Секція освіти

ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Постіл С. Д.[1], *Любушкін Д. В.*[2]
[1]*Державний податковий університет,*
Київська обл., м. Ірпінь, вул. Університетська, 31
[2]*Компанія RISA Tehnologies* (*USA*)

Зростаюча кількість і складність кіберзагроз вимагають новаторських підходів до захисту кіберпростору. Інциденти кібербезпеки, такі як крадіжка даних, атаки на критичну інфраструктуру та кібертероризм, можуть мати серйозні наслідки для економічної стабільності та національної безпеки.

Одним з найперспективніших напрямків у кібербезпеці, безумовно, є застосування штучного інтелекту (ШІ). В ІТ є ціла низка напрямків, у яких ШІ вже давно ефективно використовується:

1. Системи розпізнавання осіб, що дозволяють ідентифікувати людей за цифровими зображеннями, розпізнаючи риси обличчя. Власне, системи ідентифікації теж є частиною систем безпеки і певною мірою підходять під тематику кібербезпеки.

2. Виявлення фейкових новин. Детектори фейків використовують семантичні та стилістичні особливості тексту у статті, щоб відрізняти фейкові новини від достовірних.

3. Управління ІТ-активами, які включають у себе робочі станції, комутатори, маршрутизатори і т. д..

4. Рекомендаційні системи, що використовуються на різних ресурсах, здатні оцінити вибір клієнта на основі таких факторів як особиста історія, попередній вибір, зроблений клієнтом.

5. Чат бот системи, які покращують якість обслуговування клієнтів, надаючи автоматичні відповіді, коли співробітники служби підтримки клієнтів не можуть відповісти. Проте їхня діяльність не обмежується лише роботою віртуального асистента. Вони мають можливості аналізу настроїв і також можуть давати рекомендації.

Використання ШІ та автоматизованих інструментів для виявлення, оцінки та усунення вразливості потребує актуальних регла-

ментних документів для оцінки стану кібербезпеки відповідних обєктів кіберпростору. Прикладом виступає розроблена і затверджена методика оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж [1].

Загалом ШІ використовується в ІТ досить ефективно [2] і актуальною проблемою виступають концепції, методології і технології застосування ШІ для вирішення різних задач кібербезпеки.

Антивірусні рішення традиційно використовували і, власне, продовжують використовувати сигнатурний аналіз [3].

Цей метод полягає у виявленні характерних ідентифікуючих властивостей кожного вірусу та пошуку вірусів при порівнянні файлів із виявленими властивостями [4].

Провідні компанії, які спеціалізуються на розробці антивірусів дають таке визначення сигнатури: безперервна послідовність байтів [3], характерна для тієї чи іншої шкідливої програми. Припустимо, що ми маємо деякий потенційно шкідливий набір байт, які є опкодами (частини машинної мови) інструкцій асемблера. На асемблері той самий алгоритм можна реалізувати багатьма варіантами. На мовах високого рівня загалом теж, але компілятор або інтерпретатор у результаті може все оптимізувати так, що відмінності будуть не настільки суттєвими. Але й не забуваємо про різні обфускатори (перешкоди для вивчення програми з метою виявлення функціональності), які можуть змінити код шкідливості до невпізнанності [5]. Таким чином, класичний сигнатурний аналіз не дуже допоможе, використання ШІ дозволить ефективно вирішити дану проблему.

Ефективним інструментом виявлення шкідливих програм звичайно є пісочниця, але для розгортання пісочниці потрібні певні програмні та апаратні ресурси, але критичним фактором виступає час на виявлення шкідливої активності. Використання ШІ може суттєво скоротити цей час.

Традиційним засобом збору та аналізу подій інформаційної безпеки на відповідність певним правилам кореляції є рішення класу SIEM (Security Information Event Management) [6]. Справа в тому, що аналіз великого обсягу подій (десятки тисяч подій в секунду) є завдання досить ресурсоємним і використання класичних правил кореляції, може вимагати великих потужностей. Крім того, звичайні правила мають бінарну логіку. Набір подій або підпадає, або не підпадає під певні умови і якщо не підпадає, алерт (сигнальне повідомлення) не буде створено. ШІ дозволяє зробити логіку інтелектуальнішою і тим самим провести виявлення підозрілої активності ефективнішими.

Аналіз коду різними методами дозволяє виявити різні види шкідливих додатків, як відомих, так і невідомих, але які ведуть себе підозріло. Однак, крім безпосередньо вірусів, троянів та інших бекдорів, ми можемо також зіткнутися з різними інструментами хакерів, експлоїтами для вразливостей нульового дня і спробами використання легального системного програмного забезпечення (ПЗ) для різних хакерських активностей [7].

Далеко не всі подібні дії можуть виявлятися антивірусом, тому що в цьому випадку потрібно аналізувати вже не просто сигнатури коду, а саме поведінку користувача та додатків у системі: хто, коли і з якою метою запускає ті чи інші процеси [7].

Для виявлення підозрілих активностей системи EDR (Endpoint Detection & Response) на вузлах користувача розміщують агентів, які збирають необхідну інформацію про процеси, що запускаються, зміни в системі, нові налаштування і т. д. Однак тут проблема аналогічна правилам кореляції в SIEM: надто складно описати усі можливі підозрілі активності за допомогою правил. ШІ дозволяє на основі даних про легальну та підозрілу поведінку, отриману від агентів, виявляти потенційні шкідливі активності. Зокрема, ми можемо виявити компрометацію легальної програми, зараженої будь-яким шкідливим ПЗ або підозрілі дії різноманітних скриптів, які отримали команду на виконання легальним користувачем. Також до аналізу поведінки та шкідливого коду можна віднести аналіз мережевого трафіку та виявлення підозрілих пакетів (функціонал IDS – Intrusion Detection System). Тут ШІ може допомогти з виявленням різних атак у трафіку як на нижніх рівнях ієрархічної моделі, так і на рівні додатків.

Системи виявлення шахрайства (antifraud) це ще один важливий напрям кібербезпеки, який активно використовується в банківській та фінансових сферах [8]. Ці системи використовуються для зниження ризиків та забезпечення безпеки шахрайства відповідно до інтересів клієнтів та фінансових організацій. Такі системи виявляють відхилення у транзакціях та виставляють бали, вимірюючи коефіцієнти відхилення. Однак у класичних скорингових моделях є великий відсоток хибних спрацьовувань. Наприклад, системі може здатися шахрайським серія з кількох переказів від юридичної особи декільком фізичним. ШІ тут може ефективно аналізувати потік транзакцій, виявляючи потенційно підозрілі.

Однак не варто вважати ШІ «срібною кулею». Машинне навчання теж має свої недоліки. Так, генеровані SIEM оповіщення повинні перевірятися фахівцями-аналітиками SOC – Security Operations Center (Операційний центр безпеки), створення занадто великої кіль-

кості хибних попереджень може призвести до надмірного завантаження спеціалістів SOC. Взагалі велика кількість спрацьовувань говорить про те, що система безпеки в цілому працює не надто добре.

Якщо ці інциденти не є хибними спрацьовуваннями, це означає, що присутні проблеми в системах захисту. Так, наприклад, велика кількість інцидентів, пов'язаних з вірусними епідеміями говорить про те, що антивірусні політики налаштовані недостатньо добре, а велика кількість хибних спрацьовувань свідчить про те, що у нас некоректно працюють правила, які визначають підозрілу активність.

Аналогічно і у разі використання ШІ. Якщо нейромережа навчена на поганих даних, то результат вона видаватиме не надто правильний. У прикладі з SIEM, щоб запобігти проблемі помилкових спрацьовувань, аналітичні системи також отримують аналітичну інформацію із SIEM. Сигнали, що надходять із систем SIEM, порівнюються з інформацією в аналітичних системах, щоб система не генерувала сигнали, що повторюються. Таким чином, рішення для машинного навчання в галузі продуктів кібербезпеки отримують напрацювання з оточення, щоб звести помилкові спрацьовування до мінімуму.

Висновки. На сьогодні рішення, що використовують ШІ активно застосовуються в кібербезпеці для виявлення загроз, оцінки, автоматизації завдань, прогнозування майбутніх атак і захисту. При цьому ШІ особливо добре справляється зі збиранням та аналізом величезних обсягів даних, вилученням цінної інформації та відповідним реагуванням. Ці можливості значно підвищують здатність організації виявляти кібератаки і реагувати на них і, зрештою, мінімізують потенційну шкоду, яку завдають зловмисники.

Важливо відзначити, що, хоча ШІ та автоматизовані інструменти значно підвищують ефективність кібербезпеки, вони не можуть повністю замінити участь кваліфікованих фахівців. Спеціалісти з кібербезпеки повинні брати активну участь у налаштуванні та адаптації засобів під конкретні потреби організації, забезпечуючи її відповідність специфічним вимогам і умовам.

Література

1. Міністерство юстиції України. Наказ від 21.08.2024 р. за № 1278/42623. Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж. URL: https://zakon.rada.gov.ua/laws/show/z1278-24#Text

2. Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", University of Oxford, 2021. URL: (https://gcscc.ox.ac.uk/cmm-2021-edition)

3. ENISA. "National Capabilities Assessment Framework", 2020, URL https://cyberpolicy.nask.pl/wp-content/uploads/2022/02/WP2020-0.3.1.2-/National-Capabilities-Assessment-Framework.pdf

4. "Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers", 2020. URL: https://www.gp-digital.org/publication/involvingstakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/

5. OAS. "Managing National Cyber Risk", 2018. URL https://www.oas./org/es/sms/cicte/ENGcyberrisk.pdf

6. Microsoft. "Building an Effective National Cybersecurity Agency", 2018. URL: ncsguide.org ›wp-content › uploads ›2021/11 ›2021-Guide-1

7. ENISA. "National Cyber Security Strategies: Training Tool", 2016. URL: ENISA ›ncss-training-tool

8. CCDCOE. "Cybersecurity Strategy & Governance Repository". URL: https://ccdcoe.org/library/strategy-andgovernance/

ІНТЕГРАЦІЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПРОФЕСІЙНУ ПІДГОТОВКУ ПЕДАГОГІВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ДЛЯ РОЗВИТКУ КОМПЕТЕНТНОСТЕЙ

Волотовська Т. П.
ДЗВО «Університет менеджменту освіти» НАПН України
E-mail: volotovskayatanya79@gmail.com

В умовах стрімкого розвитку технологій та цифровізації освітнього простору, професійне навчання педагогів стикається з новими викликами та можливостями. Сучасні цифрові технології не лише відкривають нові горизонти для вдосконалення методик навчання, але й вимагають від педагогів набуття нових компетентностей, здатних забезпечити ефективну інтеграцію цих технологій в освітній процес.

Першочерговим завданням цього напряму є підготовка педагогічних кадрів, здатних орієнтуватися у сучасних цифрових інструментах та використовувати їх для покращення якості освіти. Це включає не лише технічні навички, а й розвиток цифрової грамотності, критичного мислення та здатності адаптуватися до змінних умов освітнього середовища. Водночас, перед педагогами постають виклики, пов’язані з інтеграцією технологій: забезпечення доступу до ресурсів, оновлення знань та вмінь, а також подолання психологічних бар’єрів.

Вивчення проблеми формування професійних компетентностей сучасних педагогів є важливою темою в академічних колах, і