

3. Тищенко К. В. Програмування систем збору і аналізу даних / К. В. Тищенко, О. П. Ткач. – Суми: Сумський державний університет, 2022. – 168 с.

4. Програмування мікроконтролерів: стратегія та тактика. Харків: "Освіта", 2021. - 310 с.

УДК 004.056.55:004.8

Сидорова Я.О., студентка

Державний торговельно-економічний університет, м. Київ, janesidorova2@gmail.com

РОЗУМНА КІБЕРБЕЗПЕКА: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МИТТЄВОГО ВИЯВЛЕННЯ ТА САМОСТІЙНОГО РЕАГУВАННЯ НА КІБЕРАТАКИ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

У сучасному цифровому середовищі, яке стрімко трансформується під впливом новітніх технологій, питання кібербезпеки набуває критичного значення для сталого функціонування державних органів, комерційних структур, освітніх закладів, об'єктів критичної інфраструктури та звичайних користувачів. Різке зростання кількості кібератак, зокрема цілеспрямованих (АРТ), атак із застосуванням штучного інтелекту та шкідливого ПЗ, що постійно еволюціонує, робить традиційні методи захисту малоєфективними. В умовах нових викликів особливого значення набуває створення та впровадження інтелектуальних систем кіберзахисту, які здатні не лише аналізувати ситуацію в режимі реального часу, а й приймати автономні рішення щодо реагування на загрози. Штучний інтелект (ШІ) пропонує принципово нову парадигму організації кіберзахисту. Завдяки здатності до аналізу великих масивів даних, виявлення прихованих закономірностей, класифікації поведінкових моделей користувачів і систем, ШІ дозволяє переходити від реактивного до проактивного захисту. Це означає, що загроза може бути не лише вчасно виявлена, але й нейтралізована до того, як вона завдасть шкоди. При цьому важливою перевагою таких систем є їх здатність до самонавчання, що дозволяє їм адаптуватися до нових типів атак, навіть якщо ці атаки ще не були зафіксовані у відкритих базах даних чи сигнатурних системах. Як зазначено у звіті Національного координаційного центру кібербезпеки при РНБО України, саме впровадження адаптивних інтелектуальних рішень є головним пріоритетом цифрової безпеки в державному секторі [1].

Функціонування інтелектуальної системи кібербезпеки базується на комплексному підході. В основі лежить постійний моніторинг трафіку, логів, поведінкових патернів користувачів, даних з кінцевих точок та серверів. Отримані дані обробляються за допомогою алгоритмів машинного навчання, зокрема нейронних мереж, які ідентифікують аномалії або підозрілу активність. У разі виявлення потенційної загрози, система здійснює автоматизоване реагування — ізоляцію вузлів, блокування доступу, зміни в конфігурації, повідомлення адміністраторам або навіть активацію резервних копій. Такий підхід дозволяє значно скоротити час реагування — від кількох хвилин, як це було раніше, до мілісекунд, що є критичним у сучасних умовах. Значним кроком вперед у цій галузі є використання глибокого навчання, зокрема згорткових нейронних мереж (CNN), рекурентних мереж (LSTM) та трансформерів, які здатні працювати з послідовностями подій і передбачати розвиток загроз у часі. Іншим важливим напрямом є застосування генеративних моделей (наприклад, GAN), які дозволяють моделювати потенційні атаки для тренування захисних механізмів. Це дає змогу «перевірити на міцність» систему ще до реального вторгнення. В Україні вже реалізуються пілотні проекти, що базуються на принципах розумної кібербезпеки. Зокрема, дослідницькі інститути при РНБО, СБУ та Кіберполіції впроваджують моделі, що дозволяють забезпечувати раннє виявлення аномалій у державних інформаційних системах. У приватному секторі окремі великі компанії використовують платформи з інтегрованим ШІ для захисту фінансових даних, клієнтських баз, інтелектуальної власності. Одним з прикладів є експериментальний програмно-

апаратний комплекс «Січ-АІ», що проходить тестування у рамках національної програми цифрової стійкості. Його алгоритм самостійно моделює мережеву поведінку системи й автоматично коригує захисні протоколи у разі виявлення підозрілих відхилень від стандарту. Проте, незважаючи на очевидні переваги, широке впровадження систем ШІ у сферу кібербезпеки супроводжується низкою викликів. Передусім це питання достовірності та якості навчальних даних, оскільки некоректні дані можуть призвести до хибних рішень. Як зазначає дослідниця Притула Я.О., системи штучного інтелекту повинні функціонувати за принципом пояснюваності, а їх дії мають бути верифікованими для збереження довіри з боку користувачів [3]. Тим не менше, впровадження таких систем у практичну діяльність потребує комплексного підходу, що включає вирішення низки правових, етичних та технічних питань. Питання якості даних для навчання моделей, а також прозорість та верифікація прийнятих ШІ рішень, є важливими аспектами для забезпечення довіри користувачів до таких систем. У майбутньому, розвиток цієї технології має бути тісно пов'язаний із законодавчим регулюванням та міждисциплінарною співпрацею вчених, інженерів і правників, що забезпечить ефективне та етичне використання інтелектуальних систем кібербезпеки. З огляду на дедалі складніші та непередбачувані кібератаки, розумна кібербезпека, побудована на штучному інтелекті, може стати ключовим інструментом для досягнення надійного та сталого захисту. Завдяки здатності таких систем до проактивного реагування й самонавчання, надається можливість не лише вчасно виявляти загрози, а й попереджати їх до того, як вони завдадуть шкоди. При цьому важливим є створення умов для інтеграції таких рішень в екосистему національної безпеки, зокрема шляхом стратегічних інвестицій у дослідження та розвиток технологій штучного інтелекту. Національний контекст впровадження ШІ в кібербезпеку є особливо важливим в умовах глобальних кіберзагроз. Україна має всі шанси стати лідером у розвитку інтелектуальних систем кіберзахисту, що дозволить зміцнити цифровий суверенітет і безпеку. У цьому контексті важливим є не лише технічне забезпечення, а й розробка нормативно-правових актів, які б регулювали використання таких технологій у критичних секторах. Потрібно також пам'ятати про важливість постійного вдосконалення інфраструктури й регулярного навчання персоналу, що дозволяє забезпечити довготривалий ефект від використання таких технологій.

У підсумку, інтеграція ШІ в кібербезпеку є стратегічною необхідністю для забезпечення стійкості цифрової інфраструктури. Вона дозволяє створити новий рівень захисту, здатний ефективно реагувати на загрози в реальному часі та адаптуватися до еволюції кіберзагроз. Подальший розвиток таких технологій має бути підтриманий міжвідомчою співпрацею та інвестиціями у підготовку кадрів, що стане основою для сталого забезпечення кібербезпеки на національному рівні.

Список посилань

1. Національний координаційний центр кібербезпеки при РНБО України. Звіт про стан кібербезпеки в Україні, 2023. – Режим доступу: <https://ncsc.gov.ua>
2. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
3. Притула Я.О. Інтелектуальні системи виявлення атак у хмарних обчисленнях // Науковий вісник ХНУРЕ. – 2023. – №1.
4. Український інститут кібербезпеки. Аналітика новітніх підходів до захисту інформаційних систем. – 2024.
5. Miller R. Deep Learning in Cybersecurity: A Review // ACM Computing Surveys. – 2023.
6. National Institute of Standards and Technology (NIST). Artificial Intelligence for Cybersecurity: Roadmap. – 2023. – Режим доступу: <https://www.nist.gov/itl/ai-cyber>
7. Єрмоленко В.І. Технології розумного моніторингу в системах кібербезпеки // Наукові праці ОНАХТ. – 2022. – №3.