Modelowanie poziomu bezpieczeństwa trójrodzajowych systemów ochrony peryferyjnej na przykładzie obiektów kolejowych

Mirosław SIERGIEJCZYK[1], Jerzy CHMIEL[2], Adam ROSIŃSKI[3]

Streszczenie
Nadrzędnym celem stosowania systemów ochrony peryferyjnej obiektów kolejowych jest zwiększenie poziomu bezpieczeństwa. System transportowy, zaliczany do infrastruktury krytycznej, wymaga szczególnej ochrony. Przeanalizowano proces detekcji osób nieuprawnionych przekraczających granicę obszaru chronionego i przeprowadzono analizę trójrodzajowego systemu ochrony peryferyjnej. Umożliwiło to graficzne przedstawienie zaistniałych sytuacji, jako relacji w systemie ochrony peryferyjnej i opisano systemy ochrony peryferyjnej układem równań Kołmogorowa-Chapmana. Dzięki temu jest możliwe oszacowanie liczbowe poziomu bezpieczeństwa zastosowanych rozwiązań systemów ochrony peryferyjnej.

Słowa kluczowe: bezpieczeństwo, modelowanie, ochrona peryferyjna

1. Wstęp

W dokumencie opracowanym przez Rządowe Centrum Bezpieczeństwa pt. „Narodowy Program Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej [15] wymieniono 11 następujących systemów, zaliczanych do infrastruktury krytycznej:

- 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).

Systemy te mają kluczowe znaczenie dla bezpieczeństwa funkcjonowania Polski, zarówno w aspekcie ciągłości działania struktur administracyjnych, jak też ochrony obywateli przed różnego rodzaju zagrożeniami. W skład infrastruktury krytycznej jest zaliczany m.in. transport, przy czym wyróżniono w nim następujące rodzaje transportu: kolejowy, samochodowy, lotniczy, rurociągowy, żeglugę śródlądową i morską. Istotne jest zatem zapewnienie odpowiedniego poziomu bezpieczeństwa obiektom transportowym, w tym kolejowym (zarówno stacjonarnym, jak i ruchomym). W tym celu wykorzystuje się różne rozwiązania techniczne [2, 6, 23], w tym systemy ochrony peryferyjnej.

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej) tworzy się z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń:

- sygnalizacji włamania i napadu [11, 25],
- sygnalizacji pożaru,
- kontroli dostępu,
- monitoringu wizyjnego [7],
- 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.

[1] Prof. PW, dr hab. inż.; Politechnika Warszawska Wydział Transportu; e-mail: msi@wt.pw.edu.pl.
[2] Dr inż.; Politechnika Warszawska Wydział Transportu; e-mail: jhc@wt.pw.edu.pl.
[3] Dr hab.inż.; Wojskowa Akademia Techniczna Wydział Elektroniki; e-mail: adam.rosinski@wat.edu.pl.

Jednym z ważniejszych systemów jest system ochrony terenów zewnętrznych, umożliwiający wykrycie i zlokalizowanie osób nieuprawnionych, które przekraczają granicę obszaru zastrzeżonego. Na terenach kolejowych, które charakteryzują się dużą rozległością terytorialną, jest wskazane stosowanie tego rodzaju elektronicznych systemów bezpieczeństwa, gdyż wówczas będzie możliwe podjęcie racjonalnych działań, które zminimalizują skutki potencjalnych uszkodzeń, sabotaży lub aktów terrorystycznych. W artykule opisano różne rodzaje systemów ochrony peryferyjnej, które mogą być zastosowane w celu ochrony kolejowych obiektów transportowych. Zaprezentowano także metodę modelowania poziomu bezpieczeństwa trójrodzajowego systemu ochrony peryferyjnej, z uwzględnieniem poziomów zagrożenia.

2. Systemy ochrony peryferyjnej

W przypadku wykrycia zagrożenia w kolejowych obiektach transportowych, podjęcie racjonalnych działań wymaga wczesnego wykrycia zagrożenia [5, 8, 21], dlatego istotne jest dokładne zlokalizowanie miejsca wykrycia osoby nieuprawnionej, która przekroczyła granicę obszaru zastrzeżonego. Takie podejście pozwala na zminimalizowanie ewentualnych szkód, które mogą wystąpić na skutek działań intruza. Opracowano wiele metod ochrony peryferyjnej obiektów [20, 22], wykorzystano w nich różne prawa i właściwości zjawisk fizycznych. Wybór określonego rozwiązania może zależeć m.in. od:

- czynników środowiskowych, jak np.: nasłonecznienie, opady deszczu i śniegu, mgła, zakłócenia elektromagnetyczne [12], zapylenie [10], wibracje [1],
- warunków instalacyjnych: miejsce instalowania urządzeń, wytyczne zawarte w dokumentacji instalatora, zapewnienie dostępu służb serwisowych, dostęp do sieci zasilających [9],
- wymagań zawartych w obowiązujących przepisach i rozporządzeniach oraz wytycznych w zakresie ochrony danego obszaru: np. normy opublikowane przez Polski Komitet Normalizacyjny, normy obronne opublikowane przez Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji, wymagania zawarte w instrukcjach opracowanych przez PKP Polskie Linie Kolejowe,
- wymagań inwestora i użytkownika: np. koszty urządzeń i ich instalacji, niezawodność [16, 17, 19] a także późniejsza eksploatacja [4, 13, 14], wewnętrzne procedury bezpieczeństwa w ochranianym obiekcie.

Współczesne systemy ochrony peryferyjnej obiektów o specjalnym przeznaczeniu (w tym baz logistycznych) można podzielić na [3, 24]:

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 rozwiązania stosowane w systemach ochrony terenów zewnętrznych, znajdują także zastosowanie w kolejowych obiektach transportowych. Dotyczy to w szczególności rozległych obiektów, które są wykorzystywane w procesach transportowych (np. stacje kolejowe, kolejowe przejścia graniczne).

Do ziemnych systemów ochrony zewnętrznej zaliczany jest m.in. kabel światłowodowy. Najczęściej jest on stosowany jako medium transmisyjne wykorzystywane do budowy sieci telekomunikacyjnych. Ze względu na swoje właściwości, może być także wykorzystany jako element detekcyjny systemu ochrony peryferyjnej. Wykrywa wówczas nacisk lub wibracje, które są powodowane przez osobę nieuprawnioną przekraczającą granicę obszaru zastrzeżonego. Jedną z zalet stosowania tego rozwiązania w ochronie peryferyjnej kolejowych obiektów transportowych jest całkowita odporność na zakłócenia elektromagnetyczne. Dzięki temu, że nie przewodzi elektrycznego sygnału, można go bezpiecznie stosować w pobliżu linii energetycznych zasilających urządzenia kolejowe [18]. Do wad tego rozwiązania należy zaliczyć m.in.: koszt instalacji związany z drogimi pracami ziemnymi, koszt urządzeń oraz koszt ewentualnych napraw uszkodzeń kabla światłowodowego.

Do naziemnych systemów ochrony zewnętrznej zaliczane są m.in. aktywne bariery podczerwieni. W ich skład wchodzą dwie części: nadawcza i odbiorcza. Nadajnik emituje promieniowanie podczerwone, które jest odbierane przez odbiornik. Pojedynczy nadajnik i odbiornik stanowią tzw. tor podczerwieni. Kilka takich torów ustawionych w jednej linii tworzy

tzw. barierę podczerwieni – przeważnie jest to od 2 do 16 wiązek. Zasięgi działania zewnętrznych barier podczerwieni wynoszą od kilkunastu do około kilkuset metrów (jest to uzależnione od warunków atmosferycznych, np. opady śniegu, deszczu). Jako kryterium alarmu stosuje się często wymóg przerwania dwóch wiązek (np. sąsiadujących ze sobą) w określonym czasie – pozwala to na uniknięcie fałszywych alarmów związanych z przelatującymi ptakami lub spadającymi w okresie jesiennym liśćmi z drzew.

Do naziemnych systemów ochrony zewnętrznej zaliczany jest m.in. system monitoringu wizyjnego (ang. CCTV – *Closed Circuit TeleVision*). Jest to zespół środków technicznych i programowych przeznaczony do obserwowania, wykrywania, rejestrowania i sygnalizowania różnego rodzaju warunków wskazujących na istnienie niebezpieczeństwa. W ich skład (zależnie od konfiguracji i rodzaju systemu) mogą wchodzić następujące urządzenia:

- kamery telewizyjne wewnętrzne lub zewnętrzne,
- obiektywy,
- monitory,
- urządzenia rejestrujące,
- media transmisyjne,
- układy zasilania,
- klawiatury sterownicze,
- inne (np. krosownice wizyjne, oświetlacze podczerwieni).

Każde z wymienionych rozwiązań ma określone zalety i wady, dlatego bardzo często stosuje się systemy ochrony peryferyjnej, w których skład wchodzą różne pojedyncze systemy. Z analizy opisanych systemów wynika, że dobre właściwości ma zintegrowany system bezpieczeństwa, w którym do detekcji intruzów zastosowano trzy spośród wymienionych systemów: kabel światłowodowy, aktywna bariera podczerwieni i system monitoringu wizyjnego. Ich współdziałanie pozwala zwiększyć prawdopodobieństwo wykrycia intruza. Oczywiście należy także pamiętać o odpowiednich służbach ochrony (np. Straż Ochrony Kolei) i procedurach reakcji w sytuacji wystąpienia zagrożenia.

3. Modelowanie poziomu bezpieczeństwa trójrodzajowych systemów ochrony peryferyjnej

Do modelowania poziomu bezpieczeństwa trójrodzajowych systemów ochrony peryferyjnej kolejowych obiektów transportowych, wybrano następujące systemy:

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

W rzeczywistych obiektach stosuje się także innego rodzaju systemy wymienione w poprzednim rozdziale. Zaprezentowane rozważania można także zastosować do innych rodzajów systemów ochrony peryferyjnej.

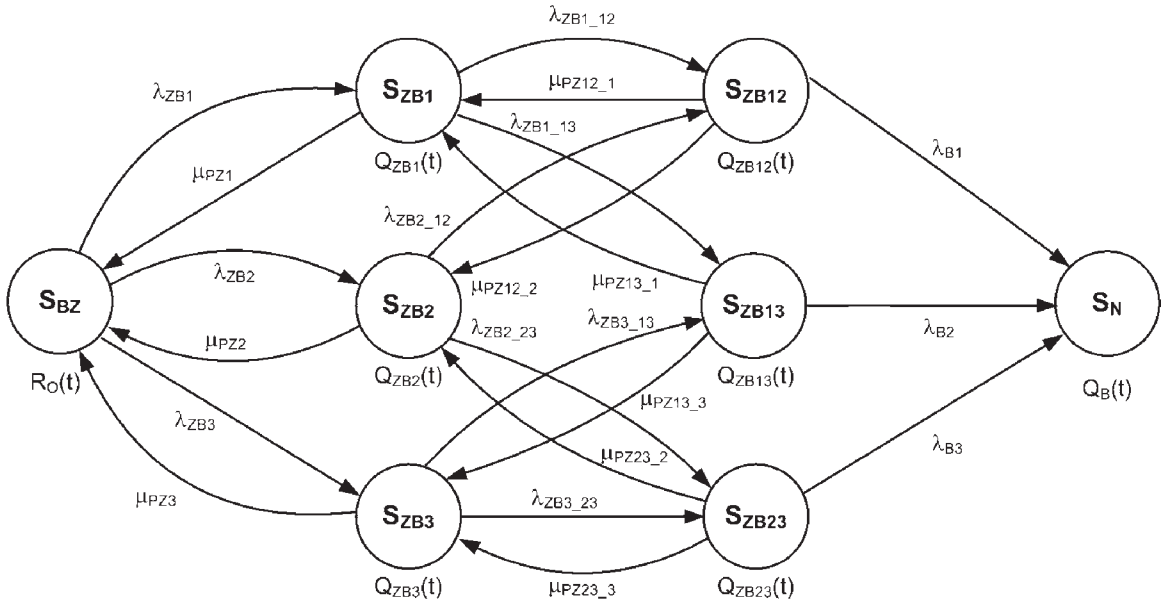
Analizując funkcjonowanie trójrodzajowego systemu ochrony peryferyjnej, można stwierdzić, iż zachodzące w nim relacje mogą być zobrazowane jak na rysunku 1.

Stan braku zagrożenia bezpieczeństwa S_{BZ} jest stanem, w którym prawidłowo funkcjonują wszystkie trzy podsystemy ochrony peryferyjnej, czyli: kabel światłowodowy, aktywne bariery podczerwieni, monitoring wizyjny. Stan zagrożenia bezpieczeństwa S_{ZB1} jest stanem, w którym kabel światłowodowy jest niezdatny. Stan zagrożenia bezpieczeństwa S_{ZB2} jest stanem, w którym aktywne bariery podczerwieni są niezdatne. Stan zagrożenia bezpieczeństwa S_{ZB3} jest stanem, w którym monitoring wizyjny jest niezdatny. Stan zagrożenia bezpieczeństwa S_{ZB12} jest stanem, w którym zarówno kabel światłowodowy, jak i aktywne bariery podczerwieni są niezdatne. Stan zagrożenia bezpieczeństwa S_{ZB13} jest stanem, w którym zarówno kabel światłowodowy, jak i monitoring wizyjny są niezdatne. Stan zagrożenia bezpieczeństwa S_{ZB23} jest stanem, w którym aktywne bariery podczerwieni i monitoring wizyjny są niezdatne. Stan niebezpieczeństwa S_N jest stanem, w którym wszystkie trzy podsystemy ochrony peryferyjnej są niezdatne.

Gdy system jest w stanie braku zagrożenia bezpieczeństwa S_{BZ}, w przypadku uszkodzenia kabla światłowodowego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB1} z intensywnością l_{ZB1}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB1}, jest możliwe przejście do stanu braku zagrożenia bezpieczeństwa S_{BZ} w przypadku podjęcia działań polegających na przywróceniu stanu zdatności kablowi światłowodowemu.

Gdy system jest w stanie braku zagrożenia bezpieczeństwa S_{BZ}, w przypadku uszkodzenia aktywnych barier podczerwieni następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB2} z intensywnością l_{ZB2}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB2} możliwe jest przejście do stanu braku zagrożenia bezpieczeństwa S_{BZ} w przypadku podjęcia działań polegających na przywróceniu stanu zdatności aktywnym barierom podczerwieni.

Gdy system jest w stanie braku zagrożenia bezpieczeństwa S_{BZ}, w przypadku uszkodzenia monitoringu wizyjnego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB3} z intensywnością l_{ZB3}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB3} możliwe jest przejście do stanu braku zagrożenia bezpieczeństwa S_{BZ} w przypadku podjęcia działań polegających na przywróceniu stanu zdatności monitoringowi wizyjnemu.



Rys. 1. Relacje w trójrodzajowym systemie ochrony peryferyjnej [źródło: opracowanie własne]; opis oznaczeń:
$R_O(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie braku zagrożenia bezpieczeństwa S_{BZ},
$Q_{ZBi}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa S_{ZBi}, gdzie „i" oznacza numer stanu; $i \in \{1,2,3,12,13,23\}$,
$Q_B(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie niebezpieczeństwa S_N,
t – czas,
l_{ZB1} – intensywność przejść ze stanu braku zagrożenia bezpieczeństwa S_{BZ} do stanu zagrożenia bezpieczeństwa S_{ZB1},
m_{ZB1} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB1} do stanu braku zagrożenia bezpieczeństwa S_{BZ},
l_{ZB2} – intensywność przejść ze stanu braku zagrożenia bezpieczeństwa S_{BZ} do stanu zagrożenia bezpieczeństwa S_{ZB2},
m_{ZB2} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB2} do stanu braku zagrożenia bezpieczeństwa S_{BZ},
l_{ZB3} – intensywność przejść ze stanu braku zagrożenia bezpieczeństwa S_{BZ} do stanu zagrożenia bezpieczeństwa S_{ZB3},
m_{ZB3} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB3} do stanu braku zagrożenia bezpieczeństwa S_{BZ},
l_{ZB1_12} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB1} do stanu zagrożenia bezpieczeństwa S_{ZB12},
m_{ZB12_1} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB12} do stanu zagrożenia bezpieczeństwa S_{ZB1},
l_{ZB1_13} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB1} do stanu zagrożenia bezpieczeństwa S_{ZB13},
m_{ZB13_1} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB13} do stanu zagrożenia bezpieczeństwa S_{ZB1},
l_{ZB2_12} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB2} do stanu zagrożenia bezpieczeństwa S_{ZB12},
m_{ZB12_2} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB12} do stanu zagrożenia bezpieczeństwa S_{ZB2},
l_{ZB2_23} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB2} do stanu zagrożenia bezpieczeństwa S_{ZB23},
m_{ZB23_2} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB23} do stanu zagrożenia bezpieczeństwa S_{ZB2},
l_{ZB3_13} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB3} do stanu zagrożenia bezpieczeństwa S_{ZB13},
m_{ZB13_3} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB13} do stanu zagrożenia bezpieczeństwa S_{ZB3},
l_{ZB3_23} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB3} do stanu zagrożenia bezpieczeństwa S_{ZB23},
m_{ZB23_3} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB23} do stanu zagrożenia bezpieczeństwa S_{ZB3},
l_{B1} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB12} do stanu niebezpieczeństwa S_N,
l_{B2} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB13} do stanu niebezpieczeństwa S_N,
l_{B3} – intensywność przejść ze stanu zagrożenia bezpieczeństwa S_{ZB23} do stanu niebezpieczeństwa S_N.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB1} w przypadku uszkodzenia aktywnych barier podczerwieni, następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB12} z intensywnością l_{ZB1_12}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB12}, możliwe jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB1} przez podjęcie działań polegających na przywróceniu stanu zdatności aktywnym barierom podczerwieni.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB1} w przypadku uszkodzenia monitoringu wizyjnego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB13} z intensywnością l_{ZB1_13}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB13}, możliwe jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB1} przez podjęcie działań polegających na przywróceniu stanu zdatności monitoringowi wizyjnemu.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB2}, w przypadku uszkodzenia kabla światłowodowego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB12} z intensywnością l_{ZB2_12}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB12}, możliwe

jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB2} przez podjęcie działań polegających na przywróceniu stanu zdatności kablowi światłowodowemu.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB2}, w przypadku uszkodzenia monitoringu wizyjnego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB23} z intensywnością l_{ZB2_23}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB23} możliwe jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB2} w przypadku podjęcia działań polegających na przywróceniu stanu zdatności monitoringowi wizyjnemu.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB3}, w przypadku uszkodzenia kabla światłowodowego następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB13} z intensywnością l_{ZB3_13}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB13}, możliwe jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB3} w przypadku podjęcia działań polegających na przywróceniu stanu zdatności kablowi światłowodowemu.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB3}, w przypadku uszkodzenia aktywnych barier podczerwieni następuje przejście do stanu zagrożenia bezpieczeństwa S_{ZB23} z intensywnością l_{ZB3_23}. Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB23} możliwe jest przejście do stanu zagrożenia bezpieczeństwa S_{ZB3} przez podjęcie działań polegających na przywróceniu stanu zdatności aktywnym barierom podczerwieni.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB12}, w przypadku uszkodzenia monitoringu wizyjnego następuje przejście do stanu niebezpieczeństwa S_N z intensywnością l_{B1}.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB13}, w przypadku uszkodzenia aktywnych barier podczerwieni następuje przejście do stanu niebezpieczeństwa S_N z intensywnością l_{B2}.

Gdy system jest w stanie zagrożenia bezpieczeństwa S_{ZB23}, w przypadku uszkodzenia kabla światłowodowego następuje przejście do stanu niebezpieczeństwa S_N z intensywnością l_{B3}.

System przedstawiony na rysunku 1 opisano następującymi równaniami Kołmogorowa-Chapmana:

Przyjmując warunki początkowe:

$$\begin{aligned} &R_0(0) = 1 \\ &Q_{ZB1}(0) = Q_{ZB2}(0) = Q_{ZB3}(0) = Q_{ZB12}(0) = \\ &= Q_{ZB13}(0) = Q_{ZB23}(0) = Q_B(0) = 0 \end{aligned} \tag{2}$$

i stosując odpowiednie przekształcenia matematyczne, można wyznaczyć zależności umożliwiające obliczenie wartości prawdopodobieństw przebywania rozpatrywanego systemu ochrony peryferyjnej w stanach: braku zagrożenia bezpieczeństwa S_{BZ}, zagrożenia bezpieczeństwa S_{ZB} oraz niebezpieczeństwa S_N.

Intensywności przejść pomiędzy wyróżnionymi stanami można oszacować na podstawie znanych prawdopodobieństw poszczególnych zdarzeń (np. na podstawie statystyk). Zatem znając wartość prawdopodobieństwa wykrycia potencjalnego zagrożenia przez określony system ochrony peryferyjnej, można oszacować intensywność określonego przejścia pomiędzy stanami.

4. Wnioski

Nadrzędnym celem stosowania systemów ochrony peryferyjnej obiektów kolejowych jest zwiększenie poziomu bezpieczeństwa. Kolejowy system transportowy zaliczany do infrastruktury krytycznej, wymaga szczególnej ochrony. W artykule przedstawiono analizę trójrodzajowego systemu ochrony peryferyjnej. Przyjmując określone stany (braku zagrożenia bezpieczeństwa S_{BZ}, zagrożenia bezpieczeństwa S_{ZB} i niebezpieczeństwa S_N) oraz przejścia pomiędzy nimi, wyznaczono układ równań, który opisuje analizowany system. Jego rozwiązanie umożliwia liczbowe oszacowanie poziomu bezpieczeństwa zastosowanych rozwiązań systemów ochrony peryferyjnej. Umożliwi to w dalszych badaniach określenie wpływu poszczególnych intensywności przejść na wartości prawdopodobieństw przebywania systemu ochrony peryferyjnej w wyróżnionych stanach.

$$\begin{aligned}
R_0'(t) &= -\lambda_{ZB1} \cdot R_0(t) + \mu_{PZ1} \cdot Q_{ZB1}(t) - \lambda_{ZB2} \cdot R_0(t) + \mu_{PZ2} \cdot Q_{ZB2}(t) - \lambda_{ZB3} \cdot R_0(t) + \mu_{PZ3} \cdot Q_{ZB3}(t) \\
Q_{ZB1}'(t) &= \lambda_{ZB1} \cdot R_0(t) - \mu_{PZ1} \cdot Q_{ZB1}(t) - \lambda_{ZB1_12} \cdot Q_{ZB1}(t) + \mu_{PZ12_1} \cdot Q_{ZB12}(t) - \lambda_{ZB1_13} \cdot Q_{ZB1}(t) + \mu_{PZ13_1} \cdot Q_{ZB13}(t) \\
Q_{ZB2}'(t) &= \lambda_{ZB2} \cdot R_0(t) - \mu_{PZ2} \cdot Q_{ZB2}(t) - \lambda_{ZB2_12} \cdot Q_{ZB2}(t) + \mu_{PZ12_2} \cdot Q_{ZB12}(t) - \lambda_{ZB2_23} \cdot Q_{ZB2}(t) + \mu_{PZ23_2} \cdot Q_{ZB23}(t) \\
Q_{ZB3}'(t) &= \lambda_{ZB3} \cdot R_0(t) - \mu_{PZ3} \cdot Q_{ZB3}(t) - \lambda_{ZB3_13} \cdot Q_{ZB3}(t) + \mu_{PZ13_3} \cdot Q_{ZB13}(t) - \lambda_{ZB3_23} \cdot Q_{ZB3}(t) + \mu_{PZ23_3} \cdot Q_{ZB23}(t) \\
Q_{ZB12}'(t) &= \lambda_{ZB1_12} \cdot Q_{ZB1}(t) - \mu_{PZ12_1} \cdot Q_{ZB12}(t) + \lambda_{ZB2_12} \cdot Q_{ZB2}(t) - \mu_{PZ12_2} \cdot Q_{ZB12}(t) - \lambda_{B1} \cdot Q_{ZB12}(t) \\
Q_{ZB13}'(t) &= \lambda_{ZB1_13} \cdot Q_{ZB1}(t) - \mu_{PZ13_1} \cdot Q_{ZB13}(t) + \lambda_{ZB3_13} \cdot Q_{ZB3}(t) - \mu_{PZ13_3} \cdot Q_{ZB13}(t) - \lambda_{B2} \cdot Q_{ZB13}(t) \\
Q_{ZB23}'(t) &= \lambda_{ZB2_23} \cdot Q_{ZB2}(t) - \mu_{PZ23_2} \cdot Q_{ZB23}(t) + \lambda_{ZB3_23} \cdot Q_{ZB3}(t) - \mu_{PZ23_3} \cdot Q_{ZB23}(t) - \lambda_{B3} \cdot Q_{ZB23}(t) \\
Q_B'(t) &= \lambda_{B1} \cdot Q_{ZB12}(t) + \lambda_{B2} \cdot Q_{ZB13}(t) + \lambda_{B3} \cdot Q_{ZB23}(t)
\end{aligned} \tag{1}$$

Literatura

1. Burdzik R., Konieczny Ł., Figlus T.: *Concept of onboard comfort vibration monitoring system for vehicles, Mikulski J.,* (Ed.): Activities of Transport Telematics, TST 2013, CCIS 395, s. 418-425, Springer, 2013 Heidelberg.
2. Chmiel J., Rosiński A.: *Integracja systemów bezpieczeństwa dworca kolejowego*, Prace Naukowe Politechniki Warszawskiej. Transport, z. 92, s. 21-28, Oficyna Wydawnicza Politechniki Warszawskiej, 2013 Warszawa.
3. Chmiel J., Rosiński A.: *Wybrane zagadnienia modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej na przykładzie bazy logistycznej*, Logistyka nr 4/2015, s. 117-123, Instytut Logistyki i Magazynowania, Poznań 2015.
4. Dyduch J., Paś J., Rosiński A.: *Podstawy eksploatacji transportowych systemów elektronicznych*, Wydawnictwo Politechniki Radomskiej, Radom 2011.
5. Dziula P., Rosiński A., Siergiejczyk M.: *An approach to analysis of transition rates between the critical infrastructure systems safety states*, Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, vol. 6, number 1, 2015.
6. Fischer R., Halibozek E., Walters D.: *Introduction to Security*. Butterworth-Heinemann, 2012.
7. Harwood E.: *DIGITAL CCTV. A Security Professional's Guide*, Butterworth Heinemann, 2Hołyst B.: *Terroryzm,* Tom 1 i 2, Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.
8. Krzykowski M.: *Ochrona odbiorców wrażliwych energii elektrycznej i paliw gazowych – uwarunkowania prawne*, Polityka Energetyczna – Energy Policy Journal, tom 17, zeszyt 3, s. 257–268, 2014.
9. Krzykowski R., Trenczek S., Krzykowski M.: *Przeciwdziałanie skutkom zapylenia obiektów przemysłowych w sektorze energetycznym*, Zeszyty Naukowe Instytutu Gospodarki Surowcami Mineralnymi i Energią PAN, nr 78/2010, s. 87-97.
10. Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
11. Paś J., Duer S.*: Determination of the impact indicators of electromagnetic interferences on computer information systems*, Neural Computing & Applications 2012, DOI:10.1007/s00521-012-1165-1.
12. Paś J.: *Eksploatacja elektronicznych systemów transportowych,* Wydawnictwo Uniwersytetu Technologiczno-Humanistycznego w Radomiu, Radom 2015.
13. Rosiński A.: *Modelowanie procesu eksploatacji systemów telematyki transportu*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.
14. Rządowe Centrum Bezpieczeństwa, Narodowy program ochrony infrastruktury krytycznej. Załącznik 1: Charakterystyka systemów infrastruktury krytycznej, Warszawa 2013.
15. Siergiejczyk M., Paś J., Rosiński A.: *Evaluation of safety of highway CCTV system's maintenance process*, monografia „Telematics – support for transport" pod redakcją J. Mikulskiego, wydana jako monograficzna seria wydawnicza – „Communications in Computer and Information Science", Vol. 471, Springer-Verlag, 2014 Berlin Heidelberg.
16. Siergiejczyk M., Rosiński A.: *Analysis of power supply maintenance in transport telematics system*, Solid State Phenomena, vol. 210 (2014), s. 14-19, 2014.
17. Siergiejczyk M., Rosiński A.: *Reliability analysis of electronic protection systems using optical links*, monografia „Dependable Computer Systems" pod redakcją: W. Zamojskiego, J. Kacprzyka, J. Mazurkiewicza, J. Sugiera i T. Walkowiaka, wydana jako monograficzna seria wydawnicza – „Advances in intelligent and soft computing", Vol. 97, Springer-Verlag, Berlin Heidelberg 2011.
18. Siergiejczyk M., Rosiński A.: *Reliability analysis of power supply systems for devices used in transport telematic systems*, monografia „Modern Transport Telematics" pod redakcją J. Mikulskiego, wydana jako monograficzna seria wydawnicza – „Communications in Computer and Information Science", Vol. 239, Springer-Verlag, Berlin Heidelberg 2011.
19. Siergiejczyk M., Rosiński A.: *Systemy ochrony peryferyjnej obiektów transportowych infrastruktury krytycznej*, Technika Transportu Szynowego nr 10/2013, s. 2083-2089, 2013.
20. Siergiejczyk M., Rosiński A.: *Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego*, monografia „Rewaluacja bezpieczeństwa publicznego" pod redakcją naukową T. Zaborowskiego, Instytut Badań i Ekspertyz Naukowych w Gorzowie Wlkp. 2011.
21. Siergiejczyk M., Rosiński A., Krzykowska K.: *Problematyka niezawodnościowo-eksploatacyjna systemów ochrony peryferyjnej portów lotniczych*, Przegląd komunikacyjny nr 11/2014, s. 5-8.
22. Skorupski J., Uchroński P.: *A fuzzy reasoning system for evaluating the efficiency of cabin luggage screening at airports*, Transportation Research Part C – Emerging Technologies 54, s. 157-175, 2015.
23. Szulc W., Rosiński A.: *Systemy monitoringu wizyjnego jako ochrona obwodowa obiektów*, monografia „Ochrona przed skutkami nadzwyczajnych zagrożeń. Tom 3" pod redakcją Z. Mierczyka i R. Ostrowskiego, wydana jako monograficzna seria wydawnicza, Wojskowa Akademia Techniczna, Warszawa 2012.
24. Szulc W., Rosiński A.: *Systemy Sygnalizacji Włamania i Napadu stosowane w obiektach transportowych wykorzystujące technologie chmury*, Logistyka nr 3/2014, s. 6140-6144, Instytut Logistyki i Magazynowania, Poznań 2014.

Modeling the Level of Security Three Generic Peripheral Protection Systems on the Example of Rail Objects

Summary
The primary purpose of using peripheral protection systems of railway objects is to increase the level of security. Because the transport system is classified into the critical infrastructure, it requires special protection. Therefore, the authors analyzed the tri-generic peripheral protection system. To accomplish it there is analyzed process crossing the border of the protected area by unauthorized persons. This has enabled the graphically presentation of occurrence of the situations, as the relations in the system of the periphery protection. Then the system of peripheral protecting is described by the set of equations Kolmogorov-Chapman equations. As a result, it is possible to estimate the numerical level of security of the applied solutions of peripheral protection systems.

Keywords: security, modeling, peripheral protection

Моделирование уровня безопасности трехрядных систем периферийной защиты на примере железнодорожных объектов

Резюме
Самой главной целью употребления систем периферийной защиты железнодорожных объектов является повышение уровня безопасности. Поскольку система транспорта причисляется к важной инфраструктуре, требует специальной защиты. Поэтому авторы провели анализ трехрядной системы периферийной защиты. Для того чтобы выполнить эту задачу, был проанализирован процесс детекции неуполномоченных лиц пересекающих границу защищенной зоны. Это позволило графически представить возникшие ситуации в виде отношений в системе периферийной защиты. После того система периферийной защиты была описана при помощи системы уравнений Колмогорова – Чепмена. Благодаря этому возможно оценить численно уровень безопасности употребленных вариантов систем периферийной защиты.

Ключевые слова: безопасность, моделирование, периферийная защита