МЕХАНІЗМИ ПЕРВИННОЇ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ ПІДХОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Балагура В.О., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкого зростання кількості кіберзагроз інформаційна безпека стає критично важливою складовою діяльності будь-якої організації [1, 2]. Однією з актуальних задач є оперативна первинна оцінка рівня захищеності інформаційних систем, яка дозволяє виявити потенційні вразливості без проведення повномасштабного аудиту. Така оцінка є особливо важливою для організацій, що не мають достатніх ресурсів для регулярного проведення комплексних перевірок. Традиційні підходи до оцінки безпеки часто потребують значних часових і ресурсних витрат, залучення експертів та використання спеціалізованих інструментів, тому актуальним є розроблення механізмів та інструментів, що забезпечують оперативне визначення стану інформаційної безпеки.

Метою доповіді є опрацювання концепції та механізмів застосування штучного інтелекту для проведення первинної оцінки рівня інформаційної безпеки організації.

Запропонований підхід базується на використанні структурованих опитувальників з фіксованими питаннями, що охоплюють ключові домени інформаційної безпеки:

управління доступом,
резервне копіювання,
моніторинг,
політики безпеки,
навчання персоналу, реагування на інциденти,
фізичний захист [1].

Кожен із зазначених доменів відображає окремий аспект системи захисту та дозволяє комплексно оцінити стан безпеки організації. Формування опитувальника передбачає уніфікацію питань та їх прив'язку до загальноприйнятих стандартів інформаційної безпеки, що забезпечує узгодженість та відтворюваність результатів оцінювання.

На відміну від бінарних оцінок, використовується градуйована шкала рівня впровадження контролів, що дозволяє більш точно відобразити реальний стан безпеки. Такий підхід дає змогу зменшити втрату інформації при оцінюванні та підвищити чутливість моделі до незначних відхилень у рівні захищеності. Подальша нормалізація отриманих оцінок створює основу для їх застосування у математичних моделях аналізу, забезпечуючи коректність обчислень та порівнюваність результатів між різними організаціями або підрозділами. Зокрема, для формування інтегрального показника захищеності доцільно використовувати моделі логістичної регресії [3], які добре зарекомендували себе для задач класифікації та оцінювання ризиків.

Модель логістичної регресії виконує функцію простої нейромережі з одним нейроном і дозволяє на основі множини вхідних параметрів (відповідей користувача) обчислювати інтегральний показник рівня захищеності у відсотках. Крім того, така модель дозволяє у майбутньому враховувати вагові коефіцієнти окремих ознак, що відображають їх відносну важливість для загального рівня безпеки. Це створює можливість подальшої адаптації моделі до специфіки різних організацій шляхом коригування вагових параметрів.

Запропонований підхід дає можливість оцінити рівень ризику виявлених проблем з урахуванням їх критичності, впливу та належності до певного домену безпеки [4]. Додатково може враховуватися взаємозв'язок між окремими контролами, що дозволяє більш точно оцінити сукупний ефект їх відсутності або часткової реалізації. Це дозволяє не лише отримати загальний рівень захищеності, але й ідентифікувати найбільш вразливі області, які потребують першочергового втручання. Таким чином, результати оцінювання можуть бути використані для пріоритезації заходів з підвищення безпеки.

Результатом застосування запропонованого підходу є формування аналітичного звіту, який включає інтегральний показник безпеки, оцінку за окремими доменами, виявлені слабкі місця та рекомендації щодо їх усунення [1]. Додатково звіт може містити візуалізацію результатів у вигляді графіків або діаграм, що полегшує їх інтерпретацію для керівництва організації. Такий підхід дозволяє суттєво підвищити ефективність первинної оцінки, забезпечити прозорість процесу прийняття рішень та зменшити навантаження на фахівців з кібербезпеки за рахунок автоматизації аналізу.

Таким чином, використання методів штучного інтелекту для первинної оцінки інформаційної безпеки не замінює спеціаліста, а доповнює його діяльність і є перспективним напрямом розвитку сучасних систем безпеки [5]. Воно дозволяє забезпечити швидке отримання узагальненої картини стану захищеності та своєчасно реагувати на потенційні загрози. Подальші дослідження можуть бути спрямовані на вдосконалення моделей, використання реальних даних аудиту, інтеграцію з системами моніторингу безпеки, а також розширення функціональних можливостей таких систем за рахунок застосування більш складних моделей машинного навчання.

Список літератури

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022.
2. Голубничий, Д. Ю., Сєвєрінов, О. В., Коломійцев, О. В., Місюра, О. М., Третяк, В. Ф., Власов, А. В., & Крук, Б. М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.
3. Goodfellow I. Deep Learning. MIT Press, 2016.
4. NIST Cybersecurity Framework (CSF) 2.0: Cybersecurity Framework. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
5. Bishop C. Pattern Recognition and Machine Learning. Springer, 2006.