Biuletyn WAT
Vol. LXIV, Nr 2, 2015

# Metoda modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej

MIROSŁAW SIERGIEJCZYK, ADAM ROSIŃSKI

Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie,
00-662 Warszawa, ul. Koszykowa 75, adro@wt.pw.edu.pl

**Streszczenie.** Bezpieczeństwo obiektów transportowych, jako obiektów o charakterze strategicznym i zaliczanych do infrastruktury krytycznej, zależy od skuteczności zastosowanych poszczególnych systemów bezpieczeństwa. Powinny one wzajemnie się uzupełniać, tak by skuteczność wykrycia zagrożenia była możliwie maksymalna przy założonych warunkach początkowych. Dlatego też stosuje się różnorodne rozwiązania. W artykule pokazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodę modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej.
**Słowa kluczowe:** ochrona peryferyjna, infrastruktura krytyczna, modelowanie
**DOI:** 10.5604/12345865.1157222

## 1. Wprowadzenie

Według „Narodowego Programu Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej w skład infrastruktury krytycznej wchodzi jedenaście systemów [11]. Mają one kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli. Jednocześnie 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 [2, 4, 12]. 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 [3, 5, 15]. W tym celu wykorzystuje się różne rozwiązania [1, 10].

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej) tworzy się z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń, jako systemy [14]:
— 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,
— zapobiegające kradzieżom,
— dźwiękowe systemy ostrzegawcze,
— zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Najkorzystniejsze (z punktu widzenia zapewnienia poziomu bezpieczeństwa) jest zastosowanie elektronicznych systemów bezpieczeństwa i odpowiednie służby ochrony, które powiązane są między sobą odpowiednimi procedurami działania. W artykule ukazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodę modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej.

## 2. Systemy sygnalizacji zagrożeń

System Sygnalizacji Włamania i Napadu (SSWiN) ma 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" [7], obejmuje 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) [16]. 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 warunków wskazujących na istnienie zagrożenia. W ich skład (zależnie od konfiguracji) mogą wchodzić następujące urządzenia [6]:

- kamery telewizyjne wewnętrzne lub zewnętrzne, czarno-białe lub kolorowe,
- obiektywy,
- monitory,
- cyfrowe rejestratory wizyjne,
- zasilacze (różnych mocy oraz zawierające odpowiednie zabezpieczenia [17]),
- klawiatury sterownicze,
- krosownice wizyjne.

System kontroli dostępu (SKD), zwany również systemem sterowania dostępem, to zespół urządzeń i oprogramowania, które mają za zadanie [8,9]:

- 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 zabezpieczać obiekty przestrzenne. Istotne jest tu 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 [13]:

— 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.

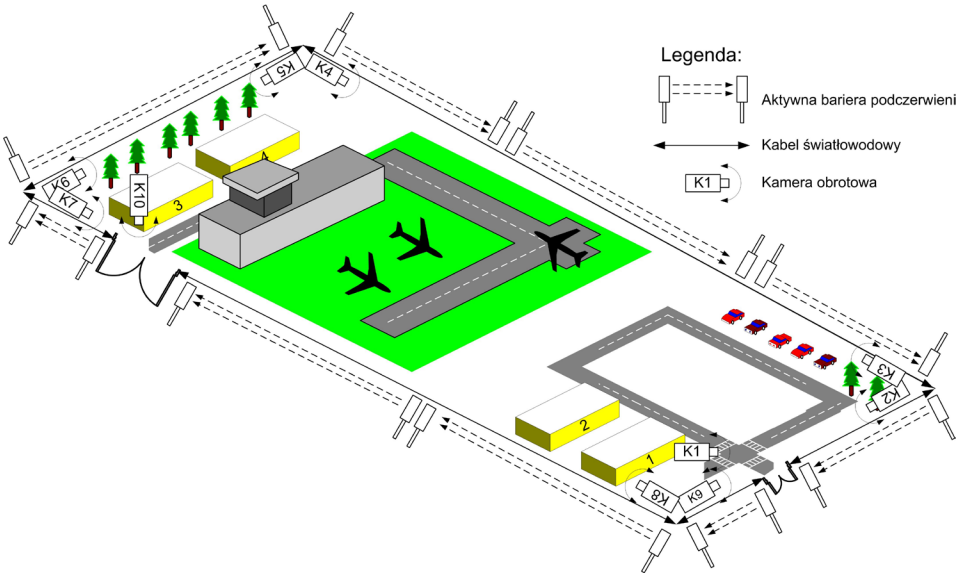
Wymienione powyżej rozwiązania stosowane w systemach ochrony terenów zewnętrznych znajdują także zastosowanie w obiektach transportowych. Dotyczy to w szczególności rozległych obiektów, które są używane w procesach transportowych (np. porty lotnicze, stacje kolejowe, metro, bazy logistyczne, terminale przeładunkowe).

## 3. Modelowanie poziomu bezpieczeństwa systemów ochrony peryferyjnej

Na rysunku 1 zaprezentowano hipotetyczny port lotniczy. Jest to teren, na którym rozmieszczone są różnego rodzaju obiekty budowlane wykorzystywane podczas procesu transportowego. Ze względu na rozległość obszaru, jaki zajmuje port lotniczy, i zagrożenia, które mogą wystąpić, powinien on być dobrze chroniony. Dlatego też tak istotne jest wykrycie intruza przekraczającego ogrodzenie. W tym celu stosuje się systemy ochrony peryferyjnej. Pozwala to na wykrycie osób nieuprawnionych

(które chciałyby się dostać na teren portu lotniczego) już w chwili przekraczania granicy obszaru chronionego. W zaprezentowanym przykładzie zastosowano trzy różnego rodzaju systemy bezpieczeństwa:

— aktywne bariery podczerwieni,
— kabel światłowodowy,
— monitoring wizyjny.

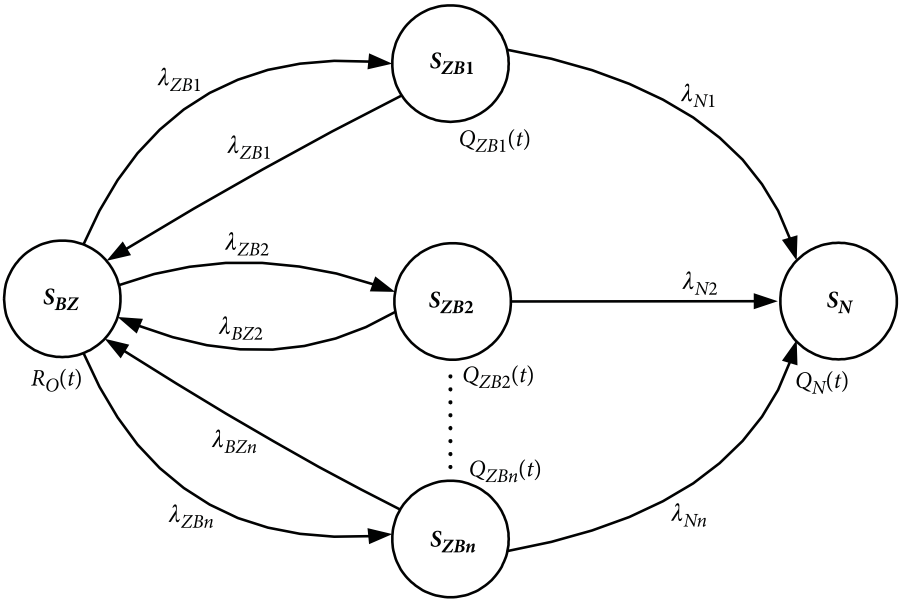



Rys. 1. Widok portu lotniczego z zastosowanymi systemami bezpieczeństwa

W rzeczywistych obiektach stosuje się różnego rodzaju systemy, które zostały przedstawione w poprzednim rozdziale.

Podczas opracowywania koncepcji ochrony peryferyjnej obiektów transportowych można zastosować, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, różne rodzaje systemów [18]. Analizując proces detekcji osób nieuprawnionych do przekroczenia granicy obszaru chronionego, można zobrazować zaistniałe sytuacje, tak jak przedstawiono to na rysunku 2. Stan braku zagrożenia bezpieczeństwa $S_{BZ}$ jest stanem, w którym systemy detekcji ochrony peryferyjnej nie wykrywają 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 intensywnością $\lambda_{ZB1}$). Stan zagrożenia bezpieczeństwa 2 $S_{ZB2}$ jest stanem, w którym drugi system ochrony peryferyjnej (np. naziemny system ochrony zewnętrznej) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu $S_{BZ}$ do stanu $S_{ZB2}$ z intensywnością $\lambda_{ZB2}$). Stan zagrożenia

bezpieczeństwa $n$ $S_{ZBn}$ jest stanem, w którym $n$-ty system ochrony peryferyjnej (np. ziemny system ochrony zewnętrznej) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu $S_{BZ}$ do stanu $S_{ZBn}$ z intensywnością $\lambda_{ZBn}$). Będąc odpowiednio w stanach $S_{ZB1}$, $S_{ZB2}$, …, $S_{ZBn}$, w przypadku stwierdzenia braku zagrożenia przez wykryty przez dany system ochrony peryferyjnej obiekt następuje powrót do stanu $S_{BZ}$ odpowiednio z intensywnościami równymi $\lambda_{BZ1}$, $\lambda_{BZ2}$, …, $\lambda_{BZn}$. Jeśli system ochrony peryferyjnej znajduje się w stanie $S_{ZB1}$ i nastąpi potwierdzenie zagrożenia przez inny system detekcji, wówczas z intensywnością $\lambda_{N1}$ 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 intensywnością $\lambda_{N2}$ 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 intensywnością $\lambda_{Nn}$ następuje przejście do stanu niebezpieczeństwa $S_N$.




Rys. 2. Relacje w systemie ochrony peryferyjnej. Oznaczenia na rysunku: $R_O(t)$ — funkcja prawdopodobieństwa przebywania systemu w stanie braku zagrożenia bezpieczeństwa $S_{BZ}$; $Q_{ZBn}(t)$ — funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa $S_{ZBn}$; $Q_N(t)$ — funkcja prawdopodobieństwa przebywania systemu w stanie niebezpieczeństwa $S_N$; $\lambda_{ZB1}$ — intensywność wykrycia potencjalnego zagrożenia przez pierwszy system ochrony peryferyjnej; $\lambda_{ZBn}$ — intensywność wykrycia potencjalnego zagrożenia przez $n$-ty system ochrony peryferyjnej; $\lambda_{BZ1}$ — intensywność stwierdzenia braku zagrożenia ze strony obiektu wykrytego przez pierwszy system ochrony peryferyjnej; $\lambda_{BZn}$ — intensywność stwierdzenia braku zagrożenia ze strony obiektu wykrytego przez $n$-ty system ochrony peryferyjnej; $\lambda_{N1}$ — intensywność potwierdzenia zagrożenia przez inny (niż pierwszy) system ochrony peryferyjnej; $\lambda_{Nn}$ — intensywność potwierdzenia zagrożenia przez inny (niż $n$-ty) system ochrony peryferyjnej

W powyższych rozważaniach założono, że przejście do stanu niebezpieczeństwa $S_N$ następuje, gdy pojawia się wykrycie zagrożenia przez dwa niezależne systemy ochrony peryferyjnej.

System przedstawiony na rysunku 2 może być opisany następującymi równaniami Kołmogorowa-Chapmana:

$$\begin{aligned}
R_0^{'}(t) &= -\lambda_{ZB1} \cdot R_0(t) + \lambda_{BZ1} \cdot Q_{ZB1}(t) - \lambda_{ZB2} \cdot R_0(t) + \lambda_{BZ2} \cdot Q_{ZB2}(t) + \ldots \\
&\quad - \lambda_{ZBn} \cdot R_0(t) + \lambda_{BZn} \cdot Q_{ZBn}(t) \\
Q_{ZB1}^{'}(t) &= \lambda_{ZB1} \cdot R_0(t) - \lambda_{BZ1} \cdot Q_{ZB1}(t) - \lambda_{N1} \cdot Q_{ZB1}(t) \\
Q_{ZB2}^{'}(t) &= \lambda_{ZB2} \cdot R_0(t) - \lambda_{BZ2} \cdot Q_{ZB2}(t) - \lambda_{N2} \cdot Q_{ZB2}(t) \\
&\ldots \\
Q_{ZBn}^{'}(t) &= \lambda_{ZBn} \cdot R_0(t) - \lambda_{BZn} \cdot Q_{ZBn}(t) - \lambda_{Nn} \cdot Q_{ZBn}(t) \\
Q_N^{'}(t) &= \lambda_{N1} \cdot Q_{ZB1}(t) + \lambda_{N2} \cdot Q_{ZB2}(t) + \ldots + \lambda_{Nn} \cdot Q_{ZBn}(t)
\end{aligned} \tag{1}$$

gdzie: $R_0^{'}(t)$ — pochodna prawdopodobieństwa przebywania systemu w stanie braku zagrożenia bezpieczeństwa;
$Q_{ZBn}^{'}(t)$ — pochodna prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa;
$Q_N^{'}(t)$ — pochodna prawdopodobieństwa przebywania systemu w stanie niebezpieczeństwa.

Intensywności przejść można oszacować w oparciu o prawdopodobieństwa poszczególnych zdarzeń. Zatem znając wartość prawdopodobieństwa wykrycia potencjalnego zagrożenia przez określony podsystem ochrony peryferyjnej $R_{ZB}$, można oszacować intensywność przejść ze stanu braku zagrożenia bezpieczeństwa do stanu zagrożenia bezpieczeństwa. Zakładając najprostszy, wykładniczy model tego procesu, możemy wykorzystać następującą zależność:

$$R_{ZB}(t) = e^{-\lambda_{ZB}t} \text{ dla } t \geq 0,$$

więc

$$\lambda_{ZB} = -\frac{\ln R_{ZB}(t)}{t}.$$

Przykładowo, dla $t$ = 8760 [h] i $R_{ZB1}(t)$ = 0,95, otrzymujemy:

$$\lambda_{ZB} = -\frac{\ln R_{ZB}(t)}{t} = -\frac{\ln 0{,}95}{8760} = 5{,}855398 \cdot 10^{-6} \left[\frac{1}{\text{h}}\right].$$

Przyjmując warunki początkowe:

$$R_0(0) = 1$$
$$Q_{ZB1}(0) = Q_{ZB2}(0) = ... = Q_{ZBn}(0) = Q_B(0) = 0. \tag{2}$$

oraz stosując odpowiednie przekształcenia matematyczne (m.in. przekształcenie Laplace'a), można wyznaczyć wartości prawdopodobieństw przebywania w wyróżnionych stanach. Umożliwia to ocenę skuteczności funkcjonowania zaproponowanego rozwiązania, a zarazem pozwala na modelowanie poziomu bezpieczeństwa systemów ochrony peryferyjnej. Możliwe jest zatem wykorzystanie proponowanej metody analizy funkcjonowania systemów ochrony peryferyjnej do porównania różnego rodzaju rozwiązań i wyboru wariantu optymalnego przy założonych warunkach początkowych.

## 4. Podsumowanie i wnioski

Istnieje wiele różnorodnych systemów ochrony peryferyjnej, które pozwalają na zwiększenie poziomu bezpieczeństwa obiektów transportowych. Ponieważ są one zaliczane do infrastruktury krytycznej, to powinno się stosować różne środki techniczne i organizacyjne w celu ochrony przed zagrożeniami. W artykule pokazano wykorzystanie różnego rodzaju systemów ochrony peryferyjnej do ochrony obiektów. Zaprezentowano także metodę liczbowego oszacowania poziomu bezpieczeństwa systemów ochrony peryferyjnej. W dalszych badaniach planuje się uwzględnienie kosztów wdrożenia poszczególnych rozwiązań z zakresu systemów ochrony peryferyjnej.

Artykuł opracowany na podstawie referatu prezentowanego na XXVIII Międzynarodowej Konferencji Naukowo-Technicznej „Ekomilitaris 2014", Zakopane 9-12.09.2014 r.

*Artykuł wpłynął do redakcji 19.11.2014 r. Zweryfikowaną wersję po recenzji otrzymano 18.01.2015 r.*

LITERATURA

[1] Balejko M., Rosiński A., *Bezpieczeństwo w porcie lotniczym*, XXVII Międzynarodowa Konferencja Naukowo-Techniczna EKOMILITARIS 2013, Zakopane, 2013.

[2] Dyduch J., Paś J., Rosiński A., *Podstawy eksploatacji transportowych systemów elektronicznych*, Wydawnictwo Politechniki Radomskiej, Radom, 2011.

[3] Fischer R.J., Halibozek E.P., Walters D., *Introduction to Security*, Butterworth-Heinemann, 2012.

[4] Fries R., Chowdhury M., Brummond J., *Transportation infrastructure security utilizing inteligent transportation systems*, John Wiley & Sons, New Jersey, 2009.

[5] Hołyst B., *Terroryzm*, tom 1 i 2, Wydawnictwa Prawnicze LexisNexis, Warszawa, 2011.

[6] Kałużny P., *Telewizyjne systemy dozorowe*, WKiŁ, Warszawa, 2008.

[7] Norma PN-EN 50131-1:2009: *Systemy alarmowe — Systemy sygnalizacji włamania i napadu — Wymagania systemowe*.

[8] Norma PN-EN 50133-1:2007 — *Systemy alarmowe — Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia*, Część 1. *Wymagania systemowe*.

[9] Paś J., *Systemy biometryczne w transporcie — wymagania*, Logistyka nr 6, 2011.

[10] 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.

[11] Rządowe Centrum Bezpieczeństwa: *Narodowy program ochrony infrastruktury krytycznej*, Załącznik 1. Charakterystyka systemów infrastruktury krytycznej, Warszawa, 2013.

[12] Siergiejczyk M., Gago S., *Public Safety Issues in Rail Transport*, Polish Journal of Environmental Studies, vol. 17, no 3C, HARD Publishing Company, Olsztyn, 2008.

[13] Siergiejczyk M., Rosiński A., *Systemy ochrony peryferyjnej obiektów transportowych infrastruktury krytycznej*, Technika Transportu Szynowego, 10, 2013.

[14] Siergiejczyk M., Rosiński A., *Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego*, [w:] „Rewaluacja bezpieczeństwa publicznego", [red. nauk.] T. Zaborowski, Instytut Badań i Ekspertyz Naukowych, Gorzów Wlkp., 2011.

[15] Siergiejczyk M., Rosiński A., *Zagrożenia podczas podróży w transporcie kolejowym*, [w:] „SATORI w publicznym bezpieczeństwie", [red. nauk.] T. Zaborowski, Instytut Badań i Ekspertyz Naukowych, Gorzów Wlkp., 2012.

[16] Siergiejczyk M., Rosiński A., *Reliability analysis of electronic protection systems using optical links*, [w:] „Dependable Computer Systems", [red.] W. Zamojski, J. Kacprzyk, J. Mazurkiewicz, J. Sugier i T. Walkowiak, „Advances in intelligent and soft computing", vol. 97, Springer-Verlag, Berlin–Heidelberg, 2011.

[17] Siergiejczyk M., Rosiński A., *Reliability analysis of power supply systems for devices used in transport telematic systems*, [w:] „Modern Transport Telematics", [red.] J. Mikulski, „Communications in Computer and Information Science", vol. 239, Springer-Verlag, Berlin–Heidelberg, 2011.

[18] Szulc W., Rosiński A., *Metody ochrony obwodowej obiektów*, XXIV Międzynarodowa Konferencja Naukowo-Techniczna EKOMILITARIS 2010, Zakopane, 2010.

M. SIERGIEJCZYK, A. ROSIŃSKI

## Methodology of modelling the level of security of systems of peripheral protection

**Abstract.** Safety of transport objects, as objects of strategic character and belonging to a critical infrastructure depends on the effectiveness of the 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 it 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.

**Keywords:** peripheral protection, critical infrastructure, modelling