

УДК 681.5

Ащепкова Н.С., канд. техн. наук, доцент
Карпенко М.Є., студент

Дніпровський національний університет ім. О. Гончара, ashchepkova.ftf.dnu@gmail.com

ВПРОВАДЖЕННЯ СИСТЕМИ КЕРУВАННЯ МІКРОКЛІМАТОМ ЦЕХУ

Промислові контролери застосовуються для автоматизації технологічних процесів, які передбачають виконання великої кількості логічних операцій [1].

Програмований логічний контролер (ПЛК; англ.: Programmable Logic Controller або PLC) – це спеціалізована мікропроцесорна система, що використовується для автоматизації технологічних процесів та загальнопромислових установок і комплексів (конвеєрів, рольгангів, підйомних кранів, подрібнювачів, млинів, класифікаторів, змішувачів, пакувальників, робототехнічних та гнучких виробничих комплексів, тощо) [2]. ПЛК широко використовуються для автоматизації будівель (контроль доступу до приміщення, керування освітленням, обігрівом, вентиляцією та кондиціонуванням повітря, керування ліфтами, ескалаторами, тощо).

У сучасних автоматизованих системах ПЛК забезпечують точне та стабільне керування обладнанням. Вони виконують: моніторинг параметрів, регулювання режимів роботи, синхронізацію роботи механізмів та аналіз виробничих даних у реальному часі. Завдяки цьому можливо не лише покращити якість технологічних процесів, а й підвищити рівень безпеки на підприємствах [3].

Більшість програмованих промислових контролерів немає екрану і клавіатури; їх програмування здійснюється через вбудований RJ-45 порт, на комп'ютері у спеціальному програмному середовищі [4].

Стан людини залежить від інтенсивності праці, характеристик обладнання, організації робочого місця, тривалості впливу шкідливих факторів, а також індивідуальних особливостей адаптації організму до умов праці. Тривала дія на організм людини несприятливих виробничих факторів погіршує самопочуття, знижує продуктивність праці і часто призводить до професійних захворювань і порушень стану здоров'я. В наш час багато виробничих вакансій пропонується для жінок, інвалідів та ветеранів. Таким чином, організаційні заходи по забезпеченню сприятливих умов праці є актуальним науково-прикладним завданням.

Об'єкт дослідження – система автоматичного контролю мікроклімату на виробничій дільниці. Для розробки та впровадження системи автоматичного контролю мікроклімату виробничої дільниці проаналізовано технічні характеристики обладнання. До складу виробничої дільниці входять:

- технологічне обладнання - токарно-револьверний верстат моделі 1Е365ПФ30 з вертикальною віссю револьверної головки,
- пристрій керування - мікроконтролер Arduino Uno;
- допоміжне обладнання - датчики температури та вологості DHT11;
- виконавчі пристрої - вентилятори, обігрівачі, зволожувачі;
- система візуалізації - LCD-екран або комп'ютер з SCADA-системою.

Для забезпечення узгодженої роботи обладнання розроблено програмне забезпечення для мікроконтролера. За заданим алгоритмом мікроконтролер зчитує дані з датчиків, аналізує їх та генерує керуючі впливи на виконавчі пристрої.

Список посилань

1. Ельперін І.В. Промислові контролери. К: НУХТ, 2003. – 320с.
2. Бублик В.В. Об'єктно-орієнтоване програмування. К.: "ІТ книга", 2015. – 624 с.

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-