Запропонований алгоритм дозволяє перевірити, чи всі дані з бази даних потрапили до резервної копії, та чи не були вони пошкоджені під час процесу створення резервної копії, звісно є дуже малий шанс того, що під час обчислення обох хеш сум резервні копії будуть пошкоджені однаково і перевірка буде успішною. Використання алгоритму MD5 забезпечує високу швидкість обчислень, однак він має обмеження в контексті криптографічної стійкості. Наприклад, MD5 уразливий до атак типу "зіткнення", що може бути критичним для деяких застосувань. Однак для цілей перевірки цілісності резервних копій цей алгоритм є прийнятним завдяки своїй ефективності.

Для перевірки методу було проведено тестування на реальних даних. У результаті було підтверджено, що метод здатний виявляти навіть незначні розбіжності між вихідними даними та резервними копіями. Крім того, запропонований підхід є універсальним і може бути адаптований для інших баз даних та форматів резервного копіювання.

Метод перевірки хеш-сум забезпечує ефективний механізм контролю цілісності резервних копій баз даних. Запропонована методологія дозволяє виявляти втрати чи пошкодження даних під час резервування, що підвищує загальну надійність системи.

1. Смарт Н. Криптографія пер. с англ. / Н. Смарт – М.: Техносфера, – 2005 – 528с.
2. Борд Р.В., Лозовська Л.І., «Методологічний вибір хеш-функції для оптимальної синхронізації бази даних національних парків Хорватії». – 2016. , – С. 25-27.

Виявлення та запобігання витоку даних у реальному часі за допомогою систем моніторингу мережевого трафіку

УДК 004.056.5 (043.2)
Іван Тихонов[1], Олександр Сиропятов[2]
Національний університет «Одеська Політехніка»,
[1]9560414@stud.op.edu.ua, [2]o.a.syropiatov@op.edu.ua

У сучасних інформаційних середовищах захист конфіденційних даних набуває особливої актуальності: лише у 2024 році кількість інцидентів витоку даних у світі зросла на 25% порівняно з попереднім роком. Збільшення складності кібератак, поява нових векторів проникнення, а також використання зловмисниками штучного інтелекту та машинного навчання вимагають переходу від класичних методів безпеки до систем, що аналізують мережевий трафік у реальному часі. Мета роботи – розробити методику виявлення та запобігання витоку даних у режимі реального часу шляхом кореляції даних DLP і IDS.

Сигнатурний аналіз (IDS/IPS) забезпечує високу точність у виявленні відомих атак, наприклад SQL-ін’єкцій чи експлойтів SMB, проте не здатний реагувати на нові зразки загроз без оновлення сигнатур.

Аномалійний аналіз із використанням моделей машинного навчання дозволяє виявляти нетипові патерни поведінки, такі як раптове зростання вихідного трафіку чи зміна структури запитів.

Гібридні моделі, що комбінують сигнатурний та аномалійний підходи, створюють баланс між швидкістю реагування і адаптивністю до нових загроз. Такий багаторівневий конвеєр забезпечує низький рівень хибних спрацьовувань та здатність адаптуватися до еволюції загроз, що особливо важливо в середовищах із високими вимогами до DLP та NGFW [1, 2].

На основі цього аналізу запропоновано методику, яка корелює події DLP із виявленими IDS аномаліями.

Для практичного впровадження рекомендується:

- інтегрувати DLP та IDS у SIEM-платформу (Splunk, QRadar) для централізованої кореляції подій і автоматизації реагування;
- налаштувати автоматичне оновлення сигнатурних баз із перевірених джерел та періодично проводити аудит правил;
- забезпечити регулярне навчання аналітиків моделюванню інцидентів і користувачів – базовим принципам інформаційної безпеки, а також впроваджувати періодичне тестування та адаптацію моделей машинного навчання відповідно до появи нових типів загроз [3].

Запропонована методика є універсальною та може бути адаптована для різних галузей, що робить її перспективною для широкого впровадження у сучасних корпоративних інформаційних системах.

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційна та кібернетична безпека: підручник. Київ: ДУТ, 2018. 456 с.

2. Шерстюк В. І., Жуков С. О. Кібербезпека інформаційних систем: монографія. Київ: НАУ, 2020. 320 с.

Darktrace. AI-Powered Network Security [Електронний ресурс]. URL: https://www.darktrace.com/products/network

Використання ШІ для виявлення інформаційних операцій у медіапросторі

УДК04.8:316.774.3

Віталій Тищенко[1], Олександр Дьячук[2]

Державний університет інформаційно-комунікаційних технологій,

[1]v.tyshchenko@duikt.edu.ua, [2]realjewua@gmail.com

Інтеграція штучного інтелекту (ШІ) у виявлення інформаційних операцій у медіа-просторі стала критично важливою через зростання дезінформації та її соціальних наслідків. Дезінформація, навмисно оманливий контент для завдання шкоди, поширюється цифровими платформами, вимагаючи передових методів протидії. Технології ШІ, зокрема машинне навчання (ML) і обробка природної мови (NLP), автоматизують виявлення, але проблеми етики, алгоритмічної упередженості та зловживань залишаються.

Автоматизовані системи перевірки фактів використовують алгоритми ML для аналізу даних з перевірених джерел, застосовуючи семантичний аналіз і синтаксичне розпізнавання шаблонів. Інтеграція блокчейну забезпечує незмінні записи, покращуючи верифікацію в реальному часі [1]. Ефективність залежить від якісних наборів даних, що ускладнено динамікою тактик дезінформації та дефіцитом маркованих даних для маловивчених мов.