УДК 004.7
О. В. Смик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВНУТРІШНІХ ЗАГРОЗ

UDC 004.7
O. V. Smyk

METHODS AND MEANS OF PROTECTING THE INFORMATION AND COMMUNICATION SYSTEM OF AN INFORMATION ACTIVITY OBJECT FROM INTERNAL THREATS

Сучасні інформаційно-комунікаційні системи (ІКС) є основою функціонування організацій та підприємств, але водночас стають мішенню для внутрішніх загроз, які залишаються одними з найскладніших для ідентифікації. Залежність організацій від ІКС збільшує потенційні ризики, що пов'язані як із людським фактором, так і з технічними недоліками [1]. Внутрішні загрози можуть виникати через ненавмисні помилки співробітників, порушення правил роботи із системою, або навмисні дії, що мають на меті завдання шкоди.

Мета дослідження полягає у створенні системи, яка забезпечить виявлення внутрішніх загроз в ІКС за допомогою аналізу поведінки користувачів та класифікації їх дій із застосуванням методів машинного навчання.

За основу роботи системи захисту ІКС взято модель класифікації, що дозволяє аналізувати взаємозв'язки між різними параметрами поведінки користувачів. Для навчання та тестування моделі було обрано датасет Data Leakage Detection із відкритої платформи Kaggle [2]. Датасет містить інформацію про активність користувачів у комп'ютерній мережі або системі, охоплюючи такі показники, як методи автентифікації, рівень доступу до даних, операції з файлами, рівень чутливості даних та ознаки аномальної поведінки. Використання цього датасету обґрунтоване його відповідністю специфіці задачі та наявністю збалансованого розподілу класів для «нормальної» та «аномальної» активності.

Розроблена система включає функціонал моніторингу поведінки користувачів у реальному часі, що дозволяє виявляти аномалії у діях співробітників. Алгоритм класифікує дії як нормальні або аномальні, спираючись на заздалегідь визначені параметри, такі як частота доступу до конфіденційної інформації, час входу в систему, кількість запитів тощо.

Застосування розробленої системи дозволяє вчасно виявляти потенційні загрози, знижуючи ризики витоку інформації, а також фінансових і репутаційних збитків.

Важливою особливістю запропонованого підходу є використання машинного навчання для моніторингу поведінкових патернів та автоматичного аналізу аномалій. Це дозволяє адаптувати розроблену систему до потреб різних галузей, що підкреслює її практичну цінність у забезпеченні безпеки інформаційно-комунікаційних систем.

Література

1. Insider Threats: From Malicious to Unintentional. URL: https://www.sentinelone.com/blog/insider-threats-from-malicious-to-unintentional/?utm_source=chatgpt.com (дата звернення: 05.12.2024).
2. Data Leakage Detection. URL: https://www.kaggle.com/datasets/syedmarslanalvi /data-leakage-detection (дата звернення: 05.12.2024).