УДК 004.056.5

І. С. Гуцько

УДОСКОНАЛЕННЯ ЗАХИСТУ МОБІЛЬНИХ КОРПОРАТИВНИХ КОМУНІКАЦІЙ НА ОСНОВІ ГІБРИДНОЇ МОДЕЛІ BERT ТА ISOLATION FOREST

Вінницький національний технічний університет

Анотація

У даній статті розглянуто гібридний підхід до виявлення кіберзагроз у мобільних корпоративних комунікаціях на основі поєднання трансформерної моделі BERT для інтелектуального аналізу контенту та алгоритму Isolation Forest для виявлення поведінкових аномалій. Експериментальні результати показують, що запропонована модель демонструє вищу точність виявлення фішингу, спаму та аномальних активностей порівняно з традиційними методами машинного навчання.

Ключові слова: кібербезпека, мобільні комунікації, BERT, Isolation Forest, гібридна модель, виявлення аномалій, фішинг.

Abstract

This article explores a hybrid approach to detecting cyber threats in mobile corporate communications, based on combining the BERT transformer model for intelligent content analysis and the Isolation Forest algorithm for identifying behavioral anomalies. Experimental results indicate that the proposed model demonstrates higher accuracy in detecting phishing, spam, and anomalous activities compared to traditional machine learning methods.

Keywords: cybersecurity, mobile communications, BERT, Isolation Forest, hybrid model, anomaly detection, phishing.

Вступ

Сучасні корпоративні комунікації все частіше здійснюються через мобільні пристрої, що значно підвищує ризики кіберзагроз, таких як фішинг, спам та поведінкові аномалії. Традиційні системи захисту, засновані на сигнатурному аналізі або простих фільтрах, часто не забезпечують достатньої ефективності через динамічний характер загроз та складність аналізу текстових і поведінкових даних [1]. Зростання обсягів даних та витонченість атак вимагають застосування інтелектуальних методів, здатних адаптуватися до нових загроз у реальному часі.

Існуючі підходи, засновані на окремих методах машинного навчання, не завжди здатні одночасно враховувати семантику контенту та відхилення у поведінці користувачів [2]. Наприклад, моделі, орієнтовані виключно на обробку природної мови (NLP), можуть ефективно виявляти фішинг за змістом, але часто ігнорують аномальні шаблони активності. І навпаки, алгоритми виявлення аномалій можуть фіксувати незвичайну поведінку, але не розрізняти шкідливий контент у легальних за формою повідомленнях. Це обмеження зумовлює необхідність поєднання різнотипних методів у єдиній архітектурі. Однак інтеграція таких різнорідних підходів у практичну систему залишається складною задачею через розбіжності у форматах даних, вимогах до обчислювальних ресурсів та семантиці їх вихідних показників.

Метою роботи є розробка гібридної моделі захисту мобільних корпоративних комунікацій на основі поєднання передових методів обробки природної мови (з використанням трансформерної моделі BERT) та виявлення аномалій (з використанням алгоритму Isolation Forest) для досягнення комплексного підвищення точності та ефективності виявлення кіберзагроз. Запропонований підхід покликаний подолати обмеження існуючих рішень шляхом одночасного аналізу семантичного змісту повідомлень та виявлення відхилень у поведінкових паттернах користувачів.

Успішна реалізація такої гібридної архітектури дозволить створити більш надійну, адаптивну систему, здатну виявляти як контекстуально складні, так і поведінково атипові атаки, що особливо критично для захисту мобільних каналів з їх розширеною поверхнею атаки.

Результати дослідження

Запропоновано архітектуру гібридної моделі, яка включає два взаємодоповнюючі модулі, що працюють у синергії:

1. Модуль контент-аналізу на основі легковагової трансформерної моделі MobileBERT [2]. Ця модель, оптимізована для роботи на пристроях з обмеженими ресурсами, відповідає за глибинний семантичний аналіз текстових повідомлень у реальному часі. Вона визначає контекст, наміри та потенційно шкідливі ознаки у вмісті (наприклад, ознаки фішингових запитів, спамових конструкцій).
2. Модуль виявлення аномалій на основі алгоритму Isolation Forest [3]. Цей алгоритм, що належить до родини методів виявлення аномалій без навчання, працює за принципом ізоляції об'єктів у просторі ознак. Його ключова перевага – ефективна робота з багатовимірними даними та здатність виявляти рідкісні події без попереднього маркування "нормальної" поведінки. Модуль аналізує поведінкові та мета-ознаки комунікацій: частоту надсилання повідомлень, час активності, розміри даних, геолокаційні метадані та інші параметри [3].

Синергія між цими модулями полягає у їх здатності покривати різні аспекти кіберзагрози, які поодинці можуть залишатися непоміченими. MobileBERT ефективно виявляє загрози, що мають явні текстові ознаки, тоді як Isolation Forest спрацьовує на незвичайні поведінкові шаблони, навіть якщо текст формально бездоганний. Ця двостороння перевірка значно підвищує надійність системи. Наприклад, складний цільовий фішинг (spear phishing) може мати грамотно складений текст, який обійде контент-фільтр, але надсилатиметься з незвичного місця або в нестандартний час, що буде виявлено аномалійним модулем. І навпаки, спам із явними ознаками може розсилатися з імітованих, але статистично «нормальних» джерел.

Архітектура організована таким чином, що рішення кожного модулю інтегруються на фінальному етапі за допомогою механізму зваженої або мета-класифікації, що дозволяє отримати єдину оцінку ризику. Для цього виходи обох моделей (наприклад, ймовірність шкідливості від MobileBERT та бал аномальності від Isolation Forest) агрегуються за допомогою додаткового класифікатора (логістична регресія або градієнтний бустинг) або ж правил, навчених на валідаційних даних. Такий підхід дозволяє моделі адаптуватися до різноманітних сценаріїв атак, поєднуючи сили глибинного розуміння мови та статистичного аналізу поведінки. Крім того, модульна структура дає можливість незалежного оновлення або заміни будь-якого з компонентів, що підвищує гнучкість та довготривалу життєздатність системи в умовах швидкої еволюції кіберзагроз.

Для навчання та перевірки моделі було сформовано комбінований набір даних. Він включав: а) публічні корпуси фішинг- та спам-повідомлень (зокрема, адаптовані вибірки з набору Enron); б) синтетично згенеровані аномальні поведінкові паттерни, що імітують нестандартну активність. Такий підхід дозволив одночасно навчати модель розпізнавати шкідливий контент і незвичайну поведінку. Для комплексної оцінки якості роботи системи використовувались стандартні метрики: точність (precision), повнота (recall) та F1-міра, що є гармонійним середнім двох попередніх показників. Ця комбінована метрика особливо важлива в задачах виявлення кіберзагроз, де необхідно знаходити баланс між виявленням максимальної кількості атак і мінімізацією помилкових сповіщень, які знижують довіру до системи. Високий показник F1-міри прямо вказує на практичну придатність моделі для впровадження в реальні умови. У ході експериментів кожна модель проходила оцінку на ідентичних тестових даних, що забезпечило чисте та об'єктивне порівняння їх здібностей.

Експериментальні результати показали, що запропонована гібридна модель досягає значень F1-міри на рівні 0,94. Цей результат є суттєво вищим порівняно з підходами, що використовують окремі компоненти: вона перевершує модель лише на основі BERT (F1 ≈ 0,84) приблизно на 12% та модель лише на основі Isolation Forest (F1 ≈ 0,82) на 15%. Крім того, гібридна модель показала стабільно кращі результати на 8–15% у порівнянні з класичними алгоритмами машинного навчання, такими як Support Vector Machine (SVM, F1 ≈ 0,86) та Random Forest (F1 ≈ 0,82), які застосовувались до того ж комбінованого набору ознак. Отримані показники підтверджують гіпотезу про те, що інтеграція глибинного семантичного аналізу з методами виявлення статистичних відхилень дозволяє

створити більш надійну систему захисту, здатної протистояти різнотипним кіберзагрозам. На рис. 1 представлено наочне порівняння ефективності усіх досліджуваних моделей за ключовою метрикою F1.

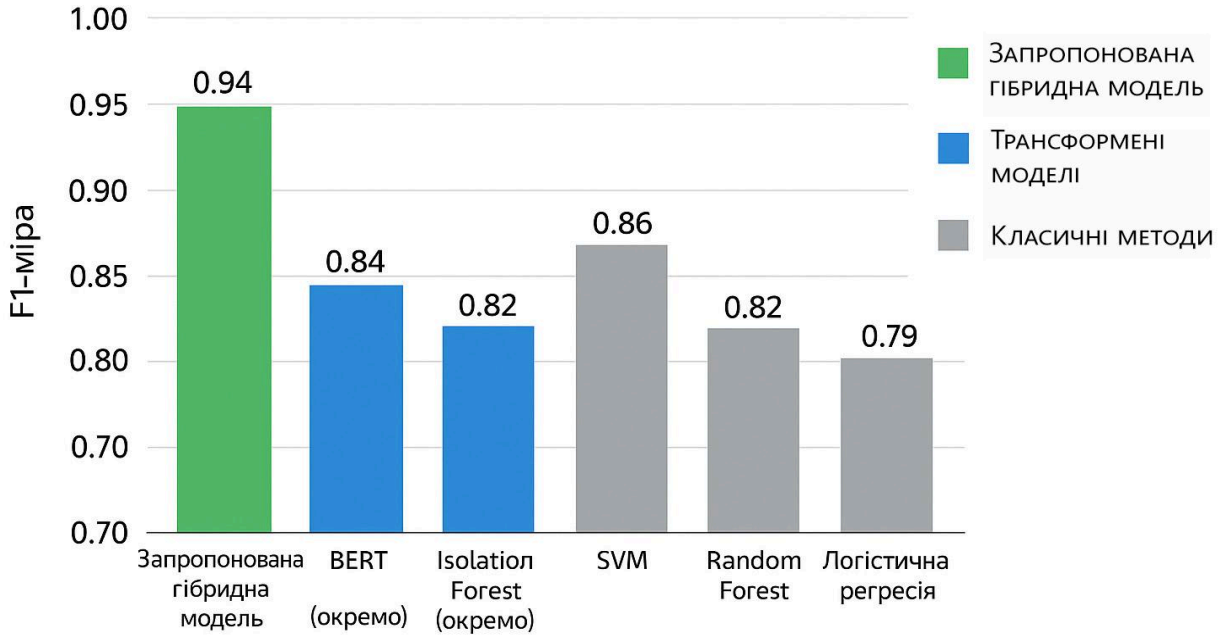

Рис. 1. Порівняння F1-міри запропонованої гібридної моделі з базовими підходами

Отримані результати демонструють, що інтеграція модуля контент-аналізу на основі BERT з модулем виявлення аномалій на базі Isolation Forest створює синергетичний ефект. Модель BERT забезпечує глибоке розуміння семантичного змісту повідомлень, ефективно ідентифікуючи маніпулятивні техніки фішингу та контекстно-залежні загрози [2]. Водночас алгоритм Isolation Forest [3] виявляє статистично відхилені поведінкові паттерни, які можуть не мати явних текстових ознак шкідливості, але свідчать про потенційну компрометацію системи, наприклад, незвичайну частоту повідомлень або активність у неслужбовий час.

Така двостороння перевірка дозволяє системі ухвалювати більш обґрунтовані рішення та знижувати частоту помилок обох типів: хибнопозитивних (коли безпечна активність визнається загрозою) та хибнонегативних (коли реальна загроза залишається непоміченою). Це особливо критично в корпоративному середовищі, де баланс між безпекою та безперебійністю бізнес-процесів є ключовим. Ефективність запропонованого підходу підтверджується його перевагою над окремими методами та класичними алгоритмами, що робить його перспективним для впровадження в сучасних системах корпоративної мобільної безпеки. Модель демонструє не лише високу точність, а й здатність адаптуватися до нових, невідомих загроз завдяки комбінації превентивного та реактивного аналізу. Подальші дослідження можуть бути спрямовані на оптимізацію продуктивності моделі для роботи в умовах обмежених обчислювальних ресурсів та розширення спектру аналізованих типів загроз.

Висновки

1. Запропоновано гібридну модель захисту мобільних корпоративних комунікацій, що поєднує BERT для контент-аналізу та Isolation Forest для виявлення поведінкових аномалій.
2. Експериментально доведено, що модель забезпечує вищу точність виявлення загроз порівняно з окремими методами машинного навчання.
3. Модель є масштабованою та придатною для впровадження в реальних корпоративних системах безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Васильєв О. М. Сучасні загрозы кібербезпеки в мобільних мережах / О. М. Васильєв // Вісник кібербезпеки. – 2023. – № 4. – С. 45–52.
2. Devlin J. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding / J. Devlin, M.-W. Chang // Proceedings of NAACL-HLT. – 2019. – P. 4171–4186.
3. Liu F. T. Isolation Forest / F. T. Liu, K. M. Ting // Proceedings of the 2008 Eighth IEEE International Conference on Data Mining. – 2008. – P. 413–422.

Ігор Сергійович Гуцько — студент групи 1КІТС24м, факультет менеджменту та інформаційної безпеки, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: egucko970@gmail.com;
Науковий керівник: ***Юрій Євгенович Яремчук*** — д-р техн. наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Ihor S. Huts'ko — student of group 1KITS24m, Faculty of Management and Information Security, Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, e-mail: egucko970@gmail.com;
Supervisor: ***Yurii Y. Yaremchuk*** — Dr. Sc. (Eng.), Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia. e-mail: @yurevyar