ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В DLP-СИСТЕМАХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Єнальєва Г.С., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні загрози інформаційній безпеці постійно розвиваються, створюючи значні проблеми для захисту конфіденційних даних. Системи Data Loss Prevention (DLP) є ключовим інструментом у боротьбі з витоком інформації. Однак звичайні методи часто виявляються недостатньо ефективними в умовах зростаючої складності кіберзагроз [1]. Впровадження штучного інтелекту (ШІ) у DLP-системи дозволяє значно підвищити ефективність виявлення, класифікації та запобігання втратам даних. Це робить їх більш адаптивними та надає можливість реагувати на нові атаки [2]. Інтеграція ШІ у DLP-системи покращує автоматизоване виявлення загроз завдяки алгоритмам машинного навчання, які аналізують значні обсяги трафіку в реальному часі, виявляючи аномалії та підозрілу активність. Обробка природної мови (NLP) сприяє більш точному контекстуальному аналізу даних, що забезпечує кращу класифікацію конфіденційної інформації. Головною перевагою цих систем є здатність знижувати кількість хибних спрацьовувань, оскільки ШІ ефективно розрізняє справжні загрози від безпечних дій, що посилює заходи безпеки [3].

Метою доповіді є аналіз можливостей використання штучного інтелекту в DLP-системах для підвищення ефективності інформаційної безпеки, зокрема виявлення загроз, класифікації конфіденційних даних та мінімізації ризику їх витоку.

Інтеграція ШІ дозволяє DLP-системам не лише реагувати на порушення, але й прогнозувати ризики, аналізувати поведінку користувачів і розрізняти нормальні та підозрілі дії.

В доповіді наводяться результати дослідження впливу алгоритмів машинного навчання та прогнозної аналітики на функціональність DLP. Адаптивність і масштабованість є значними перевагами використання ШІ в DLP-системах, оскільки алгоритми постійно навчаються на основі нових даних, що дозволяє коригувати політики безпеки відповідно до нових загроз. Це особливо корисно для великих організацій із розгалуженою розподіленою інфраструктурою, де традиційні системи безпеки можуть не справлятися з обробкою значних обсягів інформації.

Використання ШІ в DLP-системах суттєво підвищує інтеграцію з SIEM та SOAR системами. Штучний інтелект автоматично передає дані про витоки (або потенційні витоки) з DLP до SIEM (систем управління інформаційною безпекою), які аналізують ці дані у загальному контексті безпеки: логіни, мережеві аномалії, привілейовані дії. Потім, у SOAR (платформах автоматизації відповідей), ШІ може ініціювати автоматичне блокування, сповіщення або розслідування.

Важливою складовою є також виявлення внутрішніх загроз. Системи, керовані ШІ, можуть аналізувати поведінку користувачів, створюючи профілі типових дій і виявляючи відхилення, які можуть свідчити про потенційні внутрішні загрози [4]. Крім того, використання прогнозної аналітики дає змогу передбачати можливі витоки даних шляхом аналізу історичних тенденцій, тим самим полегшуючи коригування політик безпеки. Цей комплексний підхід сприяє створенню безпечнішого та стійкішого інформаційного середовища [2].

Попри значні переваги, інтеграція ШІ у DLP-системи супроводжується певними викликами. Основна проблема полягає в забезпеченні конфіденційності даних, враховуючи, що для навчання моделей ШІ зазвичай потрібні великі набори даних. Крім того, постійна розробка та підтримка AI-рішень вимагає значних фінансових і кадрових ресурсів. Додатковий виклик є складність інтерпретації рішень, керованих ШІ, може створювати перешкоди, оскільки деякі моделі працюють як "чорний ящик". Ця непрозорість ускладнює здатність аналізувати основні фактори, що сприяють певним активаціям [3].

Також деяким проблемним питанням є те, що навчання моделей потребує якісних даних.

Останнім часом проблемним стає можливість обходу ШІ-перевірки шляхом обфускації даних. Подолання цієї проблеми можливо тільки у разі правильного навчання і використання комбінації технологій.

Впровадження DLP-систем на основі штучного інтелекту є значним прогресом у розвитку інформаційної безпеки.

Такі системи пропонують підвищену точність, масштабованість і гнучкість.

Хоча можуть виникнуть певні виклики, як захист конфіденційності даних та значні ресурси, вони можуть бути ефективно вирішені шляхом продуманого планування та впровадження сучасних технологічних рішень.

Список літератури

1. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків : ХНУРЕ, 2019. – С. 104–105.

2. Dorcas Esther. AI in Data Loss Prevention: Safeguarding Sensitive Data Against Unauthorized Access and Leakage.

3. Kunle-Lawanson O. The Role of AI in Information Security Risk Management. World Journal of Advanced Engineering Technology and Sciences, vol. 7, no. 2, 2022, pp. 308–319.

4. Пасєка І., Сєвєрінов О.В. Проблеми впровадження системи аналітики поведінки користувачів та сутностей // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків: ХНУРЕ, 2019. – С. 82–83.