НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

МАТЕРІАЛИ VI НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ»

13 грудня 2024 року

Київ – 2024

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 12 від 28 листопада 2024 р.)

Б-39 **Безпека енергетики** в епоху цифрової трансформації, VI науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 13 грудня 2024 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2024. 191 с.

В-39 **Energy security** in the digital transformation era, VI scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, December 13, 2024). Kyiv: PIMEE NAS of Ukraine, 2024. 191 p.

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ім. Г.Є. ПУХОВА НАН УКРАЇНИ

МАТЕРІАЛИ
VI НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

13 грудня 2024 року

м. Київ

2024

Вельмишановний учасник _____

_____

Запрошуємо Вас прийняти участь в роботі VI науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», яка буде проходити 13 грудня 2024 року в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ).

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор, директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, професор,
заступник директора з наукової роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший наковий співробітник

Я.Ю. Дорогий, В.В. Цуркан, О.О. Дорога-Іванюк

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

Анотація. У статті розглянуто використання штучного інтелекту (ШІ) для захисту критичної інфраструктури енергетичних установ. Розкрито можливості ШІ у протидії кібератакам та забезпеченні стабільного функціонування систем енергозабезпечення. Особливу увагу приділено ризикам, спричиненим агресією російської федерації, а також обговорено потенційні рішення на основі технологій ШІ, що допомагають посилити захист від зовнішніх та внутрішніх загроз.

Вступ. Критична інфраструктура енергетичної галузі є фундаментальною для забезпечення національної безпеки України, оскільки від її стабільного функціонування залежить робота більшості інших секторів, зокрема військового, транспортного, медичного. Енергетичні установи України вже тривалий час стикаються з численними викликами, пов'язаними з агресією рф, яка застосовує широкий спектр методів для порушення роботи об'єктів енергетичної інфраструктури. Основні загрози включають кібератаки, фізичне пошкодження об'єктів, внутрішні інсайдерські загрози та обмеженість ресурсів для реагування на інциденти. В умовах таких викликів технології штучного інтелекту стають важливим інструментом, що допомагає вчасно виявляти та реагувати на загрози, а також оптимізувати процеси захисту.

Проблематика захисту енергетичної інфраструктури в умовах агресії рф. Енергетичні установки, зокрема електричні станції, лінії передачі, об'єкти зберігання та розподілу енергії, є пріоритетними цілями для кібератак та фізичних нападів. В останні роки рф активізувала свої дії, спрямовані на дестабілізацію української енергетичної галузі. Основні напрямки атак включають:

1. *Кібератаки на енергосистеми*. З початку військової агресії російські хакери неодноразово здійснювали складні атаки на системи керування енергопостачанням. Зокрема, кібератаки BlackEnergy та Industroyer (2015 та 2016 роки) призвели до масштабних відключень електропостачання в Україні [1]. Такі атаки спрямовані на виведення з ладу систем SCADA (Supervisory Control and Data Acquisition), які є критичними для моніторингу та управління енергетичними мережами. Штучний інтелект може допомогти у виявленні цих загроз шляхом аналізу мережевої активності в режимі реального часу та виявлення аномалій, які можуть свідчити про зловмисну активність.

2. *Фізичні атаки на об'єкти енергетики*. Пошкодження трансформаторів, підстанцій та іншого обладнання, спричинені ракетними ударами та обстрілами, стають частими подіями в умовах військової агресії.

ШІ може допомогти у моніторингу стану фізичних компонентів енергосистем за допомогою безпілотних літальних апаратів, обладнаних сенсорами. Це дозволить проводити швидке виявлення пошкоджень та планувати оперативні ремонтні роботи.

3. *Внутрішні загрози та інсайдерська діяльність*. Окрім зовнішніх загроз, існують також інсайдерські ризики, коли співробітники або особи, які мають доступ до систем, можуть сприяти порушенню функціонування об'єктів енергетичної інфраструктури. ШІ може застосовуватися для автоматизованого аналізу поведінки користувачів у системах, щоб виявляти підозрілі дії, які можуть вказувати на потенційну інсайдерську загрозу.

Використання штучного інтелекту для забезпечення кібербезпеки енергетичних установ. Сучасні технології ШІ можуть виконувати численні завдання, пов'язані із забезпеченням кібербезпеки. Серед них:

1. *Аналіз загроз і раннє виявлення аномалій*. Алгоритми ШІ, що використовуються для аналізу великих обсягів даних, допомагають виявляти аномальні патерни активності, що можуть бути ознакою кібератак. Наприклад, методи машинного навчання можуть знаходити підозрілі операції, які вказують на можливе втручання у функціонування мережевих систем.

2. *Розширений моніторинг системи*. Використання ШІ дозволяє безперервно аналізувати трафік та активність в інформаційних мережах енергетичних об’єктів. Такі системи можуть розпізнавати новітні типи шкідливого ПЗ та інші кіберзагрози, що робить можливим оперативне реагування на загрози, що з’являються.

3. *Автоматизація процесів реагування*. За допомогою ШІ стає можливим автоматизувати процеси реагування на кіберзагрози, що дозволяє знизити навантаження на персонал та зменшити час між виявленням та нейтралізацією загрози. Зокрема, алгоритми ШІ можуть автоматично ізолювати підозрілі пристрої від мережі для зменшення шкоди від потенційної атаки.

Використання ШІ для фізичного моніторингу об’єктів енергетичної інфраструктури. Фізичний захист об'єктів критичної інфраструктури є важливим елементом забезпечення їх стійкості. Використання ШІ в поєднанні з сенсорами та безпілотними апаратами може значно покращити здатність до моніторингу та управління об'єктами енергетичної інфраструктури. Основні напрямки використання:

1. *Дрони для виявлення фізичних пошкоджень*. Застосування безпілотників з ШІ-аналізом зображень дозволяє автоматизувати процес моніторингу об’єктів. За допомогою візуального аналізу та тепловізійних камер такі дрони можуть виявляти пошкодження інфраструктури, спричинені фізичними атаками, та передавати дані для швидкого ремонту.

2. *Сенсорні мережі для раннього виявлення аварій*. Установки, обладнані мережами сенсорів, можуть передавати дані в реальному часі для

аналізу ШІ. Це дозволяє швидко ідентифікувати несправності або критичні зміни у роботі обладнання, що мінімізує ризик масштабних аварій.

Прогнозування та оцінка ризиків з використанням ШІ. Однією з найбільш перспективних можливостей використання ШІ в енергетичній галузі є прогнозування ймовірних загроз та оцінка ризиків для критичної інфраструктури. ШІ дозволяє здійснювати детальний аналіз минулих інцидентів, а також поточного стану систем, що дозволяє створити точні прогнози щодо майбутніх атак і сприяє покращенню стратегії захисту енергетичних об'єктів. Такі системи можуть стати важливим інструментом у боротьбі з кіберзагрозами, дозволяючи енергетичним компаніям вчасно реагувати на потенційні загрози.

Основними напрямками застосування ШІ можуть бути:

1. *Прогнозування інцидентів на основі даних про атаки*. Використовуючи великі обсяги історичних даних про попередні кібератаки, ШІ може ефективно прогнозувати ймовірність нових атак на енергетичну інфраструктуру. За допомогою алгоритмів машинного навчання та аналізу патернів у даних про атаки, ШІ здатний ідентифікувати тренди і повторювані моделі, що можуть свідчити про підготовку до нових інцидентів. Ці алгоритми здатні враховувати різноманітні фактори, такі як тип атак, методи проникнення, вразливості в системах та особливості хакерських угруповань, що здійснюють напади.

Наприклад, якщо система спостерігає підвищену активність певних кіберзагроз у інших секторах або регіонах, ШІ може передбачити ймовірність того, що ці загрози також можуть поширитись на енергетичну інфраструктуру. Така обізнаність дозволяє заздалегідь вжити заходів, таких як оновлення безпеки або зміна тактик захисту.

2. *Аналіз вразливостей системи та оцінка ризиків*. Оцінка ризиків є важливим аспектом для виявлення слабких місць у критичних енергетичних інфраструктурах. Завдяки використанню ШІ, можна створити моделі, які прогнозують, де саме система має найбільшу вразливість до потенційних атак. ШІ здійснює постійний моніторинг і виявляє нетипові аномалії в роботі систем, які можуть свідчити про спроби проникнення чи інші шкідливі дії. В результаті цієї роботи, алгоритми здатні оцінити ступінь ризику для кожного з об'єктів енергетичної інфраструктури і, на основі цих даних, надавати конкретні рекомендації для зниження цього ризику.

3. *Автоматичне оновлення заходів безпеки*. ШІ може допомогти в автоматичному оновленні заходів безпеки на основі прогнозів і оцінки ризиків. Наприклад, алгоритми машинного навчання здатні адаптуватися до нових загроз і атак, змінюючи налаштування системи безпеки в реальному часі. Якщо ШІ виявить нові вразливості або зростання ймовірності атак у певній частині енергетичної інфраструктури, система може автоматично вжити відповідних заходів для зміцнення захисту, включаючи оновлення антивірусного програмного забезпечення, зміни в параметрах мережевого захисту або впровадження додаткових бар'єрів безпеки.

4. *Інтеграція з іншими системами безпеки*. Важливою перевагою використання ШІ є можливість інтеграції з іншими системами безпеки, що дозволяє створювати комплексні системи моніторингу та захисту. ШІ може працювати в тандемі з існуючими технологіями захисту, такими як фаєрволи, системи виявлення вторгнень (IDS) [2] та системи управління інцидентами (SIEM) [3]. Такий подхід дозволяє отримати більш точну картину загроз і забезпечує більш ефективне реагування на інциденти. Таким чином, прогнозування і оцінка ризиків за допомогою ШІ не лише підвищує рівень безпеки енергетичних об'єктів, але й інтегрує різні технології для комплексного захисту.

5. *Динамічне оновлення прогнозів з урахуванням поточних умов*. Однією з ключових переваг ШІ є можливість динамічного оновлення прогнозів у реальному часі. Коли змінюються умови, такі як зростання активності хакерських угруповань або зміна зовнішніх факторів, ШІ може швидко адаптувати свої прогнози, забезпечуючи постійне оновлення стратегій захисту. В умовах сучасного агресивного середовища здатність оперативно адаптувати прогнози та стратегічні рішення буде важливою перевагою для енергетичних компаній.

Підсумовуючи вищенаведене, використання таких можливостей дозволить енергетичним компаніям бути готовими до ймовірних атак і ефективно розподіляти ресурси для захисту своїх критичних інфраструктур. Завдяки прогностичним можливостям ШІ, енергетична галузь здатна значно покращити свої системи безпеки, знижуючи ризик кібератак і мінімізуючи потенційні збитки від інцидентів.

Висновки. Агресія рф створює численні виклики для захисту критичної інфраструктури енергетичної галузі України. У цих умовах використання штучного інтелекту стає невід'ємною частиною забезпечення надійності та безпеки енергетичних систем. ШІ не лише дозволяє автоматизувати моніторинг і виявлення загроз, але й надає можливості для прогнозування інцидентів, що значно підвищує ефективність захисту. Застосування технологій ШІ у кібербезпеці та фізичному захисті енергетичних об'єктів сприятиме зменшенню ризиків, забезпечуючи стабільне функціонування енергетичної інфраструктури в умовах агресії.

1. Повернення Industroyer: нові кібератаки на енергетичний сектор в Україні / Softico. URL: https://softico.ua/uk/news/povernennya-industroyer-novi-kiberataki-na-energetichnij-sektor-v-ukrayini/ (дата звернення: 02 листопада 2024).
2. Захист критичної інфраструктури: як зберегти безпеку в умовах нових кіберзагроз / Wezom. URL: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi (дата звернення: 12 листопада 2024).
3. Захист критичної інфраструктури: аналіз сучасних підходів / Науково-інформаційний журнал «Науковий вісник» НУОУ. DOI: 10.28925/295272. URL: https://sit.nuou.org.ua/article/download/295272/295497/700877 (дата звернення: 13 листопада 2024).