

Хрутьба Ю.С., докторант кафедри екології та природоохоронних технологій¹, доцент кафедри екологічного менеджменту та підприємництва², к.е.н., доцент
Лисак Р.С., доцент кафедри екології та технологій захисту навколишнього середовища³, к.т.н., доцент
Лисак О.О., здобувач освіти за спеціальністю 121 – Інженерія програмного забезпечення⁴
¹Державний університет «Житомирська політехніка»
²Київський національний університет імені Тараса Шевченка
³Національний транспортний університет
⁴ВСП «Оптико-механічний фаховий коледж Київського національного університету імені Тараса Шевченка»

ПРОБЛЕМИ У РОБОТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ЗАГРОЗА ЕКОЛОГІЧНІЙ БЕЗПЕЦІ

У час активної цифровізації функціонування систем управління досить сильно залежить від якості програмного забезпечення, яке використовується. Збої у роботі програмного забезпечення можуть створювати серйозні виклики для екологічної безпеки. До викликів, що стосуються управління екологічними системами можна віднести збої систем моніторингу та порушення роботи автоматизованих систем контролю. *Програмні збої у роботі систем моніторингу* можуть вимкнути системи екологічного моніторингу, залишивши «сліпі зони» у відстеженні забруднення основних складових біосфери. Це може призвести до несвоєчасного виявлення екологічних загроз. *Порушення роботи автоматизованих систем контролю* може призвести до неконтрольованих викидів забруднюючих речовин, адже пошкоджена програма може видавати некоректні та недостовірні дані, що вплине на прийняття управлінських рішень у цьому напрямку. Особливої уваги заслуговують загрози критичній інфраструктурі, в тому числі атомній енергетиці, хімічній промисловості та енергетичній промисловості. Проблеми у роботі *програмного забезпечення атомних електростанцій* можуть призвести до аварій з радіоактивним забрудненням. Проблеми у роботі *програмного забезпечення для хімічних виробництв* можуть спричинити неконтрольовані викиди токсичних речовин, що загрожує життю та здоров'ю населення, а також екосистемам на великих територіях. Порушення у роботі *програмного забезпечення для управління електромережами* може призвести до відключень електроенергії, що вплине на роботу очисних споруд, систем водопостачання та промислових підприємств. Недоліки чи проблеми у роботі програмного забезпечення роблять системи вразливими до кібератаки на об'єкти критичної інфраструктури. Збої у роботі програмного забезпечення можуть мати безліч наслідків:

- втрата екологічних даних, частину яких достатньо часто неможливо відновити;
- дезінформація, тобто поширення неточних даних про стан довкілля, що ускладнює реагування на екологічні загрози;
- збільшення енергоспоживання, оскільки програмні кризи часто вимагають додаткових обчислювальних ресурсів для відновлення систем, що призводить до зростання споживання електроенергії та збільшення вуглецевого сліду;
- збільшення обсягів електронних відходів, так як масові оновлення або заміна програмного забезпечення можуть призвести до передчасного списання обладнання, збільшуючи кількість електронних відходів;
- порушення нормального функціонування транспортних мереж, наприклад утворення заторів, які збільшують викиди парникових газів та погіршує якість повітря у містах;
- накопичення сміття, забруднення води та ґрунтів через порушення роботи систем управління відходами.

З метою запобігання порушень і збоїв у програмному забезпеченні необхідно здійснювати ряд заходів, серед яких:

- постійне проведення комплексних перевірок безпеки програмного забезпечення екологічно критичних систем;
- розробка детальних планів реагування на програмні збої з чітким розподілом відповідальності;
- навчання співробітників навичкам швидкого реагування на технічні збої та переходу на ручне управління;
- створення дублюючих систем управління для критично важливих екологічних об'єктів, що автоматично включаються при збоях основних систем;
- своєчасне встановлення вимог безпеки та оновлень програмного забезпечення для усунення вразливостей;
- впровадження цілодобового моніторингу стану програмного забезпечення з автоматичним сповіщенням про збої;
- розробка та впровадження національних стандартів кібербезпеки для екологічної інфраструктури;
- сертифікація програмного забезпечення, що використовується на екологічно критичних об'єктах;
- законодавче закріплення відповідальності розробників програмного забезпечення за збої у критичних системах;
- участь у міжнародних програмах обміну інформацією про кіберзагрози екологічній безпеці.