Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах

УДК 004.853 (043.2)

Олена Негоденко[1], Віталій Негоденко[2]

Державний університет інформаційно-комунікаційних технологій,
[1]negodenkoav@gmail.com, Київський столичний університет імені Б. Грінченка
[2]v.nehodenko.asp@kubg.edu.ua

Протягом останніх десятиліть велика увага приділяється методам Data Science для вирішення проблем безпеки. Так, для виявлення вторгнень та шкідливих програм, фішинг і атаки на відмову в обслуговуванні використовують методи машинного навчання, статистичного навчання, інтелектуального аналізу даних і обробки природної мови. Крім того, кібербезпека також стає серйозною проблемою для організацій, частково через руйнівне поширення інцидентів у кібератаках, таких як витоки даних у Equifax, Verizon, Gmail та Instagram.

Інші загрози кібербезпеки, які викликають серйозне занепокоєння, включають перевантаження даних, фальшиві сповіщення, невідомі дані, обмежені ресурси та труднощі з інтеграцією та оркестровкою. Крім того, зловмисники постійно адаптуються до методів виявлення та активно прагнуть використовувати нові вразливості. Зважаючи на складність і динамічний характер кіберзагроз, автоматизація аналітики на основі даних, а саме підтримка прийняття рішень щодо прогнозування кібератак в інформаційних системах набуває важливого значення для дослідження [1].

В першу чергу кібербезпека має справу з різними типами кіберзлочинів, але важливо визначити подібність існуючих кіберзлочинів за допомогою інтелектуального аналізу даних і технологій машинного навчання. Алгоритми машинного навчання можуть допомогти навчити систему виявляти аномалії, конкретні шаблони для прогнозування кібератак. Інтелектуальний аналіз даних відіграє вирішальну роль у забезпеченні прогностичного рішення для виправлення можливих кіберзлочинів і методів дії та дослідження системи захисту від них. Методи Data Science дозволяють системі аналізувати приховані знання та навчати експертну систему сповіщенню та процесу прийняття рішень [2].

Загальний підхід для прогнозування та ефективного виявлення аномалій та кібератак в реальному часі включає комплексну систему на основі штучного інтелекту та аналітики даних.

Першим кроком є вибір відповідних моделей машинного навчання для використання в системі виявлення аномалій та передбачення кібератак. Серед яких виділяють класичні моделі, такі як метод опорних векторів (SVM), навчання з учителем (нейронні мережі), навчання без учителя (методи кластеризації), або нові моделі, які використовують глибинне навчання (Deep Autoencoder Network та інші.)

Після вибору моделей необхідно оптимізувати їх параметри для максимізації точності передбачення та мінімізації помилок. А саме налаштування гіперпараметрів моделей, таких як розмір шарів нейронної мережі, швидкість навчання (learning rate), коефіцієнти регуляризації та інші. Даний процес також включає використання методів перехресної перевірки (cross-validation) та оптимізації на основі результатів та вибір оптимальних функцій втрат.

Для ще кращої ефективності використовують ансамблеві моделі, які комбінують кілька моделей машинного навчання для зниження помилок та підвищення стійкості передбачення Рис.1.

Ансамблеві моделі	**Bagging (Bootstrap Aggregating)**
	Random Forest
	Boosting
	Stacking (Stacked Generalization)
	Градієнтний бустинг (Gradient Boosting)

Рис.1 Ансамблеві моделі машинного навчання для зниження помилок та підвищення стійкості прогнозування

Багато даних у сфері кібербезпеки можуть бути незбалансованими, з великою кількістю зразків нормальної поведінки та обмеженою кількістю зразків аномальної поведінки. Для ефективного використання моделей машинного навчання необхідно враховувати незбалансування та використовувати відповідні техніки обробки даних (Undersampling, Oversampling, SMOTE, Weighting, ансамблі методи та використання F1-метрик та матриці помилок).

Після розробки моделей важливо провести оцінку їх ефективності та якості прогнозування, що реалізується через розрахунок метрик якості, таких як точність, чутливість, специфічність, F1-оцінка, а також перехресна перевірка стійкості моделей та уникнення перенавчання [3].

Оскільки кіберзагрози постійно еволюціонують, тому важливо надавати системі можливість навчатися на нових даних та вдосконалювати моделі з часом. Тому важливо включати автоматизований процес оновлення моделей на основі нової інформації про загрози.

1. Abomhara M, Geir M. Køien. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mob.– 2015 – V. 4(1). – P. 65 – 88.
2. Chayal, N.M., Patel, N.P. Review of Machine Learning and Data Mining Methods to Predict Different Cyberattacks. Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, 2021. 305 p.
3. J. Song, H. Takakura, Y. Okabe and K. Nakao, “Toward a more practical unsupervised anomaly detection system”, Information Sciences, vol. 231, (2013), p. 4-14.