Streszczenie

Uzasadnienie wyboru tematu i powiązanie z programem Doktorat Wdrożeniowy

Niniejsza rozprawa została zrealizowana w ramach programu *Doktorat Wdrożeniowy*, projekt pt. „Elektroniczne Systemy Zabezpieczenia Technicznego jako źródło danych w procesie automatycznej obrony przed cyberatakami oraz wykrywania sprawcy przestępstwa", co implikuje tytuł rozprawy.

Niniejsza rozprawa koncentruje się na analizie i modelowaniu *Cyber-Fizycznych Systemów Ochrony (CPPS)* z wykorzystaniem metod sztucznej inteligencji, co bezpośrednio odpowiada na problemy sformułowane w temacie badawczym. Takie podejście umożliwia z jednej strony ocenę efektywności zainstalowanych systemów ochrony, poprzez wykorzystanie danych pochodzących nie tylko z samych systemów zabezpieczeń, ale również przez uwzględnienie kontekstu bezpieczeństwa i estymowanie atrybutów potencjalnego adwersarza (np. jego motywacji czy kwalifikacji). Z drugiej strony, proponowana metodologia pozwala na planowanie racjonalnego, *evidence-based* wzmocnienia środków mitygacji zagrożeń pochodzących zarówno ze sfery fizycznej, jak i cyberprzestrzeni.

W ten sposób ESZT stają się nie tylko elementem infrastruktury ochronnej, ale przede wszystkim bogatym źródłem danych, które po odpowiedniej analizie i modelowaniu stanowią fundament dla zintegrowanych strategii cyber-fizycznej obrony.

Zidentyfikowane luki badawcze

Analiza stanu wiedzy ujawniła pięć kluczowych luk:

Po pierwsze, tradycyjna metodologia EASI (Estimated Adversary Sequence Interruption), wprowadzona w 1977 roku, nie uwzględnia zagrożeń cybernetycznych. Badania własne wykazały, że klasyczne podejście wskazywało 89,88% prawdopodobieństwo przerwania ataku, podczas gdy po uwzględnieniu cyberzagrożeń wartość ta spadła do 1,63%. **Po drugie**, brakuje modeli degradacji specyficznych dla elektronicznych systemów zabezpieczeń technicznych (ESZT). Opracowany probabilistyczny model degradacji uwzględnia pięć czynników: starzenie komponentów (rozkład normalny), wzrost wiedzy przeciwnika (rozkład normalny), postęp technologiczny narzędzi ataku (model logarytmiczny), pojawianie się podatności (proces Bernoulliego) oraz efekty konserwacji (rozkład normalny). Symulacje Monte Carlo wykazały, że efektywność systemu może spaść z 98% do około 25% w ciągu 10 lat, a średnia linia trendu przekracza poziom 50% około 75-80 miesiąca eksploatacji. **Po trzecie**, studium przypadku pokazało praktyczne konsekwencje ignorowania degradacji: klasyczna ocena EASI wskazywała 88,64% skuteczności, podczas gdy po uwzględnieniu degradacji wartość spadła do 76,19% – różnica 12,45 punktów

procentowych. **Po czwarte**, brak standaryzacji w reprezentacji elementów infrastruktury oraz automatyzacji detekcji symboli technicznych na planach. Konwencjonalne modele detekcji obiektów nie radzą sobie z interpretacją kontekstu, gdzie znaczenie symbolu zależy od otoczenia. **Po piąte**, istniejące rozwiązania są fragmentaryczne i adresują pojedyncze aspekty problemu, brakuje holistycznego podejścia integrującego wszystkie wymiary oceny CPPS.

Teza i metodologia

Teza pracy: możliwe jest opracowanie zintegrowanego, probabilistycznego modelu oceny skuteczności CPPS uwzględniającego jednocześnie degradację komponentów, zagrożenia cybernetyczne oraz kontekst operacyjny.

Proponowane rozwiązanie składa się z trzech warstw: (1) percepcyjnej/detekcji - kontekstowa analiza planów z detekcją obiektów COG (Contextual Object Grouping), (2) decyzyjnej - grafy ścieżek ataku z algorytmem A* i modyfikacją EASI o wskaźniki degradacji oraz element cyberodporności, (3) raportującej - automatyzacja z użyciem modeli językowych LLM.

Wyniki i wkład naukowy

Symulacje Monte Carlo wykazały, że uwzględnienie degradacji i cyberzagrożeń może znacząco obniżyć skuteczność systemu bezpieczeństwa. Tego rodzaju przeszacowanie efektywności systemu może nie tylko oznaczać brak gospodarności, ale prowadzić do istotnych konsekwencji dla infrastruktury krytycznej w przypadku skutecznego ataku.

Główny wkład stanowią: (1) stworzenie pierwszego probabilistycznego modelu degradacji ESZT w kontekście CPPS, (2) rozszerzenie EASI o komponenty cyber-odporności i degradację komponentów, (3) nowe podejście (COG) do kontekstowej interpretacji symboli technicznych, (4) stworzenie praktycznego narzędzia do dynamicznego zarządzania bezpieczeństwem. Praca integruje metody z dziedzin oceny ryzyka, sztucznej inteligencji i cyberbezpieczeństwa w spójną metodologię wspartą walidacją na rzeczywistych przypadkach.

Implementacja

Rezultatem pracy jest funkcjonalne narzędzie AI-SecPA implementujące pełny proces oceny, począwszy od detekcji elementów architektonicznych przez uczenie maszynowe po generowanie rekomendacji z wykorzystaniem LLM. Narzędzie wydaje się wprowadzać istotne wsparcie w procesie decyzyjnym z zakresu zarządzania bezpieczeństwem operacyjnym i cyber-fizycznym.

Abstract

Topic Selection and Connection to the Implementation Doctorate Program

This dissertation was carried out within the framework of the *Implementation Doctorate* program, project titled "Electronic Technical Security Systems as a Data Source in the Process of Automatic Defense Against Cyberattacks and Detection of Crime Perpetrators,"which implies the title of the dissertation.

This dissertation focuses on the analysis and modeling of *Cyber-Physical Protection Systems (CPPS)* using artificial intelligence methods, which directly addresses the problems formulated in the research topic. This approach enables, on one hand, the assessment of the effectiveness of installed protection systems by utilizing data not only from the security systems themselves but also by taking into account the security context and estimating attributes of potential adversaries (e.g., their motivation or qualifications). On the other hand, the proposed methodology allows for planning rational, *evidence-based* strengthening of threat mitigation measures originating from both the physical sphere and cyberspace.

In this way, Electronic Security Systems (ESS) become not only an element of protective infrastructure but, above all, a rich source of data that, after appropriate analysis and modeling, forms the foundation for integrated cyber-physical defense strategies.

Identified Research Gaps

Analysis of the state of knowledge revealed five key gaps:

First, the traditional EASI (Estimated Adversary Sequence Interruption) methodology, introduced in 1977, does not account for cyber threats. Our own research showed that the classical approach indicated an 89.88% probability of attack interruption, while after accounting for cyber threats, this value dropped to 1.63%. **Second**, there is a lack of degradation models specific to Electronic Security Systems (ESS). The developed probabilistic degradation model accounts for five factors: component aging (normal distribution), adversary knowledge growth (normal distribution), technological advancement of attack tools (logarithmic model), emergence of vulnerabilities (Bernoulli process), and maintenance effects (normal distribution). Monte Carlo simulations showed that system effectiveness can drop from 98% to approximately 25% over 10 years, with the average trend line crossing the 50% level around months 75-80 of operation. **Third**, a case study demonstrated the practical consequences of ignoring degradation: classical EASI assessment indicated 88.64% effectiveness, while after accounting for degradation, the value dropped to 76.19% – a difference of 12.45 percentage points. **Fourth**, there is a lack of standardization in infrastructure element representation and automation of technical symbol detection on plans. Conven-

tional object detection models cannot handle context interpretation, where symbol meaning depends on surroundings. **Fifth**, existing solutions are fragmentary and address individual aspects of the problem; there is a lack of holistic approaches integrating all dimensions of CPPS assessment.

Thesis and Methodology

Thesis: it is possible to develop an integrated, probabilistic model for assessing CPPS effectiveness that simultaneously accounts for component degradation, cyber threats, and operational context.

The proposed solution consists of three layers: (1) perceptual/detection – contextual plan analysis with COG (Contextual Object Grouping) object detection, (2) decision-making – attack path graphs with A* algorithm and EASI modification incorporating degradation indices and cyber-resilience element, (3) reporting – automation using LLM language models.

Results and Scientific Contribution

Monte Carlo simulations demonstrated that accounting for degradation and cyber threats can significantly reduce security system effectiveness. This type of system effectiveness overestimation may not only indicate lack of economy but lead to significant consequences for critical infrastructure in case of a successful attack.

Main contributions include: (1) creation of the first probabilistic degradation model for ESS in the CPPS context, (2) extension of EASI with cyber-resilience components and component degradation, (3) new approach (COG) for contextual interpretation of technical symbols, (4) creation of a practical tool for dynamic security management. The work integrates methods from risk assessment, artificial intelligence, and cybersecurity domains into a coherent methodology supported by validation on real-world cases.

Implementation

The result of this work is a functional AI-SecPA tool implementing the complete assessment process, from detection of architectural elements through machine learning to recommendation generation using LLM. The tool appears to provide significant support in decision-making processes regarding operational and cyber-physical security management.