TECHNIKA TRANSPORTU SZYNOWEGO

Waldemar SZULC, Adam ROSIŃSKI

STANOWISKA BADAWCZO-DYDAKTYCZNE WSPOMAGANE KOMPUTEROWO W LABORATORIUM SYSTEMÓW BEZPIECZEŃSTWA OSÓB I MIENIA

Streszczenie

W referacie zaprezentowano zagadnienia związane ze stanowiskami badawczo-dydaktycznymi dotyczącymi elektronicznych systemów bezpieczeństwa. Zwrócono szczególną uwagę na możliwości ich integracji poprzez wykorzystanie sieci LAN z zastosowaniem protokołu TCP. Wszystkie stanowiska są sterowane i nadzorowane komputerowo. Dzięki temu możliwe jest zdalne zarządzanie i nadzór nad nimi. W referacie przedstawiono to w ujęciu zarówno dydaktycznym, jak i badawczo-naukowym.

WSTĘP

W październiku 2005 roku uruchomiono w Wyższej Szkole Menedżerskiej na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa specjalność: „Bezpieczeństwo Obiektów i Informacji" (BOiI). Specjalność powstała w wyniku analizy potrzeb dotyczących tzw. Inżynierii Bezpieczeństwa traktowanej jako szerokie pojęcie. Autorzy projektu dokonali przeglądu tego typu specjalności na wielu polskich Uczelniach jak również przeglądu różnych szkoleń dotyczących tematyki Systemów Alarmowych. Te ostatnie to zwykle krótkoterminowe szkolenia dające ledwie ogólny pogląd na tę dziedzinę nauki. Wprowadzając nową specjalność (BOiI) autorzy zdawali sobie sprawę z bardzo poważnego wyzwania dotyczącego nakreślenia wielu przedmiotów specjalistycznych niezbędnych do realizacji bardzo poważnej specjalności jaką jest Bezpieczeństwo Obiektów i Informacji [1]. Nauka na tej specjalności musi być poprzedzona wieloma innymi przedmiotami niezbędnymi do zrozumienia przedmiotów specjalistycznych. Tak więc jako przedmioty podstawowe wprowadzono: matematykę, fizykę, informatykę, miernictwo i elektronikę (analogowa i cyfrowa), budowę sieci informatycznych, podstawy telekomunikacji, podstawy programowania, podstawy eksploatacji systemów, podstawy normalizacji i kodyfikacji, języki obce, itp. Poza problematyką dydaktyczną na Uczelni, autorzy postawili sobie również cel badawczy w aspekcie analizy zintegrowanych systemów bezpieczeństwa wykorzystując stanowiska badawczo-dydaktyczne oraz protokół TCP. Uczelnia wprowadziła kierunek zwany: Bezpieczeństwo Narodowe, które wg standardów jest nauką społeczną. Autorzy chcą jednak na tym kierunku prowadzić (w perspektywie) badania naukowe oraz zajęcia dydaktyczne o charakterze technicznym. Żadna Uczelnia w Polsce nie kształci przyszłych specjalistów w dziedzinie Bezpieczeństwa Narodowego w aspekcie technicznym. Niezbędne są do prowadzenia takich zajęć oraz badań wyspecjalizowane laboratoria zajmujące

się problematyką Elektronicznych Systemów Bezpieczeństwa (ESB). Poniżej podano istotne przedmioty, które muszą być znane zarówno w procesie dydaktycznym jak i badawczym:

- Projektowanie systemów alarmowych,
- Instalacje systemów alarmowych,
- Technika mikrofal,
- Przetwarzanie sygnałów,
- Technika światłowodowa,
- Mechaniczne systemy ochrony,
- Zintegrowane systemy ochrony,
- Ochrona przeciwpożarowa,
- Dźwiękowe Systemy Ostrzegania (DSO),
- Telewizja dozorowa (monitoring wizyjny),
- Kontrola dostępu (KD),
- Systemy Sygnalizacji Włamania i Napadu,
- Elementy składowe ww. systemów,
- Komputerowa symulacja układów elektronicznych,
- Ochrona systemów i baz danych,
- Ochrona informacji,
- Zarządzanie bezpieczeństwem,
- Zagadnienia prawne,
- Eksploatacja systemów bezpieczeństwa,
- Elementy kryminalistyki,
- Wybrane zagadnienia kompatybilności w systemach bezpieczeństwa,
- Monitoring Systemów Alarmowych,
- Transmisja sygnałów alarmowych,
- Metody zobrazowania informacji,
- Wstęp do kryptologii,
- Przepisy prawne,
- Przepisy normatywne.

Naturalnie ze względu na bardzo duży materiał wykładowy autorzy pogrupowali w/w przedmioty w grupy tematyczne tak aby sprostać wymaganiom wynikającym ze standardów obowiązujących w Szkolnictwie Wyższym.

Bardzo poważnym wyzwaniem stało się zbudowanie Laboratorium Systemów Alarmowych na wysokim poziomie, które obsługiwałoby studentów na specjalności BOiI. Podjęto się budowy takiego Laboratorium w połowie 2008 roku. Ze względu na olbrzymią tematykę dotyczącą Elektronicznych Systemów Bezpieczeństwa (ESB), zadanie podzielono na kilka etapów nazywając ten poważny projekt: „Zespołem Laboratoriów Systemów Bezpieczeństwa". Uczelnia nawiązała kontakty z wieloma znanymi producentami, którzy sukcesywnie pomagali w realizacji tego bardzo trudnego zadania. udostępniając sprzęt, który w wyniku doskonałej współpracy zaowocował powstaniem wielu stanowisk laboratoryjnych z tzw. „górnej półki". Producenci poza sprzętem, udostępnili bardzo wiele programów, instrukcji obsługi oraz filmów monotematycznych. W dniu 06.03.2009 r. nastąpiło uroczyste otwarcie Zespołu Laboratoriów Systemów Bezpieczeństwa (część I) w Wyższej Szkole Menedżerskiej w Warszawie na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa. W trakcie budowy stanowisk laboratoryjnych przyjęto zasadę wykorzystania protokołu TCP dla ich nadzoru i zarządzania. Tak więc wszystkie stanowiska badawcze i dydaktyczne posiadają adresy IP. Autorzy niniejszego artykułu są również twórcami i architektami powstałego Zespołu Laboratoriów Systemów Bezpieczeństwa.

1. GENEZA POWSTANIA ZESPOŁU LABORATORIÓW SYSTEMÓW BEZPIECZEŃSTWA

Zespół Laboratoriów Systemów Bezpieczeństwa. (jak wspomniano powyżej) został uruchomiony na początku marca 2009 r. Powstało Laboratorium Systemów Alarmowych I składające się z 14 stanowisk dydaktycznych. Uroczyste otwarcie Laboratorium było dokumentowane przez wszystkie branżowe pisma zajmujące się technikami bezpieczeństwa. Duży reportaż był w ZABEZPIECZNIACH Nr 2(66)/2009r. Stanowiska dydaktyczne i badawcze dotyczą różnych rozwiązań monitoringu wizyjnego (analogowego i cyfrowego). Znane na polskim rynku firmy zajmujące się monitoringiem wizyjnym, wyposażyły stanowiska dydaktyczne w znakomite programy komputerowe do nadzoru i zarządzania [3,4,6]. Stanowiska monitoringu wizyjnego są wyposażone (opcjonalnie) w oświetlacze podczerwone. W Laboratorium znajdują się Systemy Sygnalizacji Włamania i Napadu (przewodowe i bezprzewodowe) o różnych stopniach komplikacji [5], opcje Kontroli Dostępu także ze sterowaniem biometrycznym, oraz różnego typu czujek współpracujące z ESB. Poza gotowymi zestawami SSWiN w Laboratorium Systemów Alarmowych I są dwa stanowiska SSWiN, które można konfigurować wg wskazówek prowadzącego jak również wykonywać badania naukowe. Wszystkie stanowiska badawcze i dydaktyczne są wyposażone w komputery, które umożliwiają nadzór nad badanymi stanowiskami. Wszystkie stanowiska posiadają własne adresy IP co umożliwia ich administrowanie i zarządzanie drogami informatycznymi [8]. Stanowiska badawcze i dydaktyczne mogą być monitorowane drogami: radiowymi, informatycznymi oraz komutowanymi. Autorzy opracowali precyzyjne instrukcje laboratoryjne dla każdego stanowiska dydaktycznego. W Laboratorium Systemów Alarmowych I znajduje się centralny komputer, który współpracuje z rzutnikiem multimedialnym wysokiej jakości. Prowadzący ma możliwość wyboru stanowiska dydaktycznego (dla potrzeb studenckich) i wyświetleniu aktualnie prowadzonych badań na ekranie.

Na początku stycznia 2010 r. autorzy uruchomili Laboratorium Systemów Alarmowych II (część II) w ramach Zespołu Laboratoriów Systemów Bezpieczeństwa. W tej sali zlokalizowano 8 stanowisk dydaktycznych o znacznym stopniu zaawansowania (wszystkie nadzorowane komputerowo). Również powyższe stanowiska badawcze i dydaktyczne posiadają stałe adresy IP i są włączone do sieci informatycznej Uczelni. Podobnie jak Laboratorium Systemów Alarmowych I, drugie Laboratorium a w nim stanowiska dydaktyczne powstały w wyniku bardzo ścisłej współpracy z kolejnymi producentami i sponsorami. Konfiguracje stanowisk dydaktycznych zostały tak zbudowane aby w sposób klarowny można było prowadzić procesy badawcze oraz dydaktyczne ze studentami specjalności BOiI. Poza stanowiskami dydaktycznymi, sponsorzy udostępnili również programy komputerowe umożliwiające pełny nadzór i zarządzanie systemami alarmowymi. Ciekawostką w tym Laboratorium Systemów Alarmowych II jest unikalny system sygnalizacji pożarowej dla potrzeb ruchomych środków transportowych (a wiec dla pociągów, autobusów szynowych i autobusów miejskich). Jest również stanowisko kontroli dostępu, są systemy domofonowe i videodomofonowe jak również bezprzewodowe Systemy Sygnalizacji Włamania i Napadu. Ciekawostką są bardzo nowoczesne urządzenia elektromechaniczne (rygle, przyciski, trzymaki magnetyczne itp.) do współpracy z Kontrolą Dostępu jak i z SSWiN.

W trakcie budowy jest trzecie Laboratorium Systemów Alarmowych III (część III), w którym autorzy wprowadzili Dźwiękowe Systemy Ostrzegawcze (DSO), Systemy Sygnalizacji Pożarowej (SSP) wraz z różnymi typami czujek oraz przewodowe i bezprzewodowe systemy monitoringu. W Laboratorium Systemów Alarmowych III zostały

również zlokalizowane mikroprocesorowe SSP dla potrzeb Transportu. Ponadto są również stanowiska badawcze elementów składowych ESB.

2. ZESPÓŁ LABORATORIÓW SYSTEMÓW BEZPIECZEŃSTWA

Uczelnia aktualnie posiada Zespół Laboratoriów Systemów Bezpieczeństwa (trzy Laboratoria Systemów Alarmowych I, II, III), który został utworzony dzięki znanym producentom i sponsorom i przy współpracy m.in. z firmami: Satel, Sony, AAT, Altram, Astral, Multisystem, GDE Polska, Eltronik, Roger, Dom Polska, RISCO Group, PULSAR, JABLOTRON, TOA, ACO, SCHRACK Seconet. W skład wyposażenia wchodzą następujące stanowiska badawcze i dydaktyczne [2,7]:

- **Stanowisko 1 „Zastosowanie Systemów Sygnalizacji Włamania i Napadu do sterowania urządzeniami infrastruktury budynków**". Jest ono przeznaczone do badań w zakresie możliwości zastosowania Systemów Sygnalizacji Włamania i Napadu do sterowania urządzeniami infrastruktury technicznej budynku. Składa się ono z: płyty głównej centrali alarmowej INTEGRA64, manipulatora INT-KLCD-BL, modułu rozszerzeń wyjśćCA-64 O-R, czujki GRAPHITE, sterownika RE-4K wraz z dwoma pilotami czterokanałowymi, modułu GSM-4, komputera z oprogramowaniem DLOADX i GUARDX.
- **Stanowisko 2 „System Sygnalizacji Włamania i Napadu jako System bezprzewodowy".** Jest ono przeznaczone do badań w zakresie możliwości zastosowania urządzeń bezprzewodowych w Systemach Sygnalizacji Włamania i Napadu. Składa się ono z: płyty głównej centrali alarmowej INTEGRA-32, manipulatora INT-KLCD-BL, modułu kontrolera systemu bezprzewodowego ACU-100, bezprzewodowej pasywnej czujki podczerwieni APD-100, bezprzewodowej czujki magnetycznej AMD-101, bezprzewodowego sygnalizatora zewnętrznego ASP-105, bezprzewodowego sterownika 230V AC typu ASW-100E, testera poziomu sygnału radiowego ARF-100, czujki AQUA Plus, komputera z oprogramowaniem DLOADX i GUARDX.
- **Stanowisko 3 „System Sygnalizacji Włamania i Napadu realizujący funkcję Kontroli Dostępu.".** Jest ono przeznaczone do badań w zakresie możliwości zastosowania Systemów Sygnalizacji Włamania i Napadu jako System Kontroli Dostępu. Składa się ono z: płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCDR-BL, modułu ethernetowego ETHM-1, modułu generatora komunikatów głosowych VMG-16, modułu czytnika kart zbliżeniowych CA-64 SR, czytnika kart zbliżeniowych CZ-EMM2, kart zbliżeniowych KT-STD-1, dualnej czujki ruchu SILVER, komputera z oprogramowaniem DLOADX i GUARDX.
- **Stanowisko 4 „Zarządzanie Systemem Sygnalizacji Włamania i Napadu przez sieć LAN".** Jest ono przeznaczone do badań w zakresie możliwości zdalnego zarządzania Systemem Sygnalizacji Włamani i Napadu poprzez sieć komputerową (np. LAN lub WAN) oraz wykorzystania sieci z protokołem TCP do integracji elektronicznych systemów bezpieczeństwa. Składa się ono z: płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCDR-BL, modułu ethernetowego ETHM-1, dualnej czujki ruchu SILVER, komputera z oprogramowaniem DLOADX i GUARDX.
- **Stanowisko 5 „Aktywna Bariera Podczerwieni".** Jest ono przeznaczone do badań w zakresie możliwości zastosowań 8 – wiązkowej programowalnej bariery nadawczo-odbiorczej do ochrony m.in.: wejść, wyjść oraz innych dużych przestrzeni. Składa się ono z: aktywnej bariery podczerwieni ACTIVA-7, komputera wyposażonego w port RS-232 z programem ACTIVA.
- **Stanowisko 6 „System Sygnalizacji Włamania i Napadu w wersji rozproszonej".** Jest ono przeznaczone do badań w zakresie niezawodności, eksploatacji i możliwości

funkcjonalnych Systemów Sygnalizacji Włamania i Napadu zaprojektowanych jako system o strukturze rozproszonej. Składa się ono z: płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCDR-BL, manipulatora INT-KLCD-BL, wielofunkcyjna klawiatura INT-SCR-BL, modułu ethernetowego ETHM-1, modułu wejść adresowalnych CA-64 ADR, modułu wyjść na szynę DIN: INT-ORS, czujek AQUA, dualnych czujek ruchu SILVER, czujki ruchu sufitowej AQUA RING, czujek magnetycznych, czujki zbicia szkła INDIGO, przycisków napadowych z pamięcią, testera czujek zbicia szkła: Tester INDIGO, komputera z oprogramowaniem DLOADX i GUARDX.

- **Stanowisko 7 „System Sygnalizacji Włamania i Napadu w wersji mieszanej”.** Jest ono przeznaczone do badań w zakresie niezawodności, eksploatacji i możliwości funkcjonalnych Systemów Sygnalizacji Włamania i Napadu zaprojektowanych jako system o strukturze mieszanej. Składa się ono z: płyty głównej centrali alarmowej CA-10P, manipulatora CA-10KLCD, manipulatora CA-10KLED, dwóch modułów wejść CA-10E, modułu syntezera mowy SM-2, czujek AQUA, dualnych czujek ruchu SILVER, komputera z oprogramowaniem DLOAD10.
- **Stanowisko 8 „System Sygnalizacji Włamania i Napadu w wersji skupionej”.** Jest ono przeznaczone do badań w zakresie niezawodności, eksploatacji i możliwości funkcjonalnych Systemów Sygnalizacji Włamania i Napadu zaprojektowanych jako system o strukturze skupionej. Składa się ono z: płyty głównej centrali alarmowej CA-5, manipulatora CA-5KLCD, manipulatora CA-5KLED, czujek AQUA, dualnych czujek ruchu SILVER.
- **Stanowisko 9 „Analogowy System Monitoringu Wizyjnego**”. Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości funkcjonalnych analogowych Systemów Monitoringu Wizyjnego. Składa się ono z: czterech kamer analogowych, przełącznika sekwencyjnego ośmiowejściowego, dzielnika obrazu czterowejściowego, monitora czarno-białego 17” nadzoru wizyjnego, monitora czarno-białego 10” nadzoru wizyjnego. Jedna z kamer jest połączona z przełącznikiem sekwencyjnym poprzez tor bezprzewodowy pracujący na częstotliwości f = 2,4GHz. Pozostałe kamery wykorzystują tor przewodowy (kabel koncentryczny).
- **Stanowisko 10 „System Monitoringu Wizyjnego CCTV i CCTV IP**”. Jest ono przeznaczone do badań w zakresie niezawodności, eksploatacji i możliwości funkcjonalnych Systemów Monitoringu Wizyjnego zarówno analogowych jak i cyfrowych. Składa się ono z: 4 kamer analogowych czarno-białych SSC-M383CE, 4 kamer analogowych kolorowych o wysokiej rozdzielczości poziomej SSC-E453P, 4 kamer analogowych kolorowych typu dzień/noc o wysokiej rozdzielczości poziomej SSC-E478P, 4 kamer kolorowych sieciowych wykorzystujących sieć z protokołem TCP, 4 wideoserwerów SNT-V704 służących do przesyłania obrazu z kamer analogowych poprzez sieć TCP, 4 komputerów z oprogramowaniem: IP Setup Program (służy do wyszukiwania adresów IP kamer i wideoserwerów pracujących w sieci.) i Real Shot Manager (wykorzystywaniu przy tworzeniu inteligentnych systemów monitoringu wizyjnego). Całość jest połączona siecią komputerową.
- **Stanowisko 11 „Inteligentna kamera IP”.** Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości funkcjonalnych kamer IP stosowanych w Systemach Monitoringu Wizyjnego. Składa się ono z: kamery IP typu SNC-RZ50P, komputera z oprogramowaniem: IP Setup Program i Real Shot Manager. Wykorzystywana kamera jest zintegrowana z obiektywem pozwalającym na 26-ścio krotną zmianę ogniskowej. Kamera wytwarza dwa strumienie danych wyjściowych, przy czym każdy z nich może być kompresowany różnymi metodami (algorytmy: JPEG, MPEG-4, H.264). Liczne funkcje cyfrowej obróbki obrazów, w tym inteligentna detekcja ruchu, pozwalają na

dostosowanie kamery SNC-RZ50P do konkretnych warunków eksploatacji. Na osobne podkreślenie zasługuje funkcja cyfrowej stabilizacji obrazów, eliminująca ich drżenie w przypadku montażu kamery na niestabilnym podłożu, na przykład na wysokim maszcie. Dynamiczna integracja obrazów pozwala na ostre i czytelne odwzorowanie obiektów ruchomych, co jest szczególnie istotnie podczas przechwytywania pojedynczych klatek wizyjnych.

- **Stanowisko 12 „Zastosowanie podczerwieni w Systemach Monitoringu Wizyjnego”.** Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości wykorzystania promieniowania podczerwonego w Systemach Monitoringu Wizyjnego. Składa się ono z: kamery analogowej z oświetlaczem podczerwieni, kamery analogowej kolorowej typu dzień/noc o wysokiej rozdzielczości poziomej, oświetlacza podczerwieni o zasięgu 100m, monitora kolorowego 7” nadzoru wizyjnego.
- **Stanowisko 13 „Zastosowanie Systemu Sygnalizacji Włamania i Napadu do wykrycia pożaru”.** Jest ono przeznaczone do badań w zakresie niezawodności, eksploatacji i możliwości funkcjonalnych Systemów Sygnalizacji Włamania i Napadu zaprojektowanych jako system wspomagający wykrycie pożaru. Składa się ono z: płyty głównej centrali alarmowej PC 1832, manipulatora PK 5516-LED, manipulatora LCD RFK5500 z wbudowanym modułem urządzeń bezprzewodowych, modułu rozszerzeń wejść PC5108, modułu zasilacza z 4 wyjściami programowalnymi PC5204, czujek przewodowych (PIR typu LC-100-PI, PIR+MW typu LC-104-PIMW, zbicia szkła wibracyjnej typu LC-105-DGB, kontaktronowej magnetycznej typu MC-440, wibracyjnej z pamięcią alarmów typu SS-102, dymu i temperatury typu EA 318-4H,) i bezprzewodowych (PIR typu WS4904W, dymu i temperatury typu WS4916, kontaktronowej typu WS4975), przycisku napadowego ręcznego, sterownika bezprzewodowego z pilotami WS4939, nadajnika monitorującego GSM/GPRS typu GS3055-IGW, sygnalizatora optyczno-akustycznego ATEK-10, elektrozaczepu DES 07NS, przycisku wyjścia monostabilnego PB 01N, komputera z oprogramowaniem.
- **Stanowisko 14 „Systemy domofonowe”.** Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości funkcjonalnych systemów domofonowych. Składa się ono z: stacji bramowej DR 2A2N, stacji domowej DP 201R, stacji domowej DP-20HR.
- **Stanowisko 15 „Systemy videodomofonowe”.** Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości funkcjonalnych systemów videodomofonowych. Składa się ono z: stacji bramowej z kamerą DRC 4CH, stacji domowej wyposażonej w monitor kolorowy z obsługą czterech wejść wraz z wbudowanym modułem pamięci obrazów CDV-71BE, kamery kolorowej stałopozycyjnej CRC-41BQ.
- **Stanowisko 16 „Systemy wieloabonentowe”.** Jest ono przeznaczone do badań w zakresie eksploatacji i możliwości funkcjonalnych systemów wieloabonentowych (maks. obsługujących do 2400 użytkowników – 12 budynków z 200 lokatorami każdy). Składa się ono z: stacji bramowej z kamerą kolorową i klawiaturą numeryczną DRC-MSC, dystrybutora budynkowego sygnałów CCU-BS, dystrybutora mieszkaniowego sygnałów CCU-FS, stacji domowej CAV-51M.
- **Stanowisko 17 „Systemy sygnalizacji pożarowej w transporcie**”. Jest ono przeznaczone do badań w zakresie konfiguracji, programowania, eksploatacji i możliwości funkcjonalnych systemów sygnalizacji pożarowej stosowanych w obiektach mobilnych. Składa się ono z: centralki sygnalizacji pożarowej CSP1TA, koncentratorów czujek CSP1CA, symulatorów czujek pożarowych (dymu i płomienia).
- **Stanowisko 18 „System Kontroli Dostępu”.** Jest ono przeznaczone do badań w zakresie konfiguracji, programowania, eksploatacji i możliwości funkcjonalnych systemów kontroli dostępu. Składa się ono z: centrali kontroli dostępu CPR32-SE, interfejsu komunikacyjnego USB-RS232 typu UT-2USB, kontrolera zintegrowanego z

czytnikiem PR621, czytnika zbliżeniowego PRT66LT, kontrolera zintegrowanego z czytnikiem PR611, czytnika zbliżeniowego z klawiaturą PRT64LT, kontrolera zintegrowanego z czytnikiem PR311SE, czytnika zbliżeniowego PRT12LT-BK, modułu rozszerzeń wej./wyj. XM-2, kontrolera z zasilaczem PR411DR, czytnika zbliżeniowego PRT62LT, symulatorów wej./wyj.

- **Stanowisko 19 „Bezprzewodowy System Bezpieczeństwa Agility".** Jest ono przeznaczone do badań w zakresie konfiguracji, programowania, eksploatacji i możliwości funkcjonalnych bezprzewodowych Systemów Sygnalizacji Włamania i Napadu. Składa się ono z: centrali alarmowej Agility Wireless, szyfratora LCD z czytnikiem zbliżeniowym, modułu wejścia/wyjścia z wbudowanym interfejsem X10, detektora zewnętrznego PIR, detektora PIR, detektora PIR/PET, detektora stłuczenia szkła, detektora wstrząsowego detektora zalania, kontaktronu, sterownika zdalnego, pilota 4-przyciskowego, pilota sygnalizacji napadu, pilota sygnalizacji napadu w wersji „zegarek", sygnalizatora zewnętrznego (akustyczno-optyczny).
- **Stanowisko 20 „Zintegrowany System Bezpieczeństwa ProSYS".** Jest ono przeznaczone do badań w zakresie konfiguracji, programowania, eksploatacji i możliwości funkcjonalnych urządzeń bezprzewodowych (czujek i modułów) w Systemach Sygnalizacji Włamania i Napadu. Składa się ono z: płyty głównej ProSYS, klawiatury dotykowej z czytnikiem zbliżeniowym, klawiatury LCD, modułu rozszerzenia 8-liniowego, zasilacza impulsowego 3A (SMPS), zaawansowanego modułu komunikacji IP, interaktywnego modułu głosowego, modułu nasłuchu, modułu zintegrowanej kontroli dostępu, czytnika kart zbliżeniowych, modułu 44-wyjść przekaźnikowych, rozszerzenia bezprzewodowego 8-liniowego, 4-przyciskowego pilota bezprzewodowego, detektora przemysłowego WATCHIN, detektora zewnętrznego WATCHOUT, detektora dualnego serii i WISE, detektora PIR serii Zodiac, detektora zbicia szkła, detektora wstrząsowego, kart zbliżeniowych.
- **Stanowisko 21** centralne **„Zdalne zarządzanie elektronicznymi systemami bezpieczeństwa".** Jest ono przeznaczone do badań w zakresie zdalnego zarządzania Systemami Sygnalizacji Włamania i Napadu, Systemami Monitoringu Wizyjnego, Systemami Kontroli Dostępu, Systemami ochrony terenów zewnętrznych z wykorzystaniem analogowej i cyfrowej sieci telefonicznej, sieci komputerowej i interfejsów komunikacyjnych wykorzystujących RS-232 i RS-485. Składa się ono z: komputera z oprogramowaniem (DLOADX, GUARDX, DLOAD10, IP Setup Program, Real Shot Manager) dołączonego do sieci komputerowej umożliwiającej połączenie się z wymienionymi wcześniej stanowiskami badawczymi, linii telefonicznej analogowej, modułu cyfrowej telefonii komórkowej GSM.
- **Stanowisko centralne 22**: **„ Kompleksowe Zarządzanie siecią",** Jest to proaktywne monitorowanie sieci, inwentaryzacja sprzętu i oprogramowania, monitorowanie użytkowników, ochrona danych przed wyciekiem, zdalna pomoc techniczna - w jednym, centralnie zarządzanym programie. Program zawiera szereg modułów i tak: moduł Network monitoruje serwery pocztowe i adresy WWW, serwisy TCP i Windows, stan i działanie aplikacji oraz switche i routery (mapowanie portów i ruch sieciowy). Sieć jest wykrywana automatycznie i prezentowana interaktywnie na mapach. Moduł Users monitoruje i raportuje aktywność użytkowników pracujących na komputerach Windows: faktyczny czas aktywności (pracy), użytkowanie programów, odwiedzane strony WWW oraz transfer sieciowy. Moduł HelpDesk umożliwia udzielanie pomocy technicznej użytkownikom poprzez zdalny dostęp do stacji roboczych, pomaga szybko i skutecznie rozwiązywać zgłaszane problemy. Moduł DataGuard zarządza prawami dostępu do wszystkich portów wejścia i wyjścia oraz urządzeń fizycznych, przez które

użytkownik może skopiować pliki z komputera firmowego lub uruchomić na nim program zewnętrzny.

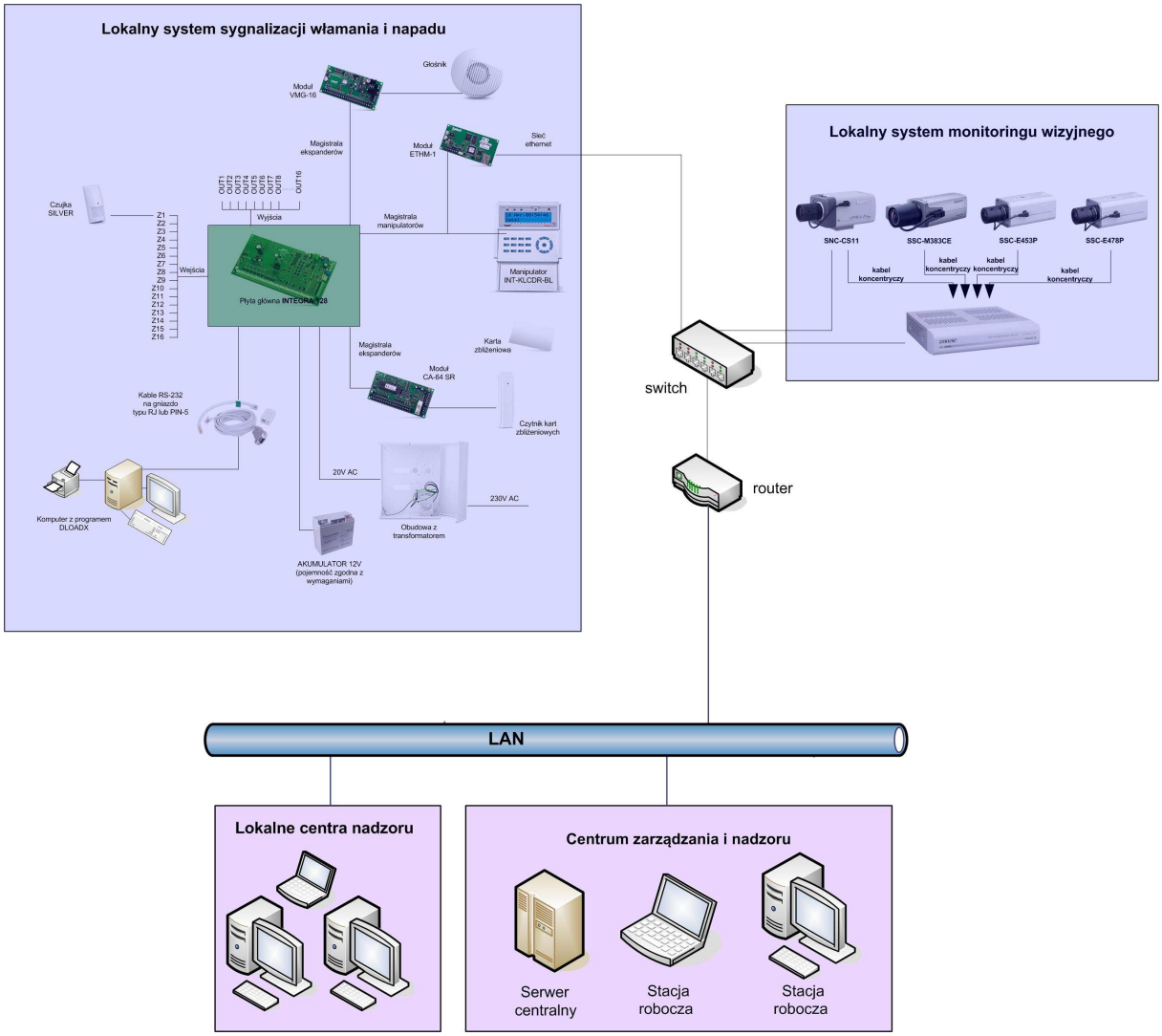
- **Stanowisko 23: Bezprzewodowy system alarmowy typu: OASiS Firmy JABLOTRON.** System SWiN czeskiej firmy JABLOTRON to bezprzewodowy system alarmowy o bardzo uniwersalnej logistyce. Ma ona wiele unikalnych funkcji. Elektroniczny system bezpieczeństwa jest wyposażony we wszystkie spotykane czujniki.
- **Stanowisko 24: „Wizyjny bezprzewodowy system bezpieczeństwa typu EYE-02"** Urządzenie bezprzewodowe rejestrujące obraz a więc i ruch o transmisji alarmu po GSM. Jest nadzorowana praca tej kamery za pośrednictwem komputera.
- **Stanowisko 25: „Badanie zasilaczy analogowych i impulsowych"** Zasilacze są przeznaczone do zasilania wszystkich elektronicznych systemów bezpieczeństwa. Aktualnie Uczelnia posiada 12 typów różnych zasilaczy przeznaczonych dla potrzeb dydaktycznych jak i badawczych. Wszystkie zasilacze to zewnętrzne urządzenia do zasilania elektronicznych systemów bezpieczeństwa. To zasilacze o napięciu wyjściowym U_{WY} = 12V i U_{WY} = 24V. Urządzenia są przystosowane do pracy buforowej z akumulatorami żelowymi. Te bardziej skomplikowane maja nadzór mikroprocesorowy. Zasilacze są firmy PULSAR, która współpracuje z Uczelnią.
- **Stanowisko 26: „Badanie Dźwiękowych Systemów Ostrzegawczych (DSO)".** Stanowisko typu VM-3000 to bardzo nowoczesny zintegrowany dźwiękowy system ostrzegawczy z cyfrowym urządzeniem rozgłoszeniowym, wywołaniem głosowym i odtwarzaniem tła muzycznego. System VM-3000 (w tym systemy wbudowane) będzie współpracował z centralą pożarową firmy Schrack (choć mogą być i inne). Docelowo kompletny system sygnalizacji pożarowej będzie monitorowany drogami informatycznymi (przewodowymi) i radiowymi. Firma TOA Electronics Europe przekazała system VM-3000 dla potrzeb w/w Laboratorium zarówno badawczego jak dydaktycznego.
- **Stanowisko 27: „Badanie cyfrowych systemów domofonowych typu CDN.** Polska Firma z Poznania wprowadziła na polski rynek trzy typy cyfrowych systemów domofonowych i videodomofonowych bardzo wysokiej jakości. Centrala typu CDNP to jednostka z cyfrowym wybieraniem i wyświetlaniem numeru lokalu oraz funkcją kontroli dostępu. Domofony cyfrowe typu CDNP pozwalają na budowę złożonych systemów wielowejściowych dla dużych obiektów. Centrale umożliwiają także otwieranie drzwi przy pomocy kart zbliżeniowych. Centrale tego typu umożliwiają dołączenie 255 abonentów. Posiadają rozbudowany system monitoringu wizyjnego. Posiadają wejście USB przez które dokonuje się zmian programowych systemu. Stanowisko zostało tak zaprojektowane, ze poza aspektami dydaktycznymi jest możliwe prowadzenie różnych zagadnień naukowo-badawczych w zakresie programowania i transmisji sygnałów.
- **Stanowisko 28: „Badanie czujek współpracujących z SSNiW".** Stanowisko zawiera 25 typów różnych czujek (pasywnych i aktywnych), współpracujących z liniami dozorowymi. Stanowisko zawiera wszystkie spotykane typy czujek (PIR, PIR+µW, 4xPIR, stłuczenia szkła, wibracyjne, sejsmiczne, antymasking, magnetyczne, aktywny PIR (wielowiązkowy), obecność CO_2, obecność wody, obecność gazu.

W roku akademickim 2012-2013 zostanie wprowadzonych kolejnych kilka stanowisk zarówno dydaktycznych jak i naukowo-badawczych o charakterze zintegrowanym. Planowane są systemy dotyczące budynków inteligentnych o nadzorze informatycznym. Daleko zaawansowane są rozmowy z producentami - sponsorami, którzy obiecali dostarczyć: systemy czytników biometrycznych współpracujące z systemami Kontroli Dostępu, systemy

sygnalizacji pożarowej firmy SCHRACK SECONET oraz systemy przywoławcze dla szpitali także w/w firmy oraz systemy monitorowania przewodowego i bezprzewodowego.

3. SYNTETYCZNY OPIS ZINTEGROWANYCH SYSTEMÓW BEZPIECZEŃSTWA WYKORZYSTUJĄCYCH PROTOKÓŁ TCP

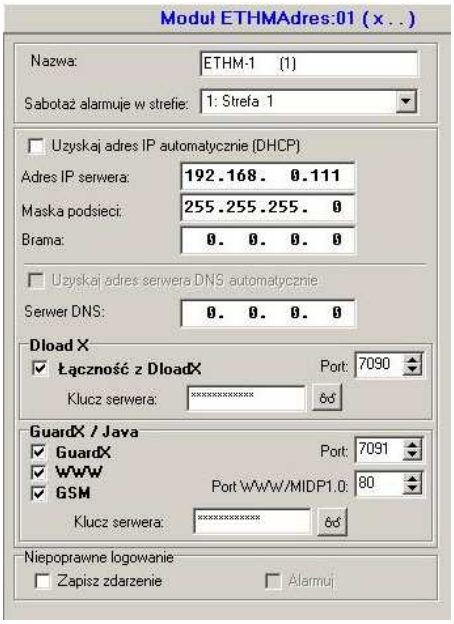
Rozwój nowoczesnych technologii informatycznych umożliwił bezpośrednie łączenie urządzeń systemów bezpieczeństwa z sieciami komputerowymi. Rozwiązanie to umożliwia podgląd zdarzeń z poszczególnych systemów zainstalowanych w różnych lokalizacjach geograficznych (nawet na różnych kontynentach) przy pomocy dowolnego komputera podłączonego do sieci Internet. Urządzenia wyposażone są w interfejs sieciowy oraz mają przydzielony własny adres IP. Na rys. 1 zobrazowano przykładowy zintegrowany system bezpieczeństwa z centrum zarządzania i nadzoru. Zintegrowany system bezpieczeństwa zbudowano z centrali Firmy SATEL typu INTEGRA 128 (stanowiący lokalny system sygnalizacji włamania i napadu) oraz lokalnego systemu monitoringu wizyjnego firmy SONY. Zintegrowany system bezpieczeństwa przedstawiony na rys.1 został dołączony do switch-a, a ten poprzez router do sieci LAN. Całość systemu jest sterowana i nadzorowana z komputerowego Centrum Zarządzania i Nadzoru.



Rys. 1. Zintegrowane systemy bezpieczeństwa z głównym centrum zarządzania i nadzoru

Źródło: opracowanie własne

Szczegółowa analiza zintegrowanych systemów bezpieczeństwa przedstawiona na rys. 1 z punktu widzenia zasady działania, ochrony danych, ochrony sieci, metod ochrony kryptograficznej byłaby bardzo obszerna. Autorzy zdecydowali się zatem tylko na przedstawienie tylko jednego zagadnienia związanego z ochroną przed nieuprawnionym dostępem do systemów. W tym celu posłużono się stanowiskiem do badania Systemów Sygnalizacji Włamania i Napadu. Na rys. 2 zobrazowano ustawienia modułu ethernetowego ETHM-1 służącego jako serwer TCP. Pozwala on obsługiwać centrale alarmową za pośrednictwem sieci LAN. Transmisja danych jest kodowana poprzez zastosowanie algorytmu wykorzystującego 192-bitowy klucz. Oczywiście niezbędne jest skonfigurowanie modułu poprzez podanie: adresu IP, maski podsieci, bramy oraz kluczy serwera i portów dla określonych programów[5].



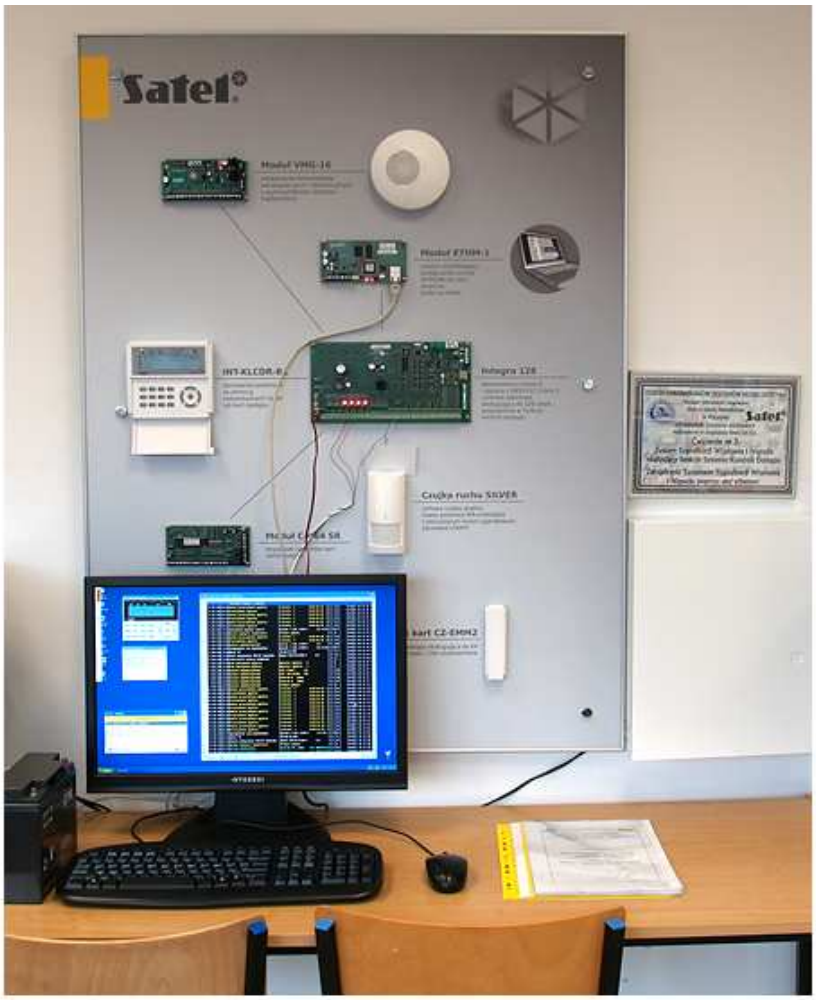
Rys. 2. Konfiguracja modułu ethernetowego ETHM-1(SATEL)

Źródło: opracowanie własne

Rys. 3. Stanowiska dydaktyczno – badawcze dot. monitoringu wizyjnego z nadzorem komputerowym (SONY)

Źródło: opracowanie własne

Na rys. 3 przedstawiono system monitoringu wizyjnego zbudowanego z 16 kamer. Kamera 17-ta (w lewej części fot.3) to kamera wysokiej jakości IP pracująca w sieci komputerowej. System monitoringu jest zintegrowany z INTEGRĄ 128 i zarządzany z centralnego komputera (Stanowisko centralne 22: „ Kompleksowe Zarządzanie siecią").



Rys. 4. Stanowisko dydaktyczno-badawcze dot. SSWiN typu INTEGRA 128 sterowane z komputera poprzez RS-232 z centralnym nadzorem komputerowym poprzez moduł ETHM-1 (SATEL)

Źródło: opracowanie własne

Stanowisko dydaktyczno – badawcze przedstawione na rys. 4 zostało dołączone do centralnego komputera sterującego poprzez moduł ETHM-1 do switch-a a ten do routera (rys. 1). Cały system współpracuje z siecią LAN. Stanowisku nadano adres IP.

PODSUMOWANIE

Na zakończenie warto wspomnieć, że nadrzędnym celem tego przedsięwzięcia było i jest kształcenie młodej kadry inżynierskiej w zakresie Inżynierii Bezpieczeństwa na przyzwoitym poziomie. Ze względu na unikatowy charakter stanowisk, są i będą prowadzone badania naukowe ze szczególnym uwzględnieniem ESB dla potrzeb obiektów o charakterze specjalnym jak również dla potrzeb nowego kierunku jakim jest Bezpieczeństwo Narodowe. Temu celowi podporządkowano budowę tego unikalnego rozwiązania. Rozbudowa i rozwój Zespołu Laboratoriów Systemów Bezpieczeństwa będzie nadal kontynuowany. Jest przy tym kładziony nacisk na integrację poszczególnych systemów m.in. poprzez zastosowanie sieci komputerowych z protokołem TCP. Autorzy podali tylko przykładowe rozwiązania stanowisk wynikających z układu przedstawionego na rys. 1 a dotyczących integracji stanowisk i ich zarządzania metodami informatycznymi.

RESAEARCH-TEACHING STANDS IN SECURITY SYSTEMS LABORATORIES OF PERSONS AND PROPERTY SUPPORTED WITH COMPUTERS

Abstract

The paper presents problems connected with security systems. In particular, it is considered the possibility of their integration by the application of the LAN using TCP protocol. That allows for the remote management and supervision. In the paper both teaching and research aspects of the problem are discussed.

BIBLIOGRAFIA

1. Hołyst B.: *Terroryzm. Tom 1 i 2*. Wydawnictwo prawnicze LexisNexis, Warszawa 2009.
2. Instrukcje laboratoryjne dotyczące systemów monitoringu wizyjnego przeznaczone dla studentów specjalności „Bezpieczeństwo obiektów i informacji" w Wyższej Szkole Menedżerskiej w Warszawie na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa.
3. Instrukcje programowania, serwisowe i użytkowników systemów monitoringu wizyjnego.
4. Materiały firmy SONY dotyczące CCTV IP i CCTV.
5. Materiały firmy SATEL (INTEGRA 128) dotyczące SSWiN oraz oprogramowanie.
6. Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
7. Norma PN-EN 50132-7:2003: Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 7: Wytyczne stosowania.
8. Szulc W. Rosiński A.: *Prace własne dot. Elektronicznych Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie*. Warszawa 2008-2012.
9. Szulc W. Rosiński A.: *Systemy sygnalizacji włamania. Część 3 – Magistrale transmisyjne i metody transmisji danych*. Zabezpieczenia Nr 4(68)/2009, Warszawa, wyd. AAT 2009.

Autorzy:
doc. dr inż. Waldemar SZULC – Wyższa Szkoła Menedżerska w Warszawie
dr inż. Adam ROSIŃSKI – Wyższa Szkoła Menedżerska w Warszawie