НАПРЯМ КОНФЕРЕНЦІЇ. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА ГІГІЄНА

DOI: https://doi.org/10.54929/conf_28_10_2024-10-01

Костюк Ю. В.
PhD,
Київський столичний університет імені Бориса Грінченка,
м. Київ, Україна
ORCID: 0000-0001-5423-0985

Рзаєва С. Л.
к.т.н, доцент,
Київський столичний університет імені Бориса Грінченка,
м. Київ, Україна
ORCID: 0000-0002-7589-2045

СТРАТЕГІЧНІ РІШЕННЯ SOC ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ КІБЕРЗАГРОЗ

У сучасних умовах розвитку інформаційних технологій і зростання кількості кіберзагроз Центр операцій безпеки (SOC) стає критично важливим інструментом для забезпечення безпеки інформаційної інфраструктури організацій. SOC виконує функцію не лише реагування на кіберінциденти, а й активної профілактики, аналізу та моніторингу кіберризиків, інтегруючи сучасні технології штучного інтелекту (ШІ) та нейронних мереж для підвищення ефективності своєї роботи. Використання цих інноваційних технологій дозволяє SOC адаптуватися до умов зростаючої складності атак і забезпечувати проактивний підхід до управління кібербезпекою [1-2].

Однією з ключових сфер застосування ШІ та нейронних мереж у роботі SOC є автоматизація процесів виявлення та класифікації загроз. Завдяки алгоритмам машинного навчання, зокрема глибокого навчання, SOC має змогу аналізувати великі обсяги даних у режимі реального часу, швидко виявляючи аномальні поведінкові патерни в мережевому трафіку, які можуть свідчити про потенційні атаки. Наприклад, нейронні мережі використовуються для аналізу базових характеристик кіберзагроз, таких як поведінка IP-адреси або аномальне використання облікових даних, дозволяючи виділяти навіть незначні відхилення від нормальної діяльності, які можуть бути першими індикаторами вторгнень [2, 5]. При цьому застосування методів глибокого навчання є особливо актуальним у випадках динамічного середовища, де кіберзагрози швидко змінюються, і традиційні методи аналізу недостатньо ефективні для їх оперативного виявлення. Крім того, використання алгоритмів ШІ дозволяє SOC будувати прогнозні моделі для оцінки ризиків на основі

історичних даних. Наприклад, за допомогою регресійного аналізу або моделей кластеризації, ШІ може надавати прогнози стосовно ймовірних сценаріїв розвитку кіберінцидентів та їхніх можливих наслідків [3-4]. Це дає змогу SOC завчасно планувати необхідні заходи захисту, коригувати існуючі стратегії та більш ефективно управляти ризиками. Прогнозна аналітика у цьому контексті сприяє зменшенню кількості хибних спрацювань, що є важливим чинником у випадках великих і складних інформаційних систем.

Впровадження технологій ШІ у діяльність SOC також дозволяє досягти значного прогресу у питаннях автоматизованого реагування на інциденти. Системи, що використовують нейронні мережі, можуть не лише виявляти загрози, але й надавати пропозиції або автоматично виконувати певні дії для запобігання поширенню загрози. Зокрема, на основі обробки попередньо визначених сценаріїв та поведінкових патернів нейронні мережі можуть автоматично блокувати підозрілі IP-адреси, змінювати налаштування фаєрволів або обмежувати доступ до вразливих сервісів до моменту повної перевірки активності. Це суттєво скорочує час на реагування та мінімізує ризики, пов'язані з можливою затримкою в ручній обробці інцидентів [2-5].

Ще однією важливою функцією штучного інтелекту (ШІ) є покращення аналітичних можливостей Центру операцій безпеки (SOC) шляхом використання методів обробки природної мови (NLP). Ці методи дозволяють автоматично аналізувати текстову інформацію, що стосується нових кіберзагроз, інцидентів і вразливостей, отриманих з відкритих джерел, новинних статей, наукових публікацій або спеціалізованих баз даних. Завдяки цьому SOC може постійно отримувати актуальні дані про потенційні загрози та швидко адаптувати свою систему безпеки відповідно до нових викликів. NLP-алгоритми здатні обробляти великі обсяги текстової інформації, що може містити важливі сигнали про загрози, такі як нові вразливості програмного забезпечення або методи атаки, які активно використовуються зловмисниками. Наприклад, аналізуючи публікації на форумах, блогах або соціальних мережах, SOC може виявити ранні ознаки нових загроз, які ще не зафіксовані в традиційних джерелах інформації. Це дозволяє аналітикам SOC отримувати своєчасні сповіщення про нові методи атак і тенденції в діяльності кіберзлочинців. Крім того, NLP допомагає системам SOC інтегрувати виявлені загрози в загальну модель захисту, що суттєво підвищує проактивність системи. Використання таких алгоритмів дозволяє SOC створювати контекстуалізовані описи загроз, що сприяє формуванню більш глибокого розуміння ситуації. Це, у свою чергу, полегшує прийняття рішень про відповідні заходи реагування. Наприклад, якщо текстовий аналіз виявляє підвищену активність зловмисників, що обговорюють нові методи експлуатації певної вразливості, SOC може негайно ініціювати перевірку системи на наявність відповідних загроз. Також варто зазначити, що NLP дозволяє SOC автоматизувати деякі рутинні завдання, пов'язані з моніторингом і аналізом інформації. Це звільняє час аналітиків для більш складних і

стратегічних завдань, таких як розробка та реалізація нових протоколів реагування на інциденти. Важливим аспектом є те, що застосування методів обробки природної мови дозволяє SOC не лише реагувати на вже виявлені загрози, але й прогнозувати нові, аналізуючи зміни в поведінці зловмисників. Залучення ШІ та NLP у процеси SOC забезпечує більш гнучкий і адаптивний підхід до кібербезпеки, що, в свою чергу, сприяє покращенню загального рівня захисту організації. У результаті, SOC стає не лише центром реагування на інциденти, а й стратегічним партнером у забезпеченні безпеки інформаційних систем, здатним швидко реагувати на нові виклики в динамічному світі кіберзагроз [4].

Багаторівневий захист інформаційної інфраструктури є основною стратегією забезпечення комплексної інформаційної безпеки, яка враховує не лише зовнішні, а й внутрішні загрози. Для цього використовуються декілька рівнів захисту, включаючи мережеві фаєрволи, системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), а також засоби для забезпечення безпеки кінцевих точок. Така архітектура дозволяє протистояти як загрозам із зовнішнього середовища, так і потенційно небезпечним діям зсередини організації, що значно підвищує загальну стійкість системи до кібератак.

Аналітика загроз та управління ризиками в режимі реального часу є невіддільним компонентом діяльності сучасного Центру операцій безпеки (SOC), особливо в умовах постійно змінюваного ландшафту кіберзагроз. У зв'язку зі зростаючою складністю атак, адаптація SOC до нових викликів стає критично важливою. Аналітичні модулі SOC, що працюють у режимі реального часу, здатні швидко обробляти величезні обсяги даних про поточний стан мережі, виявляти аномалії та потенційно шкідливі патерни в мережевому трафіку. Завдяки інструментам для обробки даних та аналітики SOC може зібрати та проаналізувати інформацію з різних джерел, таких як системи виявлення вторгнень (IDS), системи моніторингу трафіку, журнали доступу та інші елементи інформаційної інфраструктури. Використання штучного інтелекту (ШІ) та нейронних мереж дозволяє SOC розробляти індивідуальні моделі для ідентифікації та оцінки ризиків. Завдяки алгоритмам машинного навчання ці моделі можуть навчатися на історичних даних, що дозволяє їм виявляти закономірності, які можуть залишатися непоміченими для людських аналітиків. Таке навчання може включати в себе аналіз попередніх інцидентів, виявлення схожих тактик, технік і процедур (TTP), які використовують зловмисники, а також адаптацію до нових загроз. За допомогою цих моделей SOC не лише виявляє загрози, але й розраховує ймовірність розвитку інциденту. Це дає змогу оперативно приймати обґрунтовані рішення щодо реагування, які враховують не лише поточну ситуацію, але й прогнози щодо можливих сценаріїв розвитку подій. Технології аналітики в режимі реального часу також сприяють інтеграції різних систем безпеки, що дозволяє створювати комплексні рішення для захисту інформаційної інфраструктури. Завдяки таким інтеграціям SOC може отримувати та обробляти інформацію з різних джерел, що підвищує загальну ефективність системи реагування на інцидент [1, 3, 5].

Таким чином, впровадження штучного інтелекту та нейронних мереж у SOC трансформує підходи до забезпечення інформаційної безпеки, дозволяючи досягати високого рівня адаптивності, оперативності та точності в управлінні кіберзагрозами. Завдяки автоматизації та розширенню аналітичних можливостей SOC має змогу забезпечувати надійний захист інформаційних ресурсів навіть у випадках швидкої еволюції кіберзагроз, що є критичним у контексті сучасної інформаційної безпеки [4].

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Dhanasekaran, R., & Sivasubramanian, S. (2020). Cybersecurity and Artificial Intelligence: A Comprehensive Review. *Journal of Computer Networks and Communications*, 2020, 1-10. https://doi.org/10.1155/2020/8852462

2. Kaur, G., & Singh, M. (2021). Artificial Intelligence in Cybersecurity: A Review. *International Journal of Computer Applications*, 975, 1-5. https://doi.org/10.5120/ijca2021921174

3. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(25), 229–252.

4. Wang, S., Liu, C., & Wang, Y. (2019). Deep Learning for Cyber Security: A Review. *Journal of Network and Computer Applications*, 129, 74-91. https://doi.org/10.1016/j.jnca.2019.02.002

5. Kryvoruchko O., Kostiuk Y., Desiatko A. (2024) Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods// *Ukrainian Scientific Journal of Information Security*, vol. 30, issue 1, pp. 140-149.