Inżynieria Bezpieczeństwa
Obiektów Antropogenicznych

METODYKA MODELOWANIA POZIOMU BEZPIECZEŃSTWA SYSTEMÓW OCHRONY PERYFERYJNEJ

Mirosław SIERGIEJCZYK, Adam ROSIŃSKI
Politechnika Warszawska , Warszawa

Streszczenie

Bezpieczeństwo obiektów transportowych, jako obiektów o charakterze strategicznym i zaliczanym do infrastruktury krytycznej, zależy od skuteczności zastosowanych poszczególnych systemów bezpieczeństwa. Systemy te powinny wzajemnie się uzupełnić, tak by skuteczność wykrycia zagrożenia była możliwe maksymalna przy założonych warunkach początkowych. Dlatego też stosuje się różnorodne rozwiązania. W artykule ukazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodykę modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej.
Słowa kluczowe: bezpieczeństwo, obiekty transportowe, systemy bezpieczeństwa, ochrona peryferyjna.

Abstract

Safety of transport objects, as objects of strategic character and belonging into a critical infrastructure depends on the effectiveness of used various security systems. These systems should complement each other, so that the effectiveness of threat detection was possible maximum at the assumed initial conditions. Therefore, different solutions are used. In the article is shown the use of different systems of peripheral protection for objects protection. It also presents a methodology of modelling the level of security of systems of peripheral protection.
Keys words: security, transport facilities, security systems, peripheral protection.

1. WPROWADZENIE

Według „Narodowego Programu Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej w skład infrastruktury krytycznej wchodzi 11 systemów [10]. Mają one kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli. Jednocześnie też zapewniają sprawne funkcjonowanie organów administracji publicznej, a także instytucji i przedsiębiorców. W skład infrastruktury krytycznej zaliczamy następujące systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,

- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych).

Istotną rolę wśród wymienionych systemów zajmuje transport [3,11]. Jest to przemieszczanie ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu. Przemieszczanie dóbr, ludzi i usług jest jedną z podstawowych cech charakteryzujących współczesną gospodarkę i społeczeństwo. Dlatego też sprawnie funkcjonujący system transportowy stanowi jeden z filarów nowoczesnego państwa. Zatem istotne jest zapewnienie bezpieczeństwa obiektom (zarówno stacjonarnym jak i ruchomym) wykorzystywanym w procesie transportowym [2,4,14]. W tym celu wykorzystuje się różne rozwiązania [1,9].

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej) tworzy się z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń, jako systemy [13]:

- sygnalizacji włamania i napadu,
- sygnalizacji pożaru,
- kontroli dostępu,
- monitoringu wizyjnego,
- ochrony terenów zewnętrznych.

Ochrona wynikająca z działania tych systemów może być uzupełniona przez systemy:

- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe systemy ostrzegawcze,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Najkorzystniej (z punktu widzenia zapewnienia poziomu bezpieczeństwa) jest zastosować elektroniczne systemy bezpieczeństwa i odpowiednie służby ochrony, które powiązane są między sobą poprzez odpowiednie procedury działania. W artykule ukazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodykę modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej.

2. SYSTEMY SYGNALIZACJI ZAGROŻEŃ

System Sygnalizacji Włamania i Napadu (SSWiN) ma za zadanie wykryć i zasygnalizować stan zagrożenia mienia i osób. Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", która ma jednocześnie status Polskiej Normy PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" [6], zawiera wykaz części składowych (elementów), które powinien zawierać SSWiN: centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu, zasilacz podstawowy, zasilacz rezerwowy. Centrala alarmowa stanowi „serce" systemu. Do niej przesyłane są informacje o stanie poszczególnych linii dozorowych (np. czujki), linii wyjściowych (np. obciążenia wyjść) czy dane wprowadzane przez użytkownika lub konserwatora (a wcześniej podczas instalacji systemu – instalatora) [15]. W zależności od typu centrali alarmowej informacje mogą być przesyłane bezpośrednio do płyty głównej centrali alarmowej lub też do modułów, realizujących określone funkcje (np. rozszerzeniowe wejść, rozszerzeniowe wyjść, interfejsy drukarek, itd.).

Systemy monitoringu wizyjnego (CCTV) to zespół środków technicznych i programowych przeznaczony do obserwowania, wykrywania, rejestrowania i sygnalizowania nienormalnych warunków wskazujących na istnienie

niebezpieczeństwa. W skład ich (zależnie od konfiguracji) mogą wchodzić następujące urządzenia [5]:

- kamery telewizyjne wewnętrzne lub zewnętrzne, czarno-białe lub kolorowe,
- obiektywy,
- monitory,
- cyfrowe rejestratory wizyjne,
- zasilacze (różnych mocy oraz zawierające odpowiednie zabezpieczenia [16]),
- klawiatury sterownicze,
- krosownice wizyjne.

System kontroli dostępu (SKD) zwany również systemem sterowania dostępem to zespół urządzeń i oprogramowania, które mają za zadanie [7,8]:

- identyfikację osób albo pojazdów, uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia/wyjścia,
- niedopuszczenie do przejścia przez osoby albo pojazdy nieuprawnione granicy obszaru zastrzeżonego,
- wytworzenie sygnału alarmowego informującego o próbie przejścia osoby albo pojazdu nieuprawnionego przez granicę obszaru zastrzeżonego.

Systemy ochrony terenów zewnętrznych mają za zadanie zabezpieczenie obiektów przestrzennych. Istotne staje się wykrycie ingerencji osób nieuprawnionych. Celem jest więc zminimalizowanie wpływu potencjalnych strat w przypadku wystąpienia zagrożenia dla chronionego obiektu. Wcześniejsze wykrycie miejsca takiego incydentu pozwala na szybszą interwencję służb ochrony i podjęcie racjonalnych działań zmierzających do zminimalizowania zagrożenia.

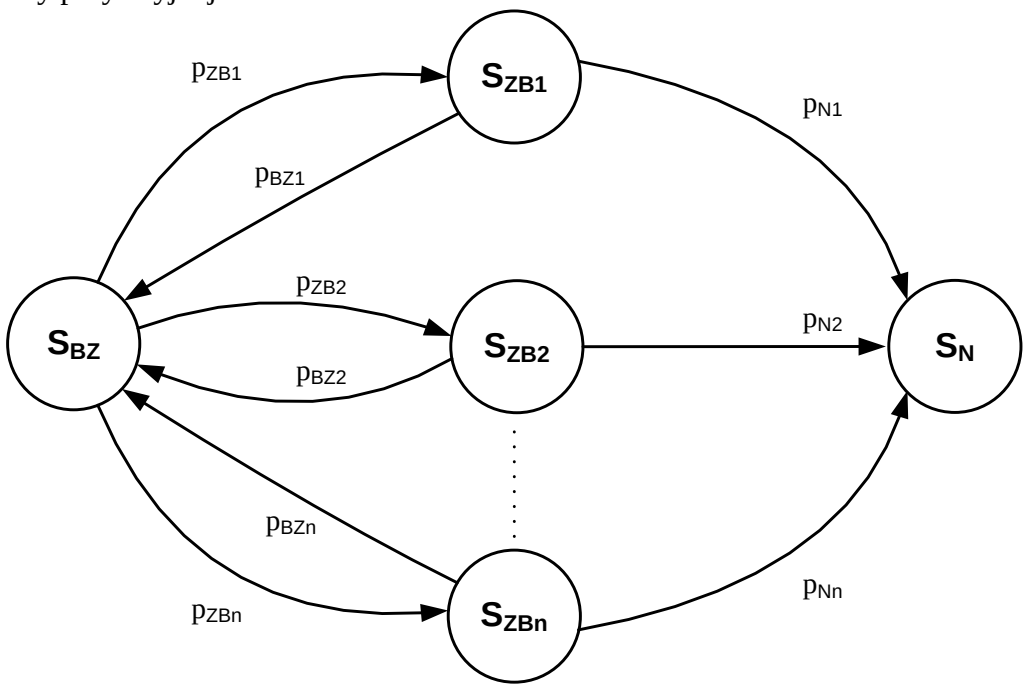
Współczesne systemy ochrony terenów zewnętrznych obiektów o specjalnym przeznaczeniu można podzielić na [12]:

- systemy ogrodzeniowe instalowane na wewnętrznym ogrodzeniu obwodnicy:
    - kablowe tryboelektryczne,
    - kablowe mikrofonowe,
    - kablowe elektromagnetyczne,
    - kablowe światłowodowe (natężeniowe i interferometryczne),
    - czujniki piezoelektryczne punktowe,
    - ogrodzenie aktywne – z wmontowanymi czujnikami mechaniczno-elektrycznymi,
- naziemne systemy ochrony zewnętrznej:
    - aktywne bariery mikrofalowe,
    - aktywne bariery podczerwieni,
    - pasywne czujki podczerwieni,
    - dualne czujki,
    - radary mikrofalowe,
    - radary laserowe,
- ziemne systemy ochrony zewnętrznej:
    - kablowe elektryczne aktywne (pole elektryczne),
    - kablowe magnetyczne pasywne (pole magnetyczne),
    - kablowe światłowodowe naciskowe,
    - kablowe elektromagnetyczne naciskowe,
    - czujniki sejsmiczne.

3. MODELOWANIE POZIOMU BEZPIECZEŃSTWA SYSTEMÓW OCHRONY PERYFERYJNEJ

Podczas opracowywania koncepcji ochrony peryferyjnej obiektów transportowych można zastosować w celu zapewnienia odpowiedniego poziomu bezpieczeństwa różne rodzaje systemów [17]. Analizując proces detekcji osób nieuprawnionych do przekroczenia granicy obszaru chronionego, można zobrazować zaistniałe sytuacje, tak jak przedstawiono to na rys. 1. Stan braku zagrożenia bezpieczeństwa S_{BZ} jest w stanem w którym systemy detekcji ochrony peryferyjnej nie wykryły zagrożenia. Stan zagrożenia bezpieczeństwa 1 S_{ZB1} jest stanem w którym pierwszy system ochrony peryferyjnej (np. system ogrodzeniowy zainstalowany na wewnętrznym ogrodzeniu obwodnicy) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu S_{BZ} do stanu S_{ZB1} z prawdopodobieństwem p_{ZB1}). Stan zagrożenia bezpieczeństwa 2 S_{ZB2} jest stanem w którym drugi system ochrony peryferyjnej (np. naziemny systemy ochrony zewnętrznej) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu S_{BZ} do stanu S_{ZB2} z prawdopodobieństwem p_{ZB2}). Stan zagrożenia bezpieczeństwa 3 S_{ZBn} jest stanem w którym n-ty system ochrony peryferyjnej (np. ziemny systemy ochrony zewnętrznej) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu S_{BZ} do stanu S_{ZBn} z prawdopodobieństwem p_{ZBn}). Będąc odpowiednio w stanach S_{ZB1} , S_{ZB2} , … , S_{ZBn} , w przypadku stwierdzenia braku zagrożenia następuje przejście do stanu S_{BZ} odpowiednio z prawdopodobieństwami równymi p_{BZ1} , p_{BZ2} , … , p_{BZn} . Jeśli system ochrony peryferyjnej znajduje się w stanie S_{ZB1} i nastąpi potwierdzenie zagrożenia przez inny system detekcji, wówczas z prawdopodobieństwem p_{N1} następuje przejście do stanu niebezpieczeństwa S_N. Jeśli system ochrony peryferyjnej znajduje się w stanie S_{ZB2} i nastąpi potwierdzenie zagrożenia przez inny system detekcji, wówczas z prawdopodobieństwem p_{N2} następuje przejście do stanu niebezpieczeństwa S_N. Jeśli system ochrony peryferyjnej znajduje się w stanie S_{ZBn} i nastąpi potwierdzenie zagrożenia przez inny system detekcji, wówczas z prawdopodobieństwem p_{Nn} następuje przejście do stanu niebezpieczeństwa S_N.

W powyższych rozważaniach założono iż przejście do stanu niebezpieczeństwa S_N jest możliwe, jeśli nastąpi wykrycie zagrożenia przez dwa niezależne systemy ochrony peryferyjnej.



Rys. 1. Relacje w systemie ochrony peryferyjnej

Dla grafu przejść przedstawionego na rys. 1 można zapisać następujące równania:

$$\begin{aligned} P_{SBZ} &= p_{BZ1} \cdot P_{SZB1} + p_{BZ2} \cdot P_{SZB2} + ... + p_{BZn} \cdot P_{SZBn} \\ P_{SZB1} &= p_{ZB1} \cdot P_{SBZ} \\ P_{SZB2} &= p_{ZB2} \cdot P_{SBZ} \\ &... \\ P_{SZBn} &= p_{ZBn} \cdot P_{SBZ} \\ P_{SN} &= p_{N1} \cdot P_{SZB1} + p_{N2} \cdot P_{SZB2} + ... + p_{Nn} \cdot P_{SZBn} \end{aligned} \tag{1}$$

Oczywiście:

$$P_{SBZ} + P_{SZB1} + P_{SZB2} + ... + P_{SZBn} + P_{SN} = 1 \tag{2}$$

Stosując odpowiednie przekształcenia matematyczne, można wyznaczyć wartości prawdopodobieństw przebywania w wyróżnionych stanach. Umożliwi to ocenę skuteczności funkcjonowania zaproponowanego rozwiązania, a zarazem także pozwala na modelowanie poziomu bezpieczeństwa systemów ochrony peryferyjnej. Możliwe jest zatem także wykorzystanie proponowanej metodologii analizy funkcjonowania systemów ochrony peryferyjnej do porównania różnego rodzaju rozwiązań i wyboru optymalnego przy założonych warunkach początkowych.

4. PODSUMOWANIE I WNIOSKI

Podsumowując zaprezentowane rozwiązania można stwierdzić, iż istnieje bardzo wiele różnorodnych systemów ochrony peryferyjnej, które pozwalają na zwiększenie poziomu bezpieczeństwa obiektów transportowych. Ponieważ są one zaliczane do infrastruktury krytycznej, to powinno stosować się różne środki techniczne i organizacyjne w celu ochrony przed różnymi zagrożeniami. W artykule ukazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodykę modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej. W dalszych badaniach planuje się uwzględnienie kosztów wdrożenia poszczególnych rozwiązań z zakresu systemów ochrony peryferyjnej.

Literatura

1. Balejko M., Rosiński A., *Bezpieczeństwo w porcie lotniczym*. XXVII Międzynarodowa Konferencja Naukowo – Techniczna EKOMILITARIS 2013, Zakopane 2013.
2. Fischer, Halibozek, Walters: *Introduction to Security*. Butterworth-Heinemann, 2012.
3. Fries R., Chowdhury M., Brummond J.: *Transportation infrastructure security utilizing inteligent transportation systems*. John Wiley & Sons, New Jersey 2009.
4. Hołyst B., *Terroryzm. Tom 1 i 2*. Wydawnictwa Prawnicze LexisNexis, Warszawa, 2011.
5. Kałużny P., *Telewizyjne systemy dozorowe*. WKiŁ, Warszawa, 2008.
6. Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
7. Norma PN-EN 50133-1:2007 - Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe.
8. Paś J., Systemy biometryczne w transporcie – wymagania. *Logistyka* nr **6/2011**.
9. Rozporządzenie Komisji (UE) nr 185/2010 z dnia 4 marca 2010 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych norm ochrony lotnictwa cywilnego.

10. Rządowe Centrum Bezpieczeństwa: „Narodowy program ochrony infrastruktury krytycznej. Załącznik 1: Charakterystyka systemów infrastruktury krytycznej". Warszawa 2013.
11. Siergiejczyk M., Gago S., *Public Safety Issues in Rail Transport*. Polish Journal of Environmental Studies. ISSN 1230-1485.Vol 17, No 3C (2008). HARD Publishing Company, Olsztyn 2008.
12. Siergiejczyk M., Rosiński A., Systemy ochrony peryferyjnej obiektów transportowych infrastruktury krytycznej. *Technika Transportu Szynowego* nr **10/2013**.
13. Siergiejczyk M., Rosiński A., *Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego*. Monografia „Rewaluacja bezpieczeństwa publicznego" pod redakcją naukową Tadeusza Zaborowskiego. Wydawca: Instytut Badań i Ekspertyz Naukowych w Gorzowie Wlkp., Gorzów Wlkp. 2011.
14. Siergiejczyk M., Rosiński A., *Zagrożenia podczas podróży w transporcie kolejowym*. Monografia „SATORI w publicznym bezpieczeństwie" pod redakcją naukową Tadeusza Zaborowskiego. Wydawca: Instytut Badań i Ekspertyz Naukowych w Gorzowie Wlkp., Gorzów Wlkp. 2012.
15. Siergiejczyk M., Rosiński A.: Reliability analysis of electronic protection systems using optical links. Monografia „Dependable Computer Systems" pod redakcją Wojciecha Zamojskiego, Janusza Kacprzyka, Jacka Mazurkiewicza, Jarosława Sugiera i Tomasza Walkowiaka, wydana jako monograficzna seria wydawnicza – „Advances in intelligent and soft computing", Vol. 97. Wydawca: Springer-Verlag, Berlin Heidelberg 2011.
16. Siergiejczyk M., Rosiński A.: Reliability analysis of power supply systems for devices used in transport telematic systems. Monografia „Modern Transport Telematics" pod redakcją Jerzego Mikulskiego, wydana jako monograficzna seria wydawnicza – „Communications in Computer and Information Science", Vol. 239. Wydawca: Springer-Verlag, Berlin Heidelberg 2011.
17. Szulc W., Rosiński A., *Metody ochrony obwodowej obiektów*. XXIV Międzynarodowa Konferencja Naukowo – Techniczna EKOMILITARIS 2010, Zakopane 2010.