

Adam ROSIŃSKI¹

ROZPROSZONE SYSTEMY SYGNALIZACJI WŁAMANIA I NAPADU W BAZACH LOGISTYCZNYCH

W referacie zaprezentowano zagadnienia związane z Systemami Sygnalizacji Włamania i Napadu (SSWiN). Przedstawiono ich elementy składowe wymienione w Polskiej Normie PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe”. Pokazano również przykładowe rozwiązanie SSWiN o strukturze rozproszonej z zastosowaniem konwerterów światłowodowych dla baz logistycznych.

DISTRACTED INTRUSION AND HOLD-UP SYSTEMS IN LOGISTIC BASES

In the paper are presented the problems connected with intrusion and hold-up systems (SSWiN). There are presented their component units specified in the Polish standards PN-EN 50131-1:2009 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements”. There is also shown the example solution of SSWiN with structure distracted with the use of optical converters for logistic bases.

1. WSTĘP

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” [4], zawiera wykaz części składowych (elementów), które powinien zawierać System Sygnalizacji Włamania i Napadu (SSWiN): centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu, zasilacz podstawowy, zasilacz rezerwowy. Połączenia pomiędzy elementami systemu powinny spełniać określone wymagania, a zarazem muszą także zawierać się w dopuszczalnych przez producenta parametrach. Ogólnie można je podzielić na połączenia przewodowe lub bezprzewodowe. Zaprojektowanie oraz realizacja Systemu Sygnalizacji Włamania i Napadu dla dużego i rozległego obiektu wymaga sporej wiedzy technicznej, jak również dużego doświadczenia. Istnieją obiekty, w których ze względów ekonomicznych, a także logistycznych można tylko zabezpieczyć poprzez zastosowanie

¹Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej, Polska, 03-772 Warszawa, ul. Kawęczyńska 36,

Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie, Polska, 00-662 Warszawa, ul. Koszykowa 75, tel.: 22 2347038, e-mail: adro@it.pw.edu.pl

integracji mniejszych, skupionych systemów. Pojawia się wtedy problem zarządzania wieloma pojedynczymi systemami, które tworzą jeden duży system bezpieczeństwa. W referacie zostaną zaprezentowane różne koncepcje rozproszonych SSWiN.

Norma PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe” określa stopień zabezpieczenia, którą powinny spełniać systemy sygnalizacji włamania. Są one następujące:

- stopień 1: Ryzyko małe (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada łatwo dostępne narzędzia w ograniczonym wyborze),
- stopień 2: Ryzyko małe do średniego (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada ogólnie dostępne narzędzia i przenośne urządzenia, np. multimetr),
- stopień 3: Ryzyko średnie do wysokiego (zakłada się, że intruz zna biegle system alarmowy i posiada złożony zestaw zaawansowanych narzędzi i przenośnego sprzętu elektronicznego),
- stopień 4: Ryzyko wysokie (ma zastosowanie, gdy bezpieczeństwo ma priorytet nad wszystkimi innymi czynnikami. Zakłada się, że intruz posiada zdolności bądź środki by szczegółowo zaplanować włamanie i posiada zestaw dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Po określeniu stopnia zabezpieczenia jaką system sygnalizacji włamania ma spełniać, dobiera się urządzenia, które spełniają założone wymagania. Oczywiście norma podaje jakie elementy muszą być zastosowane. Z tego też m.in. względu spotyka się różne rozwiązania konstrukcyjne central alarmowych. Mogą one spełniać wymagania określonego stopnia zabezpieczenia, ale zarazem w zależności od producenta różnią się pomiędzy sobą.

Jak już wspomniano centrala alarmowa stanowi „serce” systemu sygnalizacji włamania. 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). 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.) [5,8]. Obecnie najczęściej informacje pomiędzy centralą alarmową a poszczególnymi modułami są przesyłane cyfrowo z zastosowaniem formatu transmisji RS-232 lub RS-485 lub innego (bardzo często opracowanego przez producenta). Istnieją też rozwiązania systemów sygnalizacji włamania, w których magistrale transmisyjne mogą łączyć [6]:

- kilka central alarmowych między sobą (pracujące one w tzw. pierścieniu),
- układ sterowania (np. klawiatura sterująca),
- centrale alarmowe z centrum nadzorowania, zarządzania i administrowania zintegrowanym systemem bezpieczeństwa.

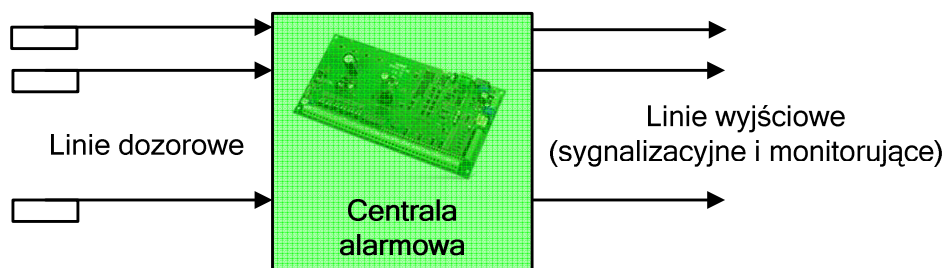
Należy tutaj nadmienić iż większość stosowanych jeszcze kilka lat temu rozwiązań wykorzystywała połączenia przewodowe. Obecnie bardzo wiele rozwiązań oferowanych na rynku umożliwia wykorzystanie transmisji bezprzewodowej, która może być przykładowo typu on-line z zastosowaniem częstotliwości transmisji 433MHz. W praktyce spotykane są

częściej systemy mieszane a więc takie gdzie transmisja sygnałów odbywa się zarówno drogami przewodowymi jak i radiowymi.

Wymienione rozwiązania konstrukcyjne powodują, że producenci stosują różne media transmisyjne, które mogą być zastosowane przy projektowaniu a następnie instalowaniu rozproszonych Systemów Sygnalizacji Włamania i Napadu. Zostaną one w kolejnym rozdziale wymienione i scharakteryzowane.

2. ROZPROSZONE SYSTEMY SYGNALIZACJI WŁAMANIA I NAPADU

Najczęściej obecnie spotykane centrale alarmowe to mikroprocesorowe centrale cyfrowe. System sygnalizacji włamania i napadu może mieć strukturę zwartą (skupioną), tzn. taką w której należy doprowadzić wszystkie linie dozorowe i linie wyjściowe (sygnalizacyjne oraz monitorujące) wprost do płyty głównej centrali alarmowej. Zostało to przedstawione na rys. 1. Centrale tego typu stosowane są do obiektów małych (np. mieszkania, małe biura), które wymagają kilkanaście linii dozorowych (przeważnie do 16).

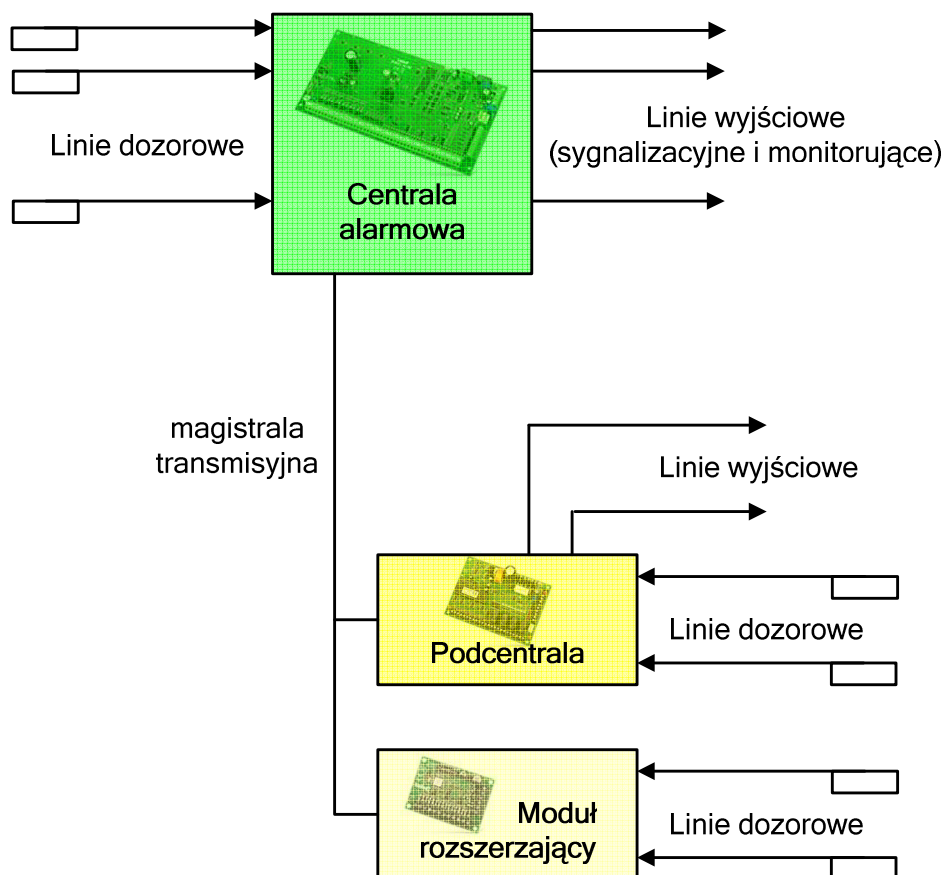


Rys. 1. System sygnalizacji włamania i napadu o strukturze zwartej (skupionej)

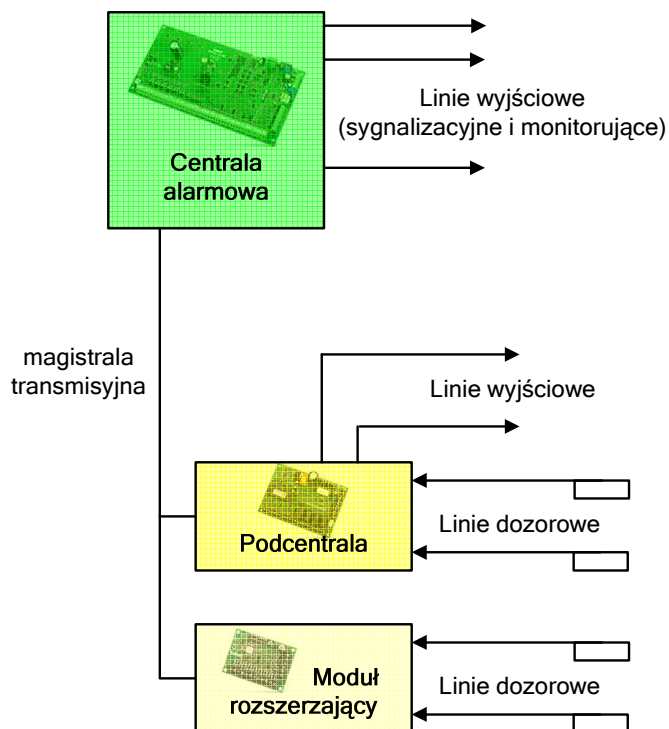
System sygnalizacji włamania i napadu typu mieszanego posiadają określoną liczbę linii dozorowych wprowadzanych do centrali. Mają także możliwość współpracy z innymi centralami po łączach RS-232 lub RS-485, jak również możliwość współpracy z podcentralami lub modułami za pośrednictwem magistrali transmisyjnej. Na rys. 2 przedstawiono system sygnalizacji włamania i napadu w wersji mieszanej. Stosuje się go do obiektów, które wymagają dużej liczby linii dozorowych (przeważnie powyżej 16). Zwykle kilka linii dozorowych (od 4 do 16) wprowadza się wprost do listwy łączeniowej płyty głównej centrali alarmowej. Zazwyczaj te linie dozorowe nie są zbyt długie (od kilku do kilkudziesięciu metrów) i łączą czujki usytuowane blisko centrali alarmowej. Pozostałe dołączone są do modułów rozszerzeniowych wejściowych, przeważnie o 8 wejściach. Linie wyjściowe w tym systemie mogą być dołączone do wyjść płyty głównej lub do (najczęściej 4 wyjściowego) modułu rozszerzającego wyjścia. Jeśli jest to moduł podcentrali to posiada on zwykle do 8 wejść linii dozorowych i 8 wyjść.

Na rys. 3 przedstawiono system sygnalizacji włamania i napadu o strukturze rozproszonej. Centrala połączona jest z modułami za pośrednictwem magistrali transmisyjnej. Do modułów doprowadzone są linie dozorowe i linie wyjściowe. Tego typu systemy są rzadko spotykane, ponieważ większość oferowanych na rynku central alarmowych ma na płycie głównej możliwość dołączenia linii dozorowych. Jeśli jednak projektant nie wykorzysta ich, to wtedy mamy system o strukturze rozproszonej. Linie dozorowe i linie wyjściowe dołączone są do modułów rozszerzających wejścia i wyjścia

lub podcentral. Analizując rys. 3 można stwierdzić, że moduły są dołączone do płyty głównej za pośrednictwem magistrali transmisyjnej (zwykle 4-drutowej) o długości od kilkunastu metrów do 1300m. Znane są przypadki długości magistral transmisyjnych nawet 2500m przy formacie transmisji RS-485 (dla znacznie spowolnionej prędkości transmisji dwukierunkowej).

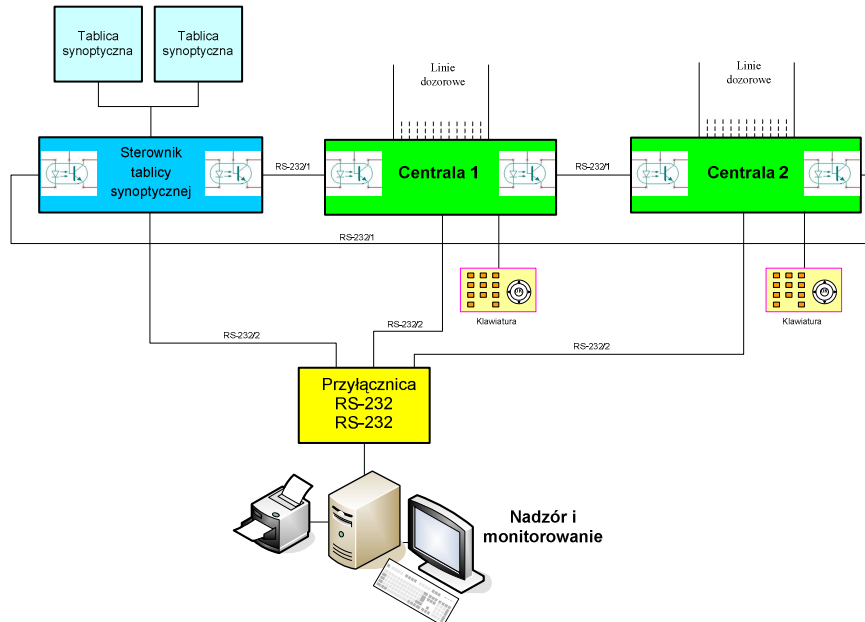


Rys. 2. System sygnalizacji włamania i napadu o strukturze mieszanej



Rys. 3. System sygnalizacji włamania i napadu o strukturze rozproszonej

Do bardzo interesujących rozwiązań konfiguracji systemów sygnalizacji włamania i napadu należy grupa central, które mogły pracować jako systemy skupione z własną klawiaturą. Są to pojedyncze systemy niezależne i autonomiczne. Każdą z tych central posiada moduł RS-232. Cały system może pracować w tzw. pętli zamkniętej, zaś wszystkie centrale są kontrolowane systemowo a ich stan edytowany na ekranie komputera. Na rys. 4 przedstawiono zespół różnych central w wersji skupionej, które w wyniku integracji utworzyły system sygnalizacji włamania i napadu o strukturze rozproszonej. Każda z central posiada niezależną klawiaturę (przedstawioną na rysunku) i została wyposażona w kartę RS-232, która umożliwiła połączenie central w duży system alarmowy (na rys. 4 to połączenie oznaczone jako „RS-232/2”). Centrala nr 2 poprzez magistralę transmisyjną RS-232/1 łączy sterownik tablicy synoptycznej. Wszystkie bloki systemu alarmowego a więc: centrale 1 i 2 oraz sterownik tablicy synoptycznej połączone są magistralami transmisyjnymi RS-232 z przyłącznicą RS-232/2 a ta z komputerem nadzorującym pracę całego systemu sygnalizacji włamania i napadu. Warto nadmienić, że w skład tego zintegrowanego systemu wchodzi jednostki o różnych wielkościach a więc o różnej liczbie linii dozorowych (od 18, poprzez 40, do 64 linii dozorowych) oraz o 40 strefach jakie posiada każda z central [3]. Jest to jedna z nielicznych central, które pozwalają łączyć się w duże systemy sygnalizacji włamania. Ważną cechą tego systemu jest możliwość decentralizacji wszystkich central wchodzących w skład tego dużego systemu.



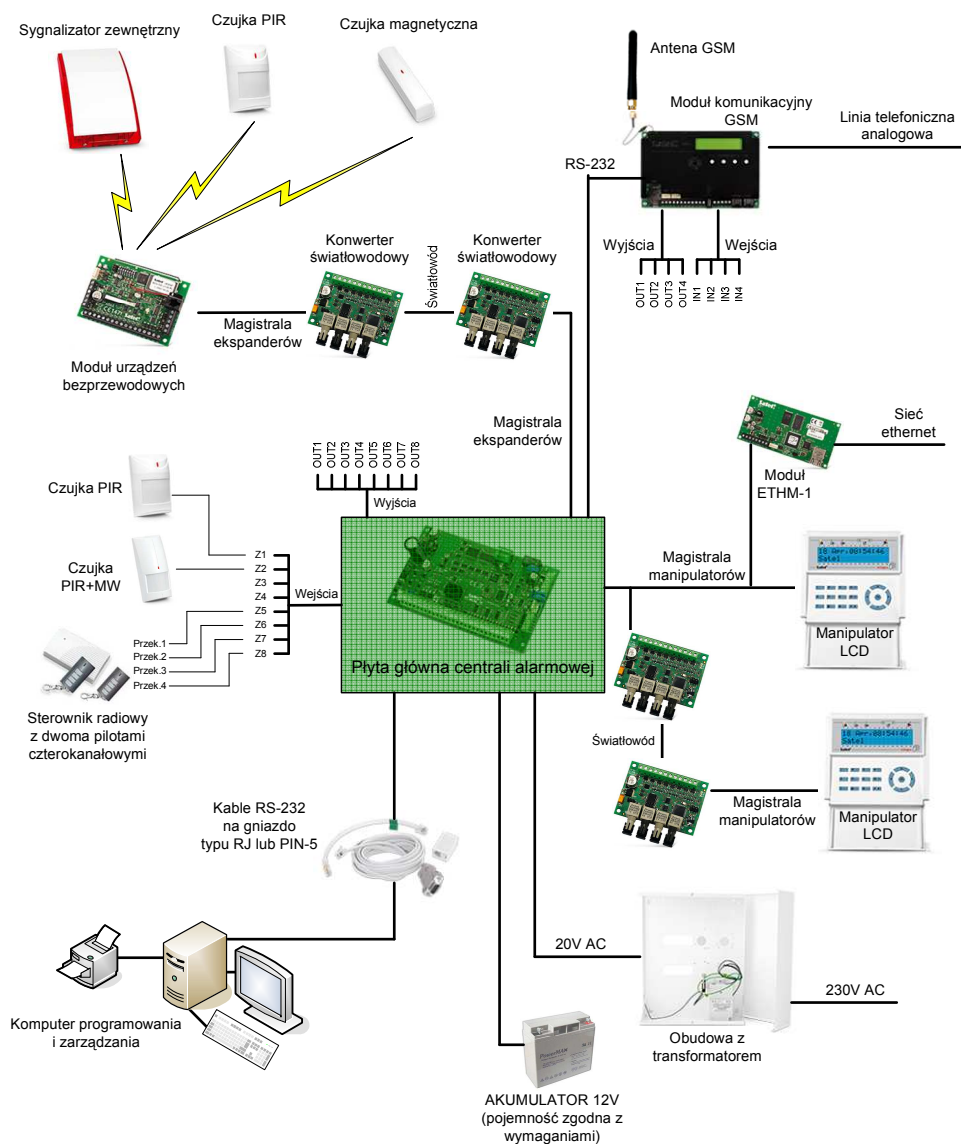
Rys. 4. System sygnalizacji włamania i napadu o strukturze rozproszonej powstały w wyniku integracji 2 central skupionych

Ze względu na specyfikę baz logistycznych, których budynki są rozmieszczone bardzo często na dużym obszarze, a jednocześnie mają one dość znaczą powierzchnię, zachodzi potrzeba zaprojektowania Systemu Sygnalizacji Włamania i Napadu, który umożliwi rozmieszczenie elementów składowych w chronionych pomieszczeniach i terenach przyległych. Zastosowanie konwencjonalnych rozwiązań przewodowych w których są stosowane magistrale transmisyjne (np. ekspanderów, manipulatorów) do transmisji sygnałów elektrycznych nie jest wystarczające ze względu na gwarantowaną jakość transmisji danych w funkcji odległości pomiędzy elementami systemu. Kolejną istotną sprawą są zakłócenia elektromagnetyczne, które mogą wystąpić. Dlatego też zaczęto stosować medium transmisyjne, jakim jest światłowód. W celu przesłania informacji niezbędne jest przetworzenie sygnałów elektrycznych na optyczne (nadajnik światłowodowy) i odwrotnie (odbiornik światłowodowy) [1,2,7] – rys. 5. Ponieważ przesyłanie informacji w magistralach SSWiN odbywa się dwukierunkowo, zatem konwerter światłowodowy powinien zawierać zarówno układ nadawczy jak i odbiorczy. Zatem również niezbędne są dwa światłowody w celu zapewnienia przesyłania informacji pomiędzy dwoma konwerterami. Kolejną zaletą stosowania transmisji światłowodowej jest wysoka odporność komunikacji na zakłócenia oraz izolacja galwaniczna urządzeń.



Rys. 5. Łącze światłowodowe przeznaczone do transmisji sygnałów

Na rys. 6 przedstawiono autorski schemat Systemu Sygnalizacji Włamania i Napadu o strukturze mieszanej, który został opracowany (z wykorzystaniem centrali alarmowej INTEGRA firmy SATEL) i uruchomiony jako stanowisko badawczo-dydaktyczne przeznaczone m.in. do zarządzania systemem.



Rys. 6. System sygnalizacji włamania i napadu o strukturze rozproszonej (z zastosowaniem konwerterów światłowodowych)

Przedstawiony SSWiN jest zaliczany do grupy układów mieszanych, tzn. część linii dozorowych (np. czujka PIR, czujka magnetyczna, sygnalizator zewnętrzny) jest połączona drogami radiowymi ze specjalnym modułem urządzeń bezprzewodowych. Moduł zaś jest połączony z płytą główną centrali alarmowej za pośrednictwem przewodowej magistrali transmisyjnej. Również część czujek jest dołączona do płyty głównej za pośrednictwem klasycznych przewodowych linii dozorowych. Całość systemu może być programowana i nadzorowana przez komputer (z odpowiednim oprogramowaniem) połączony z płytą główną centrali alarmowej za pośrednictwem interfejsu RS-232. Możliwe jest także obsługa systemu poprzez manipulator LCD. W przypadku zaistnienia konieczności przeprogramowania systemu zdalnie, można wykorzystać analogową lub cyfrową (GSM) linię telefoniczną. W tym celu niezbędny jest moduł komunikacyjny GSM.

3. WNIOSKI

W referacie zaprezentowano zagadnienia związane głównie z Systemami Sygnalizacji Włamania i Napadu w aspekcie ich konfiguracji dla ochrony rozległych obszarów. Przedstawiono najczęściej spotykane rozwiązania oraz przykładowe stanowisko badawczo-laboratoryjne umożliwiające analizę omawianych zagadnień. Zaprezentowano również różne media transmisyjne oraz podano ich zalety i wady. Pozwoli to projektantom na tworzenie SSWiN, które będą cechowały się zwiększonym poziomem bezpieczeństwa transmisji informacji pomiędzy poszczególnymi elementami składowymi tworzącymi system.

4. BIBLIOGRAFIA

- [1] Haykin S.: *Systemy telekomunikacyjne*. Tom I i II. WKiŁ, Warszawa 2004.
- [2] Horowitz P., Hill W.: *Sztuka elektroniki*. Tom I i II. WKiŁ, Warszawa 2006.
- [3] Instrukcje serwisowe: AAT, RANKOR, RISCO, SATEL.
- [4] Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
- [5] Norman T.: *Integrated security systems design*. Butterworth Heinemann, 2007.
- [6] Szulc W., Rosiński A.: *Systemy sygnalizacji włamania. Część 1 – Konfiguracje central alarmowych*. Zabezpieczenia Nr 2(66)/2009, wyd. AAT, Warszawa 2009.
- [7] Szulc W., Rosiński A.: *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków (część I – analogowa)*. Oficyna Wydawnicza WSM, Warszawa 2008.
- [8] Wójcik A. (red.): *Mechaniczne i elektroniczne systemy zabezpieczeń: fachowy poradnik dla: projektantów, instalatorów, producentów, inwestorów, agencji ochrony mienia, użytkowników*. Verlag Dashofer, Warszawa 2008.