи їх менш вразливими до атак.

Дослідження, проведене командою фахівців з Університету Каліфорнії в Лос-Анджелесі (UCLA), показало, що застосування машинного навчання для криптографії значно збільшує ефективність шифрування. Вони використовували методи глибокого навчання для автоматичного виявлення нових слабких місць у алгоритмах шифрування і створення адаптивних захисних механізмів, здатних швидко реагувати на зміни в атаках.

За словами авторів, такі підходи значно покращують безпеку мобільних додатків, роблячи їх більш стійкими до нових загроз і знижуючи ймовірність

витоку конфіденційної інформації [2].

Машинне навчання також допомагає у вдосконаленні методів генерації паролів і аутентифікації, що є критичними для захисту користувачів. Алгоритми можуть аналізувати патерни поведінки користувачів і створювати більш складні, але при цьому зручні для запам'ятовування паролі.

Крім того, система машинного навчання може автоматично виявляти слабкі паролі і пропонувати користувачам замінити їх на більш безпечні варіанти, що значно знижує ризик злому акаунтів.

Інші дослідження підтверджують, що використання методів машинного навчання в комбінації з багатофакторною аутентифікацією дозволяє значно посилити захист даних. У дослідженні, опублікованому в журналі Computers Security, зазначено, що системи з використанням машинного навчання і біометрії для аутентифікації користувачів забезпечують більш високий рівень безпеки, ніж традиційні методи паролів [3].

Це важливо, оскільки з кожним роком збільшується кількість інцидентів, пов'язаних із крадіжкою паролів та іншими формами несанкціонованого доступу до особистих даних користувачів мобільних додатків .

ШІ також допомагає у постійному оновленні алгоритмів шифрування, що дозволяє створювати системи, які адаптуються до нових атак в реальному часі. Завдяки таким підходам мобільні додатки можуть не тільки захищати дані, але й забезпечувати найвищий рівень конфіденційності для своїх користувачів, що є важливим фактором для збереження їх довіри та безпеки в цифровому середовищі.

Висновок. У роботі проаналізовано застосування штучного інтелекту для підвищення безпеки мобільних додатків. Зокрема, розглянуто можливості прогнозування кіберзагроз за допомогою машинного навчання, яке дозволяє своєчасно виявляти аномалії і знижувати ризик атак.

Крім того, приділено увагу використанню ШІ для вдосконалення методів шифрування даних та аутентифікації, що забезпечує більш високий рівень захисту персональної інформації користувачів.

Перелік використаних джерел.

1. Samar, S. (2022). AI-based threat prediction models for mobile application security. Journal of Cyber Security and Technology.

2. Chen, Z., Zhou, X. (2022). Machine learning-based cryptographic systems for mobile application security. Computers Security.

3. Ruan, K., Liu, T. (2023). Adaptive encryption methods for mobile app data protection using AI. Journal of Artificial Intelligence and Security.