Лунгол Ольга Миколаївна
к.пед.н., доц., завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки ННІ ПФПКП імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, Україна
Коломийченко Ірина Володимирівна
здобувач вищої освіти 2 курсу ННІПФПКП ім. Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, Україна

АНАЛІЗ СУЧАСНИХ НЕБЕЗПЕК ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення стійкого функціонування об'єктів критичної інфраструктури є ключовим чинником національної безпеки, особливо в умовах триваючої гібридної агресії та кібервійни [1; 2]. Інформаційні системи об'єктів критичної інфраструктури (ІС ОКІ), які включають кіберфізичні та промислові сегменти, зазнають комплексних та скоординованих кібератак, що призводить до каскадних збоїв [3, с. 878]. Відтак, актуалізується необхідність детального аналізу сучасних небезпек задля відповідного вдосконалення методологій кіберзахисту.

Метою даної роботи є системний аналіз сучасних загроз та небезпек для інформаційних систем об'єктів критичної інфраструктури, обґрунтування ключових методологічних підходів до забезпечення їх стійкості та адаптивності до динамічних викликів.

Сучасні небезпеки ІС ОКІ мають мультивекторний характер. Серед них виділяють: цілеспрямовані кібератаки, які використовують вразливості у SCADA/ICS-системах, що робить звичайні засоби захисту малоефективними [3, с. 879]; атаки на ланцюги постачання, які стають джерелом каскадних збоїв; інформаційно-психологічні операції, що використовують дезінформацію для впливу на персонал, актуалізуючи «людський фактор» [2]. В умовах високої невизначеності щодо інтенсивності експлуатаційних навантажень та зовнішніх впливів, забезпечення захищеності ІС ОКІ вимагає інтеграції різних методологічних підходів.

У науковій літературі виділяють, відповідно, три основні підходи до забезпечення захищеності [1, с. 675]:

- нормативний підхід, що базується на встановленні чисельних показників (норм) та коефіцієнтів запасу, які забезпечують стійкість системи до наближення до граничних станів. Хоча цей підхід є базовим, окремі вітчизняні науковці зазначають, що йому бракує точності аналізу невизначеностей;

- ймовірнісний підхід (за критерієм надійності), який ґрунтується на оцінці ймовірності досягнення граничного стану при кібервпливі. Для підвищення ефективності систем виявлення вторгнень у межах цього підходу рекомендують використовувати ансамблеві класифікатори та математичний апарат орієнтованих ациклічних графів для моделювання ланцюжків атак [1, с. 677];

- підхід, заснований на управлінні ризиками, який є інтегральним. При цьому ризик визначається як комбінація ймовірності реалізації граничного стану та можливих збитків [1, с. 679]. Цей підхід забезпечує ефективний розподіл ресурсів, концентруючись на найкритичніших загрозах.

Сучасні дослідження підкреслюють, що для підвищення стійкості функціонування ІС ОКІ необхідна інтеграція цих підходів з інтелектуальними технологіями. Зокрема, В. Гречанінов обґрунтовує доцільність використання сценарного моделювання та агентних систем штучного інтелекту у кризових (ситуаційних) центрах для проактивного реагування [3, с. 878, 880]. Перехід до проактивної парадигми захисту потребує розробки уніфікованих процедур, що поєднують оперативну розвідувальну інформацію з механізмами автоматизованого реагування. Ключовим викликом тут є забезпечення міжвідомчої синхронізації та обміну даними між суб’єктами сектору безпеки й операторами критичної інфраструктури, тобто юридичними особами будь-якої форми власності та/або фізичними особами-підприємцями, що на правах власності, оренди або на інших законних підставах здійснюють управління об’єктом критичної інфраструктури та відповідають за його поточне функціонування. Така координація має базуватися на єдиних стандартах таксономії загроз та обов’язковому застосуванні принципів Zero Trust для мікросегментації технологічних мереж. На наш погляд, це дозволить не лише ефективно локалізувати інциденти, але й підтримувати безперервність функціонування критичних сервісів, використовуючи керовані деградаційні режими роботи, які забезпечують стійкість у складних умовах.

Отже, забезпечення захищеності ІС ОКІ в умовах сучасних гібридних загроз вимагає переходу від реактивних заходів до інтегрованої, проактивної парадигми. Це передбачає поєднання нормативного, ймовірнісного та ризикового підходів із застосуванням інтелектуальних систем. Подальші дослідження мають бути зосереджені на розробці механізмів інтеграції даних із різних сегментів ОКІ, стандартизації процедур вимірювання стійкості та розширенні можливостей агентного ШІ для забезпечення автономного й узгодженого реагування на багатоканальні загрози.

Список літератури

1. Толюпа С. В., Кулько А. А. Забезпечення захищеності складних інформаційних та технологічних систем об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка. 2025. № 4 (28)*. С. 671–687. https://doi.org/10.28925/2663-4023.2025.28.859.

2. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Кібербезпека: освіта, наука, техніка. № 1(25). 2024*. С. 379 – 389.

3. Гречанінов В. Ф. Моделі та технології інтелектуального захисту інформаційних систем критичної інфраструктури для підвищення стійкості. *Кібербезпека: освіта, наука, техніка. 2025. № 1 (29).* С. 878 – 896.

4. Абзалов Д., Габорець О. Кібербезпека як ключовий елемент інформаційного забезпечення сектору оборони України. Науково-практична конференція «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України» (Львів, 20 грудня 2024). Львів : ЛьвДУВС, 2025. С. 3-4.