

Radosław Frydrych
Doradca Zarządu
Integrated Solutions sp. z o.o.

Jan Ekiel
Prezes Zarządu
LIKI Mobile Solutions sp. z o.o.

„Monitorowanie infrastruktury krytycznej z wykorzystaniem sztucznej inteligencji”

Teza główna: obiekt nie staje się odporny w chwili ogłoszenia alarmu. Jego gotowość trzeba budować i sprawdzać każdego dnia.

1. Gotowość obiektu jest stanem dynamicznym, a nie wpisem w rejestrze. Zależy od aktualnej dostępności energii, wody, ogrzewania, łączności i urządzeń, jakości powietrza, stanu technicznego budynku oraz kompletności procedur. Okresowa kontrola i papierowa dokumentacja nie wystarczą do oceny sytuacji podczas kryzysu.
2. Infrastruktura ochrony ludności powinna mieć charakter dual-use. Te same czujniki, systemy łączności i oprogramowanie, które na co dzień wykrywają awarie, wycieki, nieprawidłowe zużycie energii lub złą jakość powietrza, mogą podczas zagrożenia pomagać ocenić, ilu ludzi i przez jaki czas może bezpiecznie przyjąć dany obiekt. Codzienne wykorzystanie uzasadnia ekonomicznie inwestycję i pozwala stale sprawdzać jej sprawność.
3. Nie można uzależniać systemu bezpieczeństwa od infrastruktury, która podczas kryzysu może przestać działać jako pierwsza. System musi zachować najważniejsze funkcje również przy utracie Internetu, ograniczeniu łączności albo niedostępności usług chmurowych. Oznacza to potrzebę lokalnego przetwarzania danych, rozwiązań edge AI oraz zaplanowanych mechanizmów komunikacji awaryjnej.
4. Niezależność technologiczna nie oznacza izolacji ani korzystania wyłącznie z rozwiązań jednego kraju. Oznacza kontrolę nad danymi, interfejsami i dokumentacją, stosowanie otwartych standardów, możliwość wymiany poszczególnych komponentów oraz zdolność utrzymania i rozwoju systemu przez lokalnych partnerów. System Orion będzie przedstawiony jako praktyczny przykład takiego środowiska integracji – otwartego na technologie, dane i kompetencje kolejnych partnerów.