Дорогий Я. Ю., д.т.н., професор,
Донецький національний технічний університет,
Цуркан В. В., к.т.н., доцент,
Інститут спеціального зв'язку та захисту
інформації КПІ ім. Ігоря Сікорського
Дорога-Іванюк О. О., вчитель вищої категорії
Пологівський ліцей Ковалівської територіальної громади
Білоцерківського району Київської області

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ МЕДИЧНОЇ ГАЛУЗІ

Захист критичної інфраструктури медичних установ є важливим аспектом національної безпеки, особливо в умовах сучасних глобальних загроз, які включають кібератаки та фізичні вторгнення. Медична інфраструктура охоплює лікарні, клініки, центри обробки медичних даних і лабораторії, де забезпечення безпеки персональних даних пацієнтів і надійності систем є обов'язковою умовою ефективного функціонування. Зі зростанням військової агресії рф щодо України медична галузь стикається з постійними атаками, спрямованими на підрив функціонування системи охорони здоров'я. ШІ у цьому контексті стає ключовим інструментом для попередження та протидії загрозам. Використання ШІ для захисту критичної інфраструктури в медичній галузі охоплює кілька ключових напрямків, що підвищують кібербезпеку медичних установ. ШІ може допомогти виявляти загрози в режимі реального часу, аналізуючи великі обсяги даних і забезпечуючи проактивне реагування на потенційні атаки. На основі історичних даних ШІ може прогнозувати кібератаки, дозволяючи мінімізувати ризики. Крім того, ШІ має потенціал в сфері активного захисту електронних медичних записів, контролю доступу до конфіденційної інформації та виявлення аномальної поведінки користувачів. Завдяки аналізу великих даних та системам підтримки клінічних рішень, ШІ не лише може покращити кіберзахист, але й дозволить ефективно оцінювати ризики, виявляючи вразливості систем.

Законодавча база України сприяє інтеграції ШІ у сферу кібербезпеки медичних установ. Закон України «Про основні засади забезпечення кібербезпеки України» [1] зобов'язує об'єкти критичної інфраструктури, у тому числі медичні заклади, запроваджувати сучасні технології для захисту інформаційних систем. Відповідно до Закону України «Про критичну інфраструктуру» [2], Міністерство охорони здоров'я України (МОЗ) виконує важливі функції як секторальний орган, відповідальний за захист і безперервність функціонування об'єктів критичної інфраструктури у сфері охорони здоров'я. Основними завданнями МОЗ у цій сфері є ідентифікація та забезпечення безпеки ключових медичних установ, таких як лікарні, медичні дослідницькі центри, а також ланцюгів постачання ліків та обладнання, які мають стратегічне значення для держави. Завдяки цьому забезпечується не лише стабільне функціонування медичних закладів, але й доступність послуг для населення у випадку надзвичайних ситуацій.

МОЗ також зобов'язане розробляти та впроваджувати стандарти безпеки, що відповідають як національним, так і міжнародним вимогам, в тому числі, з використанням технологій ШІ. Одночасно міністерство координує свої дії з іншими державними органами, такими як Служба безпеки України та Міністерство внутрішніх справ, для створення комплексної системи управління ризиками та підвищення стійкості медичної галузі до можливих загроз.

Серед інших завдань МОЗ є розробка та реалізація планів кризового реагування, які дозволяють швидко й ефективно реагувати на загрози та забезпечувати безперебійне надання медичних послуг навіть у найскладніших обставинах.

На підставі проведеного дослідження, можна зробити висновок, що захист критичної інфраструктури медичних установ є вкрай важливим для забезпечення національної безпеки України, особливо на тлі сучасних кіберзагроз та військових викликів. Використання технологій штучного інтелекту надає нові можливості для попередження та протидії таким загрозам. Інтеграція ШІ у системи кібербезпеки дозволяє проводити моніторинг і аналіз ризиків у режимі реального часу, а також оперативно виявляти та нейтралізувати потенційні атаки.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02 листопада 2024).

2. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 08 листопада 2024).