

NADCHODZI WYJĄTKOWE WYDARZENIE W BRANŻY BEZPIECZEŃSTWA

Najważniejsze w Europie Środkowo-
-Wschodniej spotkanie poświęcone
tematyce bezpieczeństwa biznesu.

Dołącz do nas.

20 - 21 listopada 2014, Warszawa



www.business-security-conference.pl

**Business
Security
Conference** 6th EDITION
**Change Your Business
Perspective**

ORGANIZATORZY



Zabezpieczenia techniczno-ochronne zakońców karnych i aresztów śledczych

Cezary Mecwaldowski

**Ochrona
Mienia
i Informacji**

WIARYGODNY I SPRAWDZONY

wykonawca zamówień publicznych
W USŁUGACH BEZPIECZEŃSTWA

// RZETELNOŚĆ WYKONAWCZA

// UCZCIWA KONKURENCJA

// TRANSPARENTNOŚĆ BIZNESOWA

// Fizyczna ochrona osób i mienia // Monitoring
// Zarządzanie dokumentacją // Cash Handling

Monitoring osób skazanych

IMPEL SECURITY POLSKA Sp. z o.o.
ul. Śleźna 118, 53-111 Wrocław





NADCHODZI WYJĄTKOWE WYDARZENIE W BRANŻY BEZPIECZEŃSTWA

Najważniejsze w Europie Środkowo-
-Wschodniej spotkanie poświęcone
tematyce bezpieczeństwa biznesu.
Dołącz do nas.

20 - 21 listopada 2014, Warszawa



www.business-security-conference.pl

**Business
Security
Conference** 6th EDITION
Change Your Business
Perspective

ORGANIZATORZY



Zabezpieczenia techniczno-ochronne zakońców karnych i aresztów śledczych

Cezary Mecwaldowski

WIARYGODNY I SPRAWDZONY

wykonawca zamówień publicznych
W USŁUGACH BEZPIECZEŃSTWA

// RZETELNOŚĆ WYKONAWCZA

// UCZCIWA KONKURENCJA

// TRANSPARENTNOŚĆ BIZNESOWA

// Fizyczna ochrona osób i mienia // Monitoring
// Zarządzanie dokumentacją // Cash Handling



IMPEL SECURITY POLSKA Sp. z o.o.
ul. Ślężna 118, 53-111 Wrocław
infolinia: **800 190 911**
e-mail: cc.ochrona@impel.pl
www: impel.pl



Monitoring osób skazanych
– System Dozoru Elektronicznego
Jest bezpiecznie.



Ochrona
Mienia
i Informacji



OBSŁUGA



CELA/KORYTARZ



XE P-1B-CELL1

WEJŚCIE/BRAMY



PAD IP VIDEO PANEL

MONITORING



SUPERVISOR



CASTEL SERWER MAX

Cezary Mecwaldowski

Zabezpieczenia techniczno-ochronne zakońdów karnych i aresztów śledczych

**Ochrona
Mienia
i Informacji**

Euro-Media Sp. z o.o. 2014

Copyright © by Euro-Media Sp. z o.o.
Warszawa 2014

Prawa autorskie zastrzeżone. Przedruk i wykorzystywanie materiałów możliwe tylko po uzyskaniu pisemnej zgody Wydawcy. Redakcja nie ponosi odpowiedzialności za treść reklam, ogłoszeń oraz artykułów firmowych, ani za opinie wyrażone w artykułach, które pozostają prywatnymi opiniami Autorów.

Wydanie pierwsze

Redakcja:
Katarzyna Dąbrowska
Tomasz Serafin

Reklama:
Katarzyna Kalata-Kiebleisz

Projekt okładki:
As-Art. Violetta Nalazek

Zdjęcia: Jan Kempa, Katarzyna Dąbrowska, www.flickr.com

ISBN 978-83-9383-461-7

Euro-Media Sp. z o.o., Al. Komisji Edukacji Narodowej 95
02-777 Warszawa, tel. +48 22 678 37 30
redakcja@ochrona-mienia.pl

Skład i łamanie: As-Art. Violetta Nalazek

Wydrukowano w Polsce
ArtDruk Zakład Poligraficzny

Spis treści

Wstęp	4
Służba Więzienna	5
Zabezpieczenia techniczno-ochronne, środki alarmowania i łączności	10
Wymagania dla zabezpieczeń elektronicznych – założenia systemowe	14
Urządzenia do kontroli, detektory oraz łączność	26
Podsumowanie	30
O Autorze	31
Literatura	32
Technika zabezpieczeń dla jednostek penitencjarnych	33
Drzwi do cel firmy DONIMET	35
Systemy skrytkowe dla jednostek penitencjarnych	38
CASTEL – interkomowe Systemy bezpieczeństwa dla więziennictwa	40
Nedap AEOS – optymalny sposób współdziałania systemów zabezpieczeń w obiektach Służby Więziennej	41
Rozwiązania w zakresie bezpieczeństwa	44
Inteligentne ogrodzenia – gwarancją bezpieczeństwa i 100% skuteczności	46



Wstęp

Opracowanie zawiera przegląd istniejących rozwiązań w zakresie zabezpieczeń techniczno-ochronnych, środków alarmowania i łączności oraz najnowsze trendy i koncepcje w ochronie zakładów karnych oraz aresztów śledczych. Ze względu na charakter i realizowane funkcje, zabezpieczenie jednostek penitencjarnych różni się od ochrony innych obiektów i po-

mieszczeń. Nieznajomość tych różnic prowadzi w konsekwencji do problemów na linii projektant – inwestor – wykonawca – inwestor. Poradnik ma na celu przybliżyć czytelnikowi wymagania funkcjonalne stawiane przez zabezpieczenia, co w założeniu autora ma zminimalizować błędy koncepcyjne i instalatorskie w inwestycjach realizowanych przez Służbę Więzienną.

Służba Więzienna

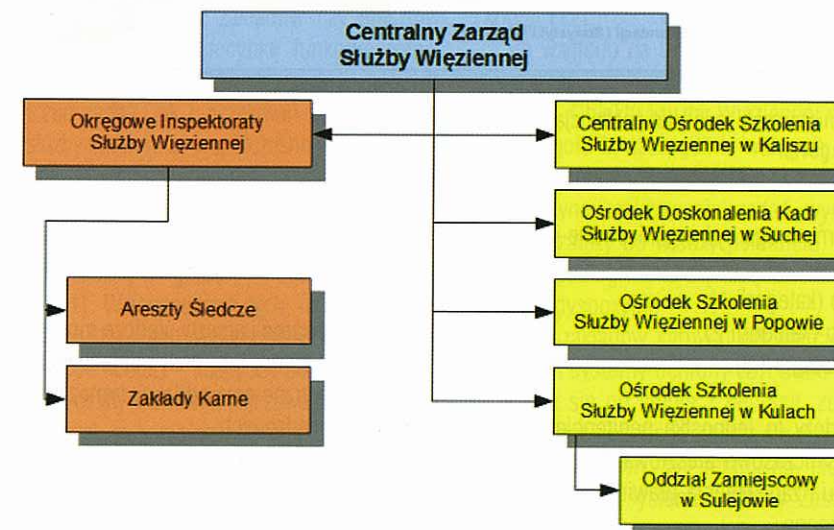
Służba Więzienna jest umundurowaną i uzbrojoną formacją apolityczną podległą Ministrowi Sprawiedliwości, posiadającą własną strukturę organizacyjną. Do podstawowych zadań Służby Więziennej należy [1]:

- prowadzenie oddziaływań penitencjarnych i resocjalizacyjnych wobec osób skazanych na karę pozbawienia wolności, przede wszystkim przez organizowanie pracy sprzyjającej zdobywaniu kwalifikacji zawodowych, nauczania, zajęć kulturalno-oświatowych, zajęć z zakresu kultury fizycznej i sportu oraz specjalistycznych oddziaływań terapeutycznych;
- wykonywanie tymczasowego aresztowania w sposób zabezpieczający prawidłowy tok postępowania karnego o przestępstwo lub przestępstwo skarbowe;
- zapewnienie osobom skazanym na karę pozbawienia wolności lub tymczasowo aresztowanym, a także osobom, wobec których są wykonywane kary pozbawienia wolności i środki przymusu skutkujące pozbawieniem wolności, przestrzegania ich praw, a zwłaszcza humanitarnych warunków bytowych, poszanowania godności, opieki zdrowotnej i religijnej;
- humanitarne traktowanie osób pozbawionych wolności;

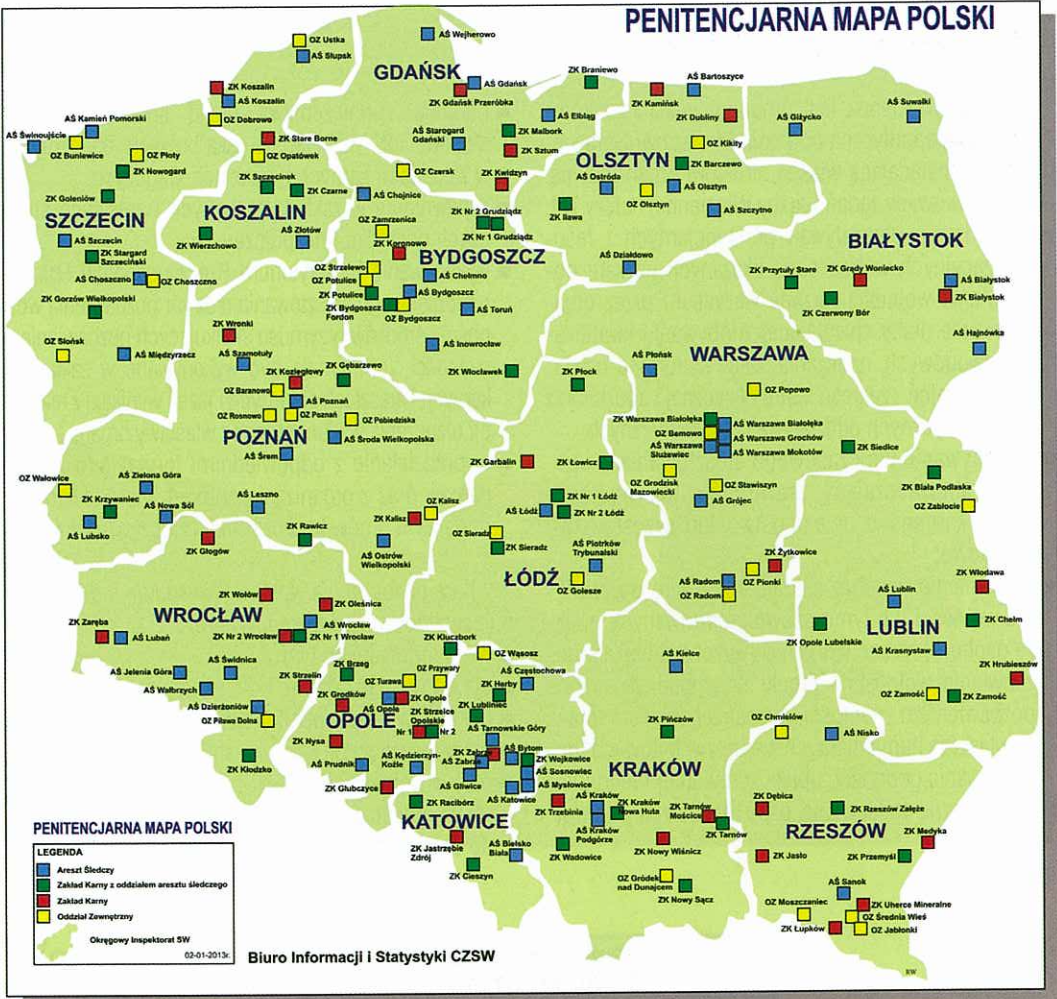
- ochrona społeczeństwa przed sprawcami przestępstw lub przestępstw skarbowych osadzonymi w zakładach karnych i aresztach śledczych;
- zapewnienie w zakładach karnych i aresztach śledczych porządku i bezpieczeństwa;
- wykonywanie na terytorium Rzeczypospolitej Polskiej tymczasowego aresztowania oraz kar pozbawienia wolności i środków przymusu skutkujących pozbawieniem wolności, jeżeli mają być wykonywane w zakładach karnych i aresztach śledczych i jeżeli wynikają z realizacji orzeczenia wydanego przez właściwy organ;
- współdziałanie z odpowiednimi formacjami innych państw oraz z organizacjami międzynarodowymi na podstawie umów i porozumień międzynarodowych.

Karę pozbawienia wolności wykonuje się w następujących rodzajach zakładów karnych:

- dla młodocianych (M),
- dla odbywających karę po raz pierwszy (P),
- dla recydywistów penitencjarnych (R),
- dla odbywających karę aresztu wojskowego (W),
- oraz w domach dla matki i dziecka dla osadzonych matek chcących sprawować opiekę nad dzieckiem do ukończenia trzeciego roku życia.



Rysunek 1. Schemat organizacyjny Służby Więziennej
Źródło: www.sw.gov.pl



Rysunek 2. Rozmieszczenie jednostek penitencjarnych
Źródło: www.sw.gov.pl

Zakłady karne mogą być organizowane jako zakłady karne typu:

- zamkniętego (kategorii 1),
- półotwartego (kategorii 2),
- otwartego (kategorii 3).

Areszt śledczy to jednostka penitencjarna, gdzie kierowani są tymczasowo aresztowani, w celu odbycia kary aresztu i zapewnienia prawidłowego toku postępowania karnego.

Jednostki penitencjarne różnią się w szczególności stopniem zabezpieczenia, izolacji skazanych oraz

wynikającymi z tego ich obowiązkami i uprawnieniami w zakresie poruszania się w zakładzie i poza jego obrębem.

Zakłady karne i areszty śledcze mogą posiadać oddziały w tej samej lub innej miejscowości i są to oddziały zewnętrzne oraz oddziały tymczasowego zakwaterowania osadzonych.

Niestety taki „krystaliczny” podział na typy zakładów karnych występuje rzadko. Najczęściej zakłady karne typu zamkniętego posiadają na swoim terenie np. oddział półotwarty, czy cały pawilon mieszkalny typu półotwartego/otwartego. Wtedy zasadą jest,

Tabela 1. Jednostki według liczby miejsc w dniu 31 grudnia 2013 r.

Liczba miejsc	Ogółem liczba jednostek	Areszty Śledcze	Zakłady Karne	Oddziały Zewnętrzne	Oddziały Tymczasowego Zakwaterowania Skazanych
Ogółem	197	69	87	37	4
do 49	5	—	—	1	4
50 – 99	18	7	1	10	
100 – 199	35	18	4	13	
200 – 299	30	12	13	5	
300 – 399	25	10	10	5	
400 – 499	19	5	12	2	
500 – 599	6	1	4	1	
600 – 699	13	1	12		
700 – 799	13	6	7		
800 – 899	7	1	6		
900 – 999	4	1	3		
1000 – 1099	13	5	8		
1100 – 1199	1	1	—		
1200 – 1299	3	—	3		
1300 – 1499	5	1	4		

Źródło: dane statystyczne [12].

że jednostka jako całość przyjmuje typ zakładu o wyższym poziomie zabezpieczenia. Równie często występuje sytuacja, w której areszty śledcze posiadają oddziały, gdzie umieszcza się skazanych skierowanych do odbywania kary w zakładzie karnym typu zamkniętego. Tego rodzaju sytuacja istotnie utrudnia działalność ochronną, ponieważ każdy z zakładów czy aresztów śledczych posiada swoją specyfikę funkcjonowania i zadania. Przekłada się to wprost na systemy ochrony.

Duża liczba zadań, jak i oczekiwań społeczeństwa względem służby sprawia, że współczesne więzienia stanowią złożoną strukturę w polskim systemie penitencjarnym [rys. 2]. Zapewne nie każdy zdaje sobie sprawę, iż wszystkie jednostki podstawowe Służby Więziennej w Polsce pełnią służbę 24 godziny na dobę i 7 dni w tygodniu [tabela 1]. W jednostkach tych, funkcjonariusze – a jest ich 27 571 (w tym 4883 kobiety) i pracownicy 1995 (w tym 1199 kobiet) – dbają aby powierzone ustawą [1] zadania zostały właściwie realizowane przy liczbie 78 994 osadzonych (w tym skazani/ukarani 72 405, tymczasowo aresztowani 6589, obcokrajowcy 521) [12].

Liczba miejsc, czyli pojemność zakładów karnych według stanu na 31 grudnia 2013 r. wynosiła łącznie 87 311 miejsc. Przy czym w jednostkach przebywało 78 994 osadzonych. W zakładach karnych typu za-

mkniętego przebywało 33 178 osadzonych, w zakładach karnych typu półotwartego 35 506 oraz w zakładach karnych otwartych 2742 [12].

W populacji osadzonych największą część stanowiły osoby w wieku 22-30 lat, dotyczyło to skazanych oraz tymczasowo aresztowanych zarówno mężczyzn jak i kobiet [12].

Ze względu na tematykę publikacji na uwagę zasługują szczególnie zadania związane z ochroną społeczeństwa. Obiekty Służby Więziennej należą do obiektów kategorii II, szczególnie ważnych dla bezpieczeństwa i obronności państwa [4].

Sprawne realizowanie zadań wymienionych we wstępie, zależy od wiedzy personelu, ale także umiejętności posługiwania się urządzeniami, techniką jaką mają do dyspozycji.

Typy zakładów karnych odzwierciedlają stosowane w nich systemy ochrony [5]. Choć systemy ochrony różnią się od siebie z definicji, zdarza się, że na terenie jednej jednostki stosuje się rozwiązania z innych systemów ochrony. Występują np. elementy pełnego i ograniczonego systemu ochrony. Zasadą jest, iż w tej sytuacji jednostka przyjmuje system o wyższym poziomie zabezpieczenia, czyli jak w podanym wyżej przykładzie – pełny system.

Tabela 2. Systemy ochrony a typy zakładów karnych

	Zakłady karne typu zamkniętego i areszty śledcze
	– cele mieszkalne skazanych mogą być otwarte w porze dziennej przez określony czas, jeżeli względy bezpieczeństwa nie stoją temu na przeszkodzie, – skazani mogą być zatrudniani poza terenem zakładu karnego w pełnym systemie konwojowania, – zajęcia kulturalno-oświatowe i sportowe oraz nauczanie organizuje się w obrębie zakładu karnego, – ruch skazanych po terenie zakładu karnego odbywa się w sposób zorganizowany i pod dozorem, – skazani mogą korzystać z własnej bielizny i obuwia, a za zezwoleniem dyrektora zakładu karnego – także z odzieży, – skazani mogą korzystać z dwóch widzeń w miesiącu, a za zgodą dyrektora zakładu karnego wykorzystać je jednorazowo, – widzenia skazanych podlegają nadzorowi administracji zakładu karnego; rozmowy skazanych w trakcie widzeń podlegają kontroli administracji zakładu karnego, – korespondencja skazanych podlega cenzurze administracji zakładu karnego, chyba że ustawa stanowi inaczej, – rozmowy telefoniczne skazanych podlegają kontroli administracji zakładu karnego.
	Zakłady karne typu półotwartego
	– cele mieszkalne skazanych pozostają otwarte w porze dziennej, natomiast w porze nocnej mogą być zamknięte, – skazani mogą być zatrudniani poza terenem zakładu karnego w systemie zmniejszonego konwojowania lub bez konwojenta, w tym również na pojedynczych stanowiskach pracy, – skazanym można zezwalać na uczestniczenie w nauczaniu, szkoleniu oraz w zajęciach terapeutycznych organizowanych poza terenem zakładu karnego, – skazani mogą brać udział w organizowanych przez administrację poza terenem zakładu karnego grupowych zajęciach kulturalno-oświatowych lub sportowych, – skazani mogą poruszać się po terenie zakładu karnego w czasie i miejscach ustalonych w porządku wewnętrznym, – skazani mogą korzystać z własnej odzieży, bielizny i obuwia, – skazanym można udzielać przepustek z zakładu karnego, nie częściej niż raz na dwa miesiące, łącznie na okres nie przekraczający 14 dni w roku, – skazani mogą korzystać z trzech widzeń w miesiącu, które za zgodą dyrektora zakładu karnego mogą być połączone, – widzenia skazanych podlegają nadzorowi administracji zakładu karnego; rozmowy skazanych w trakcie widzeń mogą podlegać kontroli administracji zakładu karnego, – korespondencja skazanych może podlegać cenzurze administracji zakładu karnego, – rozmowy telefoniczne skazanych mogą podlegać kontroli administracji zakładu karnego.

Tabela 2. Systemy ochrony a typy zakładów karnych – cd.

	Zakłady karne typu otwartego
	– cele mieszkalne skazanych pozostają otwarte przez całą dobę, – skazanych zatrudnia się przede wszystkim poza terenem zakładu karnego, bez konwojenta, na pojedynczych stanowiskach pracy, – skazanym można zezwalać na uczestniczenie w nauczaniu, szkoleniu oraz zajęciach terapeutycznych organizowanych poza terenem zakładu karnego, – skazani mogą brać udział w organizowanych przez administrację, poza terenem zakładu karnego, grupowych zajęciach kulturalno-oświatowych lub sportowych, – skazanym można zezwalać na udział w zajęciach i imprezach kulturalno-oświatowych lub sportowych organizowanych poza terenem zakładu karnego, – skazani mogą poruszać się po terenie zakładu karnego w czasie i miejscach ustalonych w porządku wewnętrznym, – skazani mogą korzystać z własnej odzieży, bielizny i obuwia, – skazani mogą otrzymywać z depozytu zakładu karnego pieniądze pozostające do ich dyspozycji, – skazanym można udzielać przepustek z zakładu karnego, nie częściej niż raz w miesiącu, łącznie na okres nie przekraczający 28 dni w roku, – skazany może korzystać z nieograniczonej liczby widzeń, – widzenia skazanych mogą podlegać nadzorowi administracji zakładu karnego. Rozmowy skazanych w trakcie widzeń nie podlegają kontroli administracji zakładu karnego, – skazanym, w miarę możliwości, stwarza się warunki do przygotowywania dodatkowych posiłków we własnym zakresie, – korespondencja skazanych nie podlega cenzurze administracji zakładu karnego, – rozmowy telefoniczne skazanych nie podlegają kontroli administracji zakładu karnego.

Źródło: na podstawie [2].



Zabezpieczenia techniczno-ochronne, środki alarmowania i łączności

Funkcjonowanie systemów ochrony realizowane jest w oparciu o ochronę fizyczną, a stosowane przez Służbę Więzienną przedsięwzięcia ochronne, polegają między innymi na stosowaniu zabezpieczeń techniczno-ochronnych, środków alarmowania i łączności [5].

Tabela 3. Zabezpieczenia techniczno-ochronne oraz środki sygnalizacji i łączności stosowane w zakładach karnych

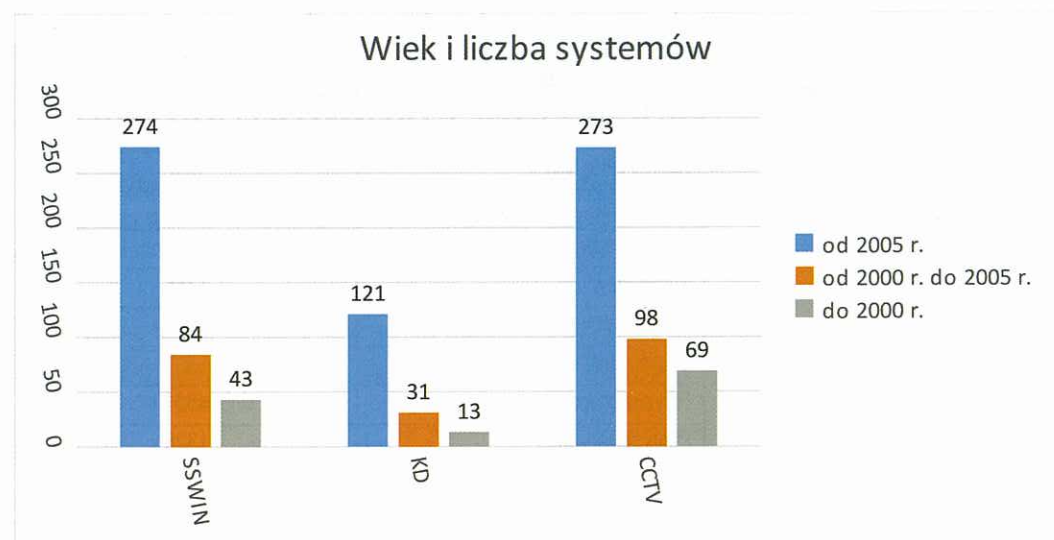
Zabezpieczenie	Opis/uzupełnienie
Linia zewnętrzna ogrodzenia ochronnego	– wykonana z materiału pełnego, która może stanowić również ścianą budynku, w którym mogą także czasowo lub na stałe przebywać osadzeni, albo wykonana z materiałów tworzących ogrodzenie ażurowe – wyposażoną w zabezpieczenia utrudniające jej pokonanie, mur, posterunki, concertina.
Linia wewnętrzna ogrodzenia ochronnego	– która może stanowić ogrodzenie pełne lub ażurowe albo może być oznaczona w inny sposób.
Wygradzenia wewnętrzne	– oddzielające poszczególne rejony jednostki organizacyjnej.
Bramy, drzwi i kraty	– o szczególnie silnej konstrukcji zamontowane przy wejściach do jednostki organizacyjnej i ważniejszych budynków.
Bramy, drzwi i kraty	– o silnej konstrukcji zamontowane przy wejściach i przejściach do poszczególnych budynków, rejonów i cel oraz pomiędzy kondygnacjami budynków.
Kraty okienne oraz wewnętrzne kraty koszarowe	– instalowane są za drzwiami wejściowymi i przed otworami okiennymi.
Przesłony i siatki	– o mocnej konstrukcji, montowane po zewnętrznej stronie okien.
Zamki i blokady do bram, drzwi i krat	– to zamki (klucze) i blokady mechaniczne, zamki – elektromechaniczne, zwory magnetyczne, elektrozaczepy, napędy do bram, samozamykacze, zasuwki, wizjery.
Agregat prądotwórczy lub inne zastępcze źródła energii elektrycznej i oświetlenia	– to agregat, UPSy, zasilacze buforowe, oświetlenie awaryjne, latarki.
Zabezpieczenia studzienek, kanałów, urządzeń wentylacyjnych, rynien, odgromników, słupów, masztów antenowych, kominów i innych punktów wysokościowych, świetlików, wejść na strychy i dachy oraz wejść do piwnic	– poprzez concertina, kraty, ostrza, pręty, siatki.
Urządzenia telewizji przemysłowej	– jako systemy telewizji przemysłowej CCTV.
Urządzenia kontroli dostępu	– czyli wszystkie elementy systemu kontroli dostępu.
Urządzenia do kontroli osób, bagaży, pojazdów i ładunków	– takie jak detektory metalu bramkowe, detektory metalu ręczne, detektory telefonów komórkowych, detektory narkotyków, skanery paczek i bagażu X-Ray, skanery osób X-Ray, skanery pojazdów X-Ray, detektory osób, elektroniki, kamery inspekcyjne, lustra inspekcyjne.
Instalacja przyzywowa	– interkomu w celach i przy przejściach, domofony i wideo domofony.
Środki łączności radiowej i przewodowej	– czyli łączność przewodowa, łączność bezprzewodowa, sieć strukturalna.
Środki alarmowania	– takie jak systemy alarmowe: SSWiN, SSP, integracje i wizualizacje, piloty napadowe, indywidualne sygnalizatory.

Źródło: opracowanie własne na podstawie rozporządzenia [5].

Tabela 4. Wielkość zabezpieczeń techniczno-ochronnych/elektronicznych

System [liczba niezależnych systemów]	Urządzenie	Ilość
Sygnalizacja włamania i napadu [412]	Centrale alarmowe	412
	Bariery (PIR, MW)	873
	Czujki ruchu (PIR, MW)	1683
	Kable sensoryczne	65
	Kontaktrony	1356
	Czujki inercyjne	158
	Czujki zalania wodą	6
	Przyciski napadowe	4521
	Piloty napadowe	1326
	Sygnalizatory	1069
Kontrola dostępu [169]	Akumulatory	1331
	Przejścia kontrolowane	2575
	Drzwi cel sterowane	441
	Czytniki kart	1762
Telewizja dozorowa [474]	Karty do kontroli dostępu	3859
	Kamery szybkoobrotowe	410
	Kamery wewnętrzne	8555
	Kamery zewnętrzne	4184
	Rejestratory video	962
	Monitory CCTV	2527
	Kamery w celi zabezpieczającej	305
	Kamery w celach mieszkalnych	797
	Systemy analogowe CCTV	449
	Systemy IP CCTV	8
Detektory	Systemy hybrydowe CCTV	17
	Bramki metali	267
	Ręczne metali	1874
	Skaner paczek X-Ray	145
	Skaner X-Ray osób	1
	Telefonów komórkowych przenośne	437
	Telefonów komórkowych zabudowane – system	1 (343 szt.)
Łączność bezprzewodowa	Stacja bazowa	177
	Ręczne radiotelefony serii GP	4253
	Stacje samochodowe	489
	Ładowarki akumulatorów	996

Źródło: stan na podstawie analizy z marca 2012 r. CZSW.



Rysunek 3. Wiek eksploatowanych systemów alarmowych w jednostkach Służby Więziennej
Źródło: analiza z 2012 r. CZSW

Zabezpieczenia techniczno-ochronne to zabezpieczenia mechaniczne, elektryczne i elektroniczne oraz

budowlane, stosowane w ochronie jednostki organizacyjnej [5].

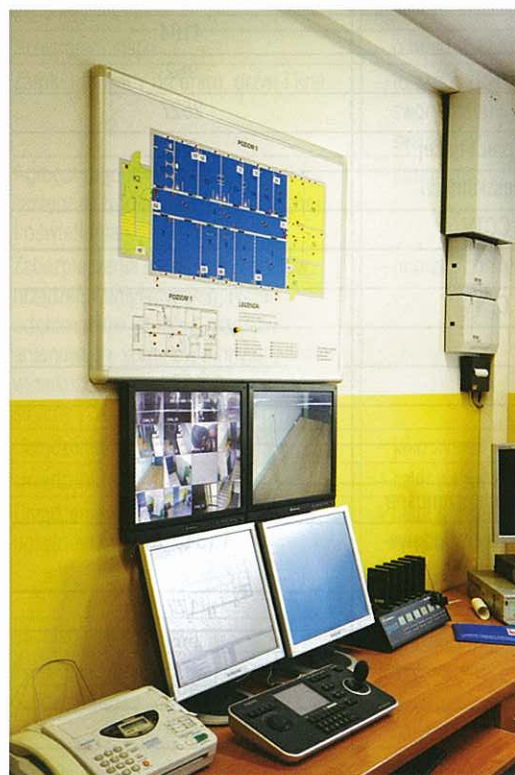
Zabezpieczenia techniczno-ochronne w jednostce organizacyjnej zależą przede wszystkim od systemu ochrony. To kierownik jednostki z kierownikiem ochrony tworzą plan ochrony, w którym między innymi określone są stosowane zabezpieczenia. Wytyczne [8, 9] narzucają procedurę, w której kierownik ochrony przygotowuje założenia funkcjonalne zabezpieczeń a na tej podstawie informatycy, funkcjonariusze działu kwatermistrzowskiego przygotowują założenia techniczne – specyfikację techniczną.

Co roku, w kwietniu i październiku realizuje się komisyjne przeglądy zabezpieczeń techniczno-ochronnych [5, 7]. Na ich podstawie sporządzany jest harmonogram planowanych prac, remontów, napraw.

Współczesne systemy zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej zaprezentowano w tabeli 3, natomiast w tabeli 4 wymienione są ilościowo systemy, a także ich elementy.

Biorąc pod uwagę wyniki przedstawione na rys. 3 oraz ostatnie inwestycje w systemy zabezpieczeń elektronicznych, można stwierdzić, iż większość systemów została uruchomiona, rozbudowana i zmodernizowana stosunkowo niedawno.

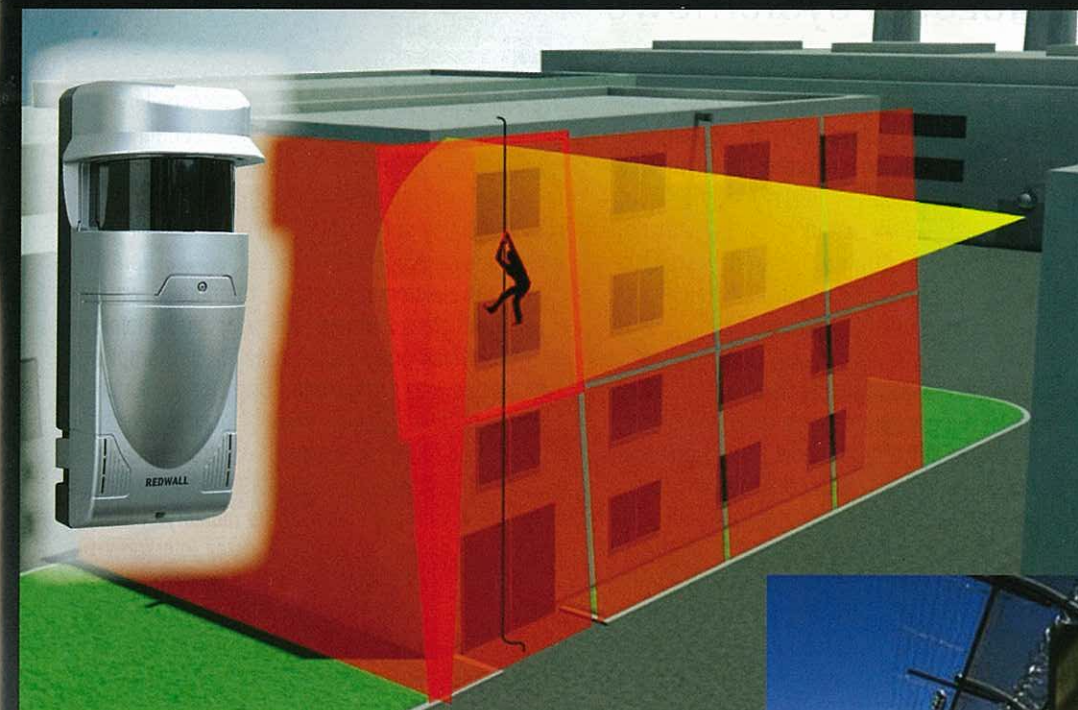
Kwestie eksploatacji systemów zabezpieczeń elektronicznych, informatycznych oraz łączności regulują zarządzenia [19, 20].



Quality detection system for video surveillance

REDWALL®
Unrivalled performance

LASEROWA CZUJKA SKANUJĄCA
RLS-3060SH



- Zasięg wykrywania: promień - 30m, kąt - maks. 190 stopni
- Przełączany tryb detekcji w pionie i w poziomie
- Łatwe dopasowanie obszaru detekcji do kształtu obiektu
- Wbudowany podgrzewacz; temperatura pracy od -40 do +90°C
- Inteligentny algorytm detekcji dopasowany do wymagań różnych aplikacji
- 4 niezależne strefy detekcji do sterowania kamerą PTZ, oświetleniem, sygnalizatorem itp. za pomocą wyjść przekąźnikowych
- 8 niezależnych stref detekcji z bezpośrednią komunikacją IP do oprogramowania nadzoru wizyjnego



www.optex.com.pl/redwall



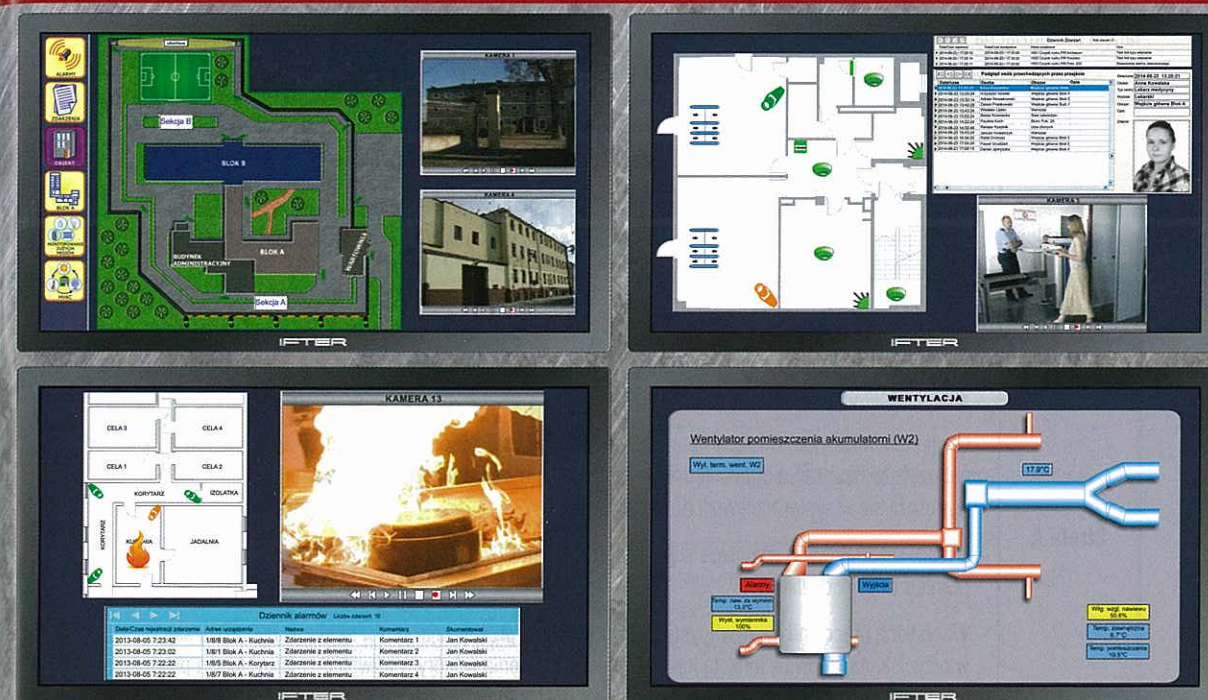
Wymagania dla zabezpieczeń elektronicznych – założenia systemowe

Z uwagi na największy postęp i kluczowe zmiany w zabezpieczeniach elektronicznych, zostały one szczegółowo przedstawione w prezentowanym materiale. Kwestie zabezpieczeń budowlanych i mechanicznych nie zmieniają się tak znacząco i są usystematyzowane w wytycznych [8,10], gdzie zawarte są informacje o materiale, średnicy krat, wysokości murów i wygrodzeń, sposobie montażu concertyny itp.

W lutym 2012 roku, na potrzeby prac nad wytycznymi związanymi z zabezpieczeniami elektronicznymi przeprowadzono w jednostkach Służby Więziennej analizę eksploatowanych systemów i urządzeń. Wynik analizy wskazał jednoznacznie, iż brak dotychczas jednolitych wytycznych spowodował zróżnicowanie w budowie systemów elektronicznych. Sposób ochrony pozostaje w gestii dyrektora jednostki, często determinowany był posiadanymi środkami w budżecie. Sytuacja ta powodowała również trudności szkoleniowe, ponieważ funkcjonariusze po odbyciu unitarnym szkoleniu wracali do różnie wyposażonych jednostek.

Jednym z pierwszych wdrożeń elektroniki do zabezpieczeń była telewizja dozorowa (obecnie w wielu

przepisach nadużywane nieprecyzyjne określenie monitoring). Przez długie lata był to tylko podgląd obrazu bez rejestracji. Następnie pojawiło się proste sterowanie wybranymi przejściami za pomocą tablicy przycisków, podających zasilanie bezpośrednio do elementów wykonawczych takich jak zamek elektromechaniczny lub elektromagnetyczny. Operator w wartowni obserwował obraz z kamer, przy przejściu zainstalowany był przycisk przywołania, zapalała się lampka sygnalizacyjna wraz z dźwiękiem. Operator po weryfikacji osoby w obrazie z kamer, otwierał przyciskiem przejście podając napięcie do zamka elektromechanicznego lub sztab magnetycznych. System ten funkcjonował przez lata w wielu jednostkach (w niektórych funkcjonuje nadal) ewoluując najpierw przez interkomu przy przejściach, umożliwiające dwustronną komunikację głosową, aż obecnie do systemów kontroli dostępu na karty zbliżeniowe. Wraz ze sterowanymi przejściami pojawiały się pierwsze przyciski napadowe. Przyciski te instalowano w wyznaczonych miejscach pełnienia służby lub pracy np.: posterunkach, dyżurkach wychowawców, ambulatorium. Działyły one na zasa-



Systemy Sygnalizacji Włamania i Napadu

Systemy Sygnalizacji Pożaru

Systemy Kontroli Dostępu

Automatyka Budynkowa

Telewizja Przemysłowa

Obsługa:

- ✓ OPC
- ✓ ModBus
- ✓ M-Bus
- ✓ BACnet
- ✓ SNMP
- ✓ Moduł SMS
- ✓ E-mail

Integracja produktów firm:

ADI, Algorinet, Aventura, Bosch, Compas, DSC, Geutebruck, Hikvision, Honeywell, Inim Electronics, Kantech, Panasonic Electric Works Fire & Security Europe, Polon Alfa, Risco, Roger, Satel, Schneider Electric, Schrack Seconet, Senstar, Siemens, System Sensor, Teletek, Tyco, Unicard, UTC Fire & Security i inni...

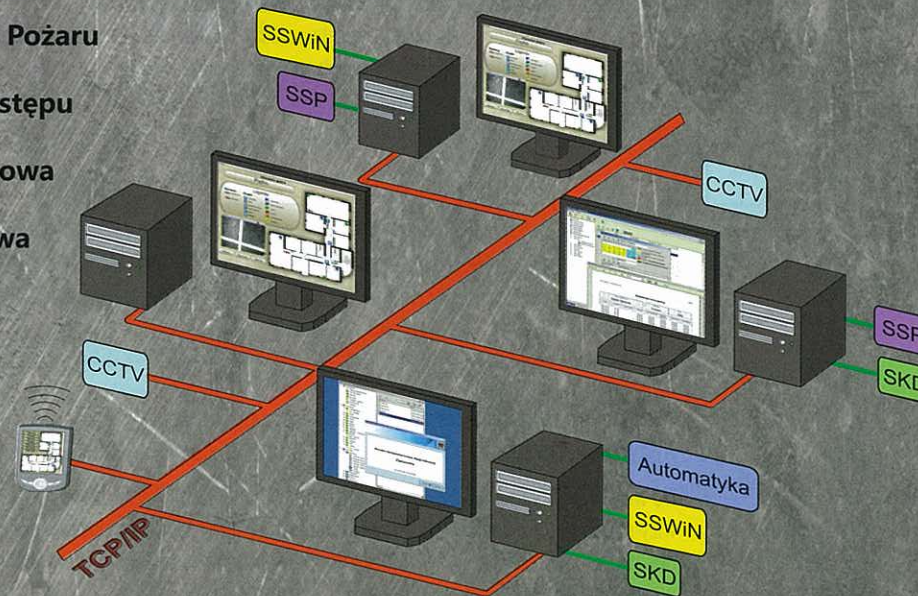


Tabela 5. Podział na strefy ochrony

Strefa A	Budynki zakwaterowania osadzonych – Wejścia i wyjścia do i ze strefy wyposaża się w system służowania (blokada wykluczająca). – Śluzę wyposaża się w system zapewniający obserwację bezpośredniego obszaru przed wejściem/wyjściem, system kontroli dostępu z pełną identyfikacją osób, system zapewniający sygnalizację otwarcia drzwi. – Wejście lub wyjście do i ze strefy wymaga podwójnej autoryzacji. – Przejścia w strefie wyposaża się w system kontroli dostępu i telewizji dozorowej. Wymagana jest pełna identyfikacja osób wchodzących i wychodzących. – Ciągi komunikacyjne, miejsca i pomieszczenia wyznaczone do: pracy, nauki, widzeń, odprawiania nabożeństw, spotkań religijnych oraz zajęć kulturalno-oświatowych, z zakresu kultury fizycznej i sportu wyposaża się w system telewizji dozorowej. – Dyżurki oddziałowych wyposaża się w urządzenia umożliwiające obserwację nadzorowanych pomieszczeń i oddziałów. – Wszystkich pracowników cywilnych i funkcjonariuszy przebywających w strefie A wyposaża się w przyciski napadowe z funkcją lokalizacji pomieszczenia w którym wywołano alarm. Alarm powinien być sygnalizowany na stanowisku dowodzenia oraz w dyżurce właściwego oddziałowego. – Włazy dachowe i klapy oddymiające wyposaża się w system sygnalizacji otwarcia. – Wyposażenie cel zabezpieczających, cel dla skazanych stwarzających poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu osadzonych w zakładzie karnym typu zamkniętego w warunkach zapewniających wzmoczoną ochronę społeczeństwa i bezpieczeństwo zakładu, cel tymczasowo aresztowanych zakwalifikowanych jako stwarzającego poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa aresztu regulują odrębne przepisy.
	Budynki bezpośrednio przyległe do budynków zakwaterowania osadzonych oraz wyznaczony obszar zewnętrzny przyległy do budynków zakwaterowania osadzonych i obiektów bezpośrednio do nich przyległych – W strefie B stosuje się system sygnalizacji włamania i napadu wyposażony w urządzenia wykrywające obecność osób. – Do weryfikacji alarmów z systemu sygnalizacji włamania i napadu stosuje się system dozoru wizyjnego oparty o kamery. Rozmieszczenie kamer musi zapewnić obserwację całego chronionego obszaru. Dopuszcza się stosowanie kamer obrotowych. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby.

Tabela 5. Podział na strefy ochrony – cd.

Strefa C	Pas ochronny, bramy wjazdowe i wyjazdowe oraz wejścia i wyjścia do i z terenu jednostki – Na pasie ochronnym stosuje się system sygnalizacji włamania i napadu wyposażony w urządzenia wykrywające obecność osób. – Do weryfikacji alarmów z systemu sygnalizacji włamania i napadu stosuje się system dozoru wizyjnego oparty o kamery stałopozycyjne. Rozmieszczenie kamer musi zapewnić obserwację całego pasa ochronnego bez martwych stref. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby. – Wejścia i wyjścia na i z pasa ochronnego wyposaża się w sygnalizację otwarcia. Dopuszcza się stosowanie systemów kontroli dostępu. – Bramy wjazdowe i wyjazdowe oraz wejścia i wyjścia piesze na i z terenu jednostki wyposaża się w system służowania (blokada wykluczająca). – Bramy, wejścia i wyjścia wyposaża się w sygnalizację otwarcia. Dopuszcza się stosowanie kontroli dostępu. – W śluzach dla pojazdów stosuje się system telewizji dozorowej zapewniający: ■ obserwację bezpośredniego, zewnętrznego obszaru przed bramą wjazdową na teren jednostki; ■ pełną identyfikację pojazdu znajdującego się wewnątrz śluzy; ■ obserwację podwozia i dachu pojazdu znajdującego się wewnątrz śluzy. – W śluzach pieszych stosuje się systemy zapewniające: ■ obserwację bezpośredniego obszaru przed wejściem i wyjściem na i z terenu jednostki; ■ kontrolę dostępu z pełną identyfikacją osób. – Stanowisko pracy bramowego wyposaża się w urządzenia umożliwiające monitorowanie i obserwację nadzorowanych przez niego obszarów.
	Strefa D – W strefie D stosuje się system telewizji dozorowej. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby.
Strefa E	Pomieszczenia i obiekty mające szczególne znaczenie dla bezpieczeństwa jednostki np.: serwerownie, magazyny, pola spacerowe, kancelarie tajne, magazyny broni, archiwa itd. – Pomieszczenia serwerowni wyposaża się w: ■ system kontroli dostępu; ■ system sygnalizacji włamania i napadu zapewniający detekcję dymu, ruchu, otwarcia drzwi, stłuczenia szyb i zalania wodą; ■ system monitorujący temperaturę i wilgotność powietrza; ■ system informujący o zaniku zasilania. – Pomieszczenia magazynów wyposaża się w system sygnalizacji włamania i napadu zapewniający detekcję dymu, ruchu i otwarcia drzwi. – Pola spacerowe wyposaża się w system telewizji dozorowej. Rozmieszczenie kamer musi zapewnić obserwację całego chronionego obszaru bez martwych stref. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby. Posterunek spacerowego w razie konieczności wyposaża się w urządzenia umożliwiające obserwację nadzorowanych pól spacerowych. – Sposób ochrony magazynów broni, kancelarii tajnych, archiwów określają odrębne przepisy.

Źródło: opracowanie własne na podstawie [9].

dzie zwykłego dzwonka czasami z sygnalizacją optyczną. Ciekawym rozwiązaniem była „cicha kontrola wartowników (posterunków)”. Był to system sygnalizatorów optycznych, kiedyś zwykłych lamp, rozlokowanych na terenie jednostki w miejscach podlegających obserwacji przez wartowników lub obszaru dozoru na posterunkach. Dowódca lub operator w wartowni łączył wybrany sygnalizator optyczny (lampę) i oczekiwał wyłączenia lub potwierdzenia zauważenia sygnału przez funkcjonariusza pełniącego służbę na posterunku.

Intensywna budowa systemów elektronicznych zabezpieczeń nastąpiła po roku 2000, a szczególnie od roku 2009, kiedy zaczęto odchodzić od obsadzania posterunków uzbrojonych. Rozbudowa – przebudowa systemów trwa nadal, skupiając się głównie na integracji i wizualizacji istniejących, eksploatowanych systemów oraz optymalizacji stanowisk operatorów-obszerników. Służba Więzienna dostosowuje elektronikę do obecnych potrzeb i funkcjonowania jednostki, oraz wprowadzanych zmian w przepisach (wytyczne czy chociażby monitoring video [2]). Często też nowe technologie wpływają na zmiany w samej Służbie Więziennej np. wideokonferencje, dostęp osadzonych do Internetu.

Różnorodność architektoniczna obiektów Służby Więziennej, lokalizacja obiektów na terenie jednostki, różne systemy ochrony sprawiają, że przyjęcie jednego rozwiązania jest praktycznie niemożliwe. Stworzono więc ogólne założenia budowy systemów zabezpieczeń elektronicznych [9] i mechanicznych [8], aby usystematyzować rozwiązania, które prezentują się następująco.

System sygnalizacji włamania i napadu (SSWiN) należy do podstawowych systemów alarmowych. W jednostkach organizacyjnych realizuje on następujące funkcje:

- napadową (stałe przyciski napadowe rozmieszczone w: dyżurkach oddziałowych, wychowawców, psychologów, w ambulatorium, u stomatologa, w kancelarii tajnej, w korytarzach oddziałów mieszkalnych, na posterunkach, w dyżurkach dozoru prac osadzonych – kuchnia, warsztaty, magazyny itp., stosowane są również piloty napadowe wśród oddziałowych, wychowawców, psychologów, funkcjonariuszy doprowadzających oraz realizujących spacer, widzenia. Jak również wyposażanie miejsc pracy kobiet-funkcjonariuszy i pracowników cywilnych);
- włamaniami (głównie ochrona obwodowa, realizowana za pomocą czujek ruchu, barier podczerw-

ni, mikrofalowych, kabli sensorycznych, czujek laserowych, czujek zbitcia szyby, wibracyjnych, kontaktów, czujek dymu itp. ale również pomieszczenia takie jak magazyny uzbrojenia, kancelarie tajne, serwerownie, archiwa, magazyny, wejścia/wyjścia z pawilonów mieszkalnych np. wyjścia ewakuacyjne, włączy bądź okna dachowe czy piwniczne).

Zasadniczą kwestią instalacji czujek w ochronie obwodowej jest miejsce i zasadność instalacji oraz prawdopodobieństwo powstawania fałszywych alarmów (spowodowanych np. przez zwierzęta). Należy przyjąć zasadę minimalizacji alarmów tak aby maksymalnie odciążyć obsługę systemów (operatora) od ich weryfikacji. Często ograniczona przestrzeń powoduje poważne kłopoty z doбором odpowiednich zabezpieczeń np. wąskie, zakręcające pasy ochronne lub bezpośrednio graniczące ściany pawilonów mieszkalnych, obszary gdzie występuje częsty ruch np. podczas podmiiany wartowników lub ruch funkcjonariuszy realizujących patrolowanie terenu. Jednostki znajdują się zarówno bezpośrednio w centrum dużych miast jak i daleko poza terenami zamieszkałymi, w lasach. Obecnie w ochronie obwodowej zakładów karnych stosuje się czujki: ruchu PIR+MW, bariery PIR i MW, kable sensoryczne zakopywane w ziemi, wieszane na wygradzeniu wewnętrznym, czujki laserowe.

Zgodnie z wytycznymi [9] system sygnalizacji włamania i napadu powinien być budowany w stopniu minimum Grade 3 zgodnie z normą PN-EN 50131-1. Ogólny podział systemów ochrony zakładów karnych na ochronę wewnętrzną i zewnętrzną o jakim czytamy w rozporządzeniu [5], wytyczne [9] uzupełniają w pięć stref, opisanych w tabeli 5.

System kontroli dostępu (SKD), często w jednostkach występuje sterowanie przejściami za pomocą przycisków a nie system kontroli dostępu definiowany normą. Takie „historyczne” rozwiązania odciągają uwagę operatora od obserwacji i dozoru chociażby obrazów z kamer podlegających obowiązkowemu dozorowi. Ta sama sytuacja dotyczy pseudosystemów kontroli dostępu, pomimo sterowania z komputera, gdzie operator steruje każdym przejściem w jednostce. Wytyczne [9] wprost mówią o tym, iż należy wprowadzać system kontroli dostępu, gdzie ruch po terenie jednostki odbywa się na podstawie nadanych uprawnień do kart zbliżeniowych. Przyjęty został standard kart zbliżeniowych jakim jest Mifare Plus.

PCSC
made in USA

ZAAWANSOWANY SYSTEM
KONTROLI DOSTĘPU
dla jednostek penitencjarnych

CZY MASZ WSZYSTKO POD KONTROLĄ?



**PCSC OD PONAD 31 LAT
ZAMYKA JEDNOSTKI PENITENCJARNE
W POLSCE I NA ŚWIECIE.**



POLSKI MISTRZ
TECHNIKI
ALARMOWEJ
2012

VOLTA
systemy zabezpieczeń
www.volta.com.pl



Karta elektroniczna traktowana jest jako klucz specjalny. Może umożliwiać otwarcie drzwi i krat wejściowych do budynków i oddziałów mieszkalnych oraz drzwi i krat przejściowych w ciągach komunikacyjnych tylko w zakresie niezbędnym do realizacji czynności służbowych wykonywanych przez jej użytkownika [7]. Do realizowanych systemów kontroli dostępu, Służba Więzienna wprowadziła RFID do legitymacji służbowej, która jest jednocześnie kartą kryptograficzną zawierającą klucze dostępu do baz danych jak i podpis elektroniczny. Karty wydawane są przez Centralny Punkt Certyfikacji w Centralnym Zarządzie Służby Więziennej. Jedynym wyjątkiem kontroli przejść wskazanym przez wytyczne jest wejście/wyjście z pawilonu mieszkalnego, gdzie zalecane jest stosowanie podwójnego potwierdzenia. Potwierdzenie otwarcia przejścia następuje przez operatora systemu. Stosować należy służby czyli gdy jedno przejście pobliskie jest otwarte, to drugiego, bezpośrednio następującego po nim, użytkownik nie może otworzyć dopóki nie zamknie pierwszego. Kolejną specyficzną funkcjonalnością jest zastosowanie centralnej blokady przejść. Sytuacja takiej blokady ma miejsce w przypadku wystąpienia zagrożenia bezpieczeństwa w oddziale mieszkalnym. Inicjowana jest przez operatora z wartowni, wtedy użytkownik pomimo uprawnień na karcie nie może otworzyć przejścia. We-

ryfikacja osoby następuje z systemu kontroli dostępu poprzez odczytanie karty i przypisanego do niej użytkownika oraz poprzez identyfikację w systemie telewizji dozorowej. Najlepiej poprzez integrację systemów, gdy po przyłożeniu karty do czytnika pojawiają się dwa obrazy na stanowisku operatora jeden to odczytane dane z karty i przypisany użytkownik np. ze zdjęciem, a drugi obraz to obraz z kamery w przejściu. Operator po weryfikacji albo blokuje przejście albo nie wykonuje nic i system automatycznie przepuszcza użytkownika.

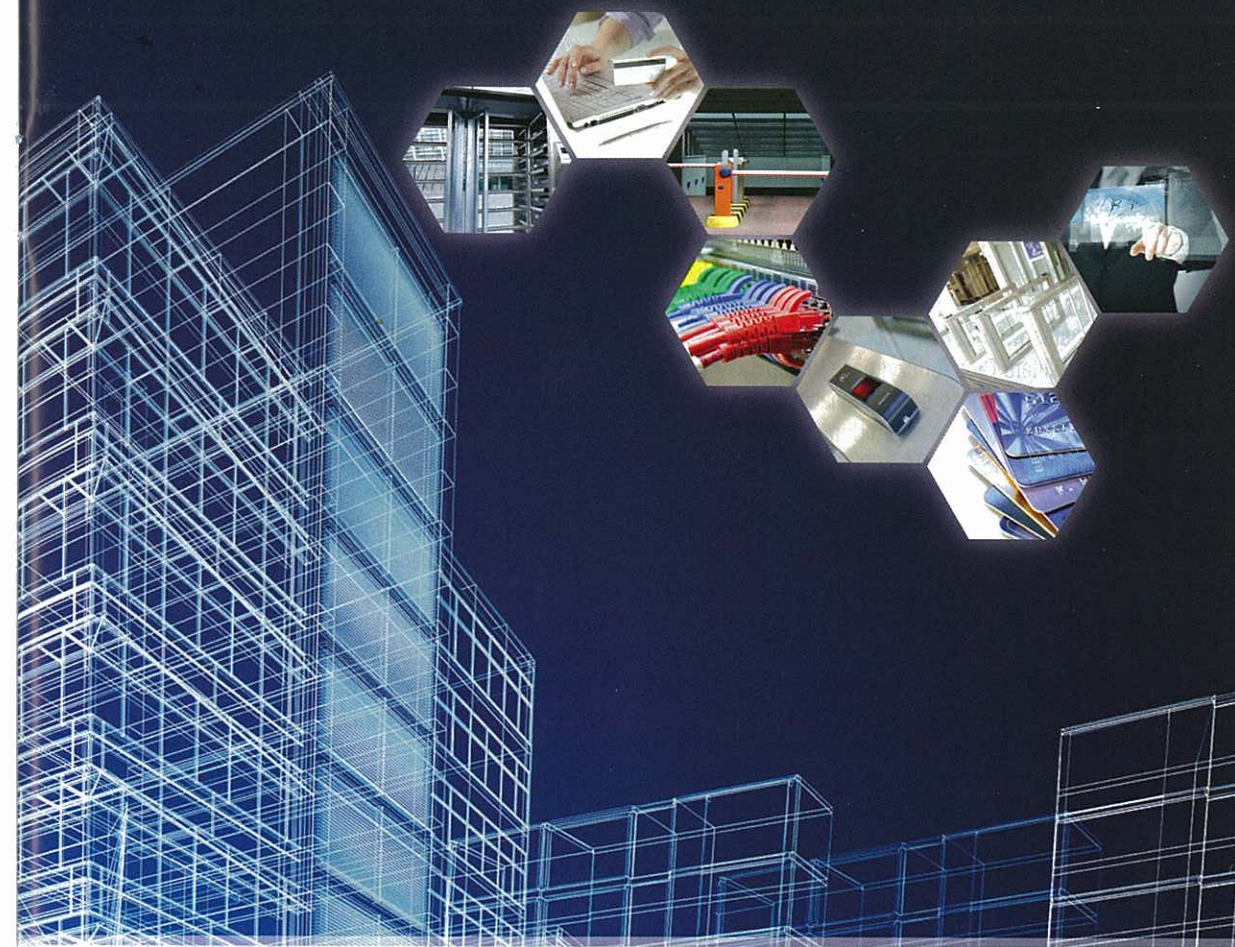
Podstawą otwierania drzwi cel nadal są klucze mechaniczne, których definicja w rozporządzeniu [5] jest następująca:

Klucze to również nośniki informacji w postaci kart elektronicznych służących do otwierania bram, drzwi lub krat.

Klucze specjalne to klucze od bram, drzwi i krat wejściowych do budynków, drzwi i krat przejściowych, cel mieszkalnych, cel zabezpieczających i cel dyscyplinarnych oraz wyznaczonych pomieszczeń.

Klucze zwykłe to klucze niewymienione powyżej.

Zamki, zwory elektromagnetyczne, elektroza-
czepty, zamki elektromechaniczne to elementy wykonawcze w systemach Kontroli Dostępu. Jakość tych urządzeń i właściwe dobranie do realizowanych funkcji gwarantuje ich sprawne funkcjonowanie. Jak wykazują



SYSTEMY BEZPIECZEŃSTWA DLA JEDNOSTEK PENITENCJARNYCH:

- KONTROLA DOSTĘPU
- REJESTRACJA CZASU PRACY
- DEPOZYTORY KLUCZY I BRONI
- SYSTEMY PARKINGOWE
- BEZPIECZEŃSTWO NA TERENIE OBIEKTU
- STABILNE I NOWOCZESNE ROZWIĄZANIE
- KARTY MIFARE PLUS, CZYTNIKI, OPROGRAMOWANIE
- PROJEKT, WDROŻENIE I SERWIS

UNICARD SA
ul. Łagiewnicka 54
30-417 Kraków

BIURO WARSZAWA
ul. Jagiellońska 78, 03-301 Warszawa
tel. 22 24 47 200, warszawa@unicard.pl

www.unicard.pl

doświadczenia jednostek są to jedne z najbardziej istotnych elementów wpływających na ruch osób i ich bezpieczeństwo w jednostce. Niewiele urządzeń dostępnych na rynku sprawdza się w tak trudnych warunkach więziennych w zakresie skrajnej eksploatacji, szczególnie pod kątem wytrzymałości mechanicznej, sposobu zasilania oraz kompatybilności elektromagnetycznej.

Wytyczne [9] określają minimum wymagań stawianych systemom kontroli dostępu:

- należy stosować kontrolery drzwi z niezależnym zasilaniem buforowym, które po utracie komunikacji z jednostką nadrzędną nadal umożliwiają realizację kontroli i sterowania przejściem,
- należy stosować czytniki kart zbliżeniowych w standardzie Mifare Plus, odczytujące nr zapisany w sektorze pamięci zabezpieczonym hasłem,
- do komunikacji z czytnikiem dopuszcza się protokoły Wieganda, RS485 i TCP/IP,
- okablowanie systemu należy zabezpieczyć przed dostępem, uszkodzeniem i sabotażem,
- należy stosować śruby z zabezpieczeniem, tak aby usunięcie czytnika wymagało specjalnego narzędzia,
- pojedyncze przejście (drzwi/krata) należy wyposażać w czytniki kart, kontaktryony oraz zamek elektromechaniczny (oraz system telewizji dozorowej wg parametrów opisanych w wytycznych),

- przejścia należy wyposażać w obustronną pełną identyfikację, wejścia do pomieszczeń (np. serwerownia, magazyn) pełna identyfikacja jednostronna (wewnątrz klamka lub przycisk wyjścia),
- przejścia (drzwi/kraty) powinny posiadać możliwość mechanicznego otwarcia kluczem w przypadku awarii systemu kontroli dostępu,
- system kontroli dostępu powinien dostarczać sygnały z przejść takie jak: otwarte, zamknięte, uszkodzenie/sabotaż, otwarcie nieautoryzowane.

Stany te powinny być zapisywane w dzienniku zdarzeń systemu.

System telewizji dozorowej (telewizji przemysłowej, CCTV), często określany w różnych przepisach jako monitoring. Jako jeden z pierwszych systemów instalowanych w jednostkach, podlegał przez lata różnym modernizacjom co spowodowało, iż w wielu obiektach znajdują się stare kamery jeszcze czarno białe, o niskich rozdzielczościach, przemieszane z nowymi rozwiązaniami. Statystycznie na jednostkę przypada ok 83 kamer. Istotne jest przy organizacji stanowiska operatora/obserwatora stworzenie odpowiednich, ergonomicznych warunków pracy aby uzyskać oczekiwaną skuteczność obserwacji.

Ta skuteczność nabiera szczególnego znaczenia gdy rozpatruje się dwa aspekty dozoru wideo w zakła-

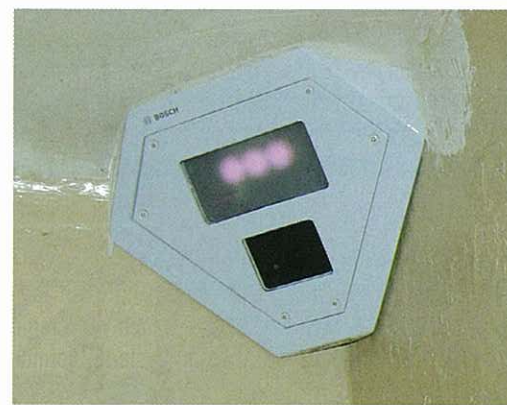


dach karnych. Fakultatywna obserwacja (art. 73a [2], obserwacja terenu, pomieszczeń itp.) i obligatoryjna obserwacja: dotyczy obserwacji osadzonych w celach (art. 88c i 212c [2], kamera w celi mieszkalnej, izolacyjnej decyzją dyrektora oraz obligatoryjnie w celi zabezpieczającej [11]). Należy rozróżnić sytuację gdy obserwator posiada możliwość realizowania innych zadań poza obserwacją lub nie posiada takiej możliwości.

Stosowane są różne technologie od starych analogowych po mega pikselowe kamery IP, z oświetlaczami podczerwieni czy termowizyjne. Kamery w celach służą stałemu dozorowi osadzonych. Cele bywają niejednolite geometrycznie, bywa też, że posiadają sklepienia po łuku, bądź są to małe przestrzenie – co stawia spore wymagania od optyki kamery, jej obudowy i sposobu montażu. Zasadą jest, aby były to kamery wandaloodporne umożliwiające dozór również w nocy przy braku oświetlenia. Tu ze względów psychologicznych istotne jest, aby podświetlacze podczerwieni pracowały w zakresie niewidzialnym, tak aby nie było widać nocą żarzących się diod.

Wytyczne [9] określają minimalne wymagania jakie powinny spełniać systemy telewizji dozorowej uwzględniając rozporządzenie [6], a są to między innymi:

- Sposób zasilania wszystkich urządzeń wchodzących w skład telewizji dozorowej musi gwarantować ich nieprzerwaną, ciągłą pracę. W celu zapewnienia takiego funkcjonowania stosuje się zasilacze buforowe z akumulatorami i UPS-y. Obwody elektryczne stanowiące źródło zasilania dla zasilaczy buforowych i UPS-ów muszą być podłączone do agregatów prądotwórczych.



- Nowe zakłady karne i areszty śledcze wyposaża się w system telewizji dozorowej w technologii cyfrowej IP. Do budowy infrastruktury kablowej stosuje się normy dotyczące budowy okablowania strukturalnego.
- W przypadku modernizacji, rozbudowy lub naprawy istniejących systemów CCTV linie sygnałowe toru audio-wideo należy realizować na bazie skrętki komputerowej kategorii minimum 5e lub światłowodu i konwerterów sygnału. Przyjmuje się dla jednego toru audio-wideo jeden przewód skrętkowy. Umożliwi to w przyszłości płynne przejście do standardu CCTV IP.
- Rejestracja PAL – D1, minimum 3 klatki/sek. dla każdego strumienia audio-wideo.
- Pojemność archiwum nagrań dla każdego kanału minimum 7 dni.
- Kamery w kąciach sanitarnych, łazienkach muszą posiadać funkcje maskowania stref służące do maskowania stref intymnych.

Charakterystyczne miejsca montażu kamer

Poza opisanymi powyżej systemami alarmowymi, urządzeniami oraz wskazanymi w tabeli 2 opisami systemów ochrony, w zakładach karnych występują miejsca charakterystyczne, gdzie stosuje się dozór wideo:

- cela zabezpieczająca (obligatoryjnie obraz i dźwięk, należy zwrócić szczególną uwagę na jakość dźwięku ze względu na specyficzną budowę celi, oraz odpowiednią optykę kamery aby widoczna była cała ceta),
- ceta izolacyjna (decyzją dyrektora osadzonego poddaje się dozorowi wideo),
- ceta mieszkalna (decyzją dyrektora osadzonego poddaje się dozorowi wideo),
- cele i pomieszczenia oddziału dla osadzonych wymagających osadzenia w wyznaczonym oddziale bądź celi (art. 88c i 212c ustawy [2] obligatoryjnie),
- świetlice, kaplice, miejsca pracy osadzonych, biblioteka,
- sale widzeń dozorowanych i bezkontaktowych,
- place spacerowe,
- pasy ochronne, śluzy bram wjazdowych, teren jednostki,
- obszar przed bramą wjazdową na teren jednostki,
- przejścia, wejścia, wyjścia na terenie jednostki i w obiektach,
- obszar przy wejściu do kancelarii tajnej.

Przy doborze kamer należy uwzględniać wytyczne [18], w których wskazane zostały strefy i parametry

try oświetlenia (współczynniki) np. w ciągach komunikacyjnych, pasach ochronnych w obszarze obserwacji elektronicznej itp.

System sygnalizacji pożarowej (SSP)

Ze względu na specyfikę obiektów, Służba Więzienna występuje o odstępstwa w zakresie stosowania przepisów przeciwpożarowych. Systemy sygnalizacji pożarowej instalowane są z reguły w pomieszczeniach, a nie w całych obiektach. Tymi szczególnymi pomieszczeniami są: magazyn uzbrojenia, podręczny magazyn uzbrojenia, kancelaria tajna oraz archiwum. Ze względu na 24 godzinny dozór ochrony fizycznej, występujące warunki środowiskowe, działania osadzonych, którzy często dewastują sprzęt, palą papierosy, stosowanie w pawilonach mieszkalnych tak czułych systemów jakimi są systemy sygnalizacji pożarowej nie wydaje się racjonalne. Doświadczenia pojedynczych obiektów gdzie zainstalowano systemy sygnalizacji pożarowej potwierdzają tę tezę.

Wizualizacja i integracja systemów alarmowych

Ze względu na ograniczenia kadrowe z jakimi boryka się Służba, w obsłudze systemów alarmowych w jednostce organizacyjnej należy szczególnie zwracać uwagę, aby operator miał jak najprostszą, intuicyjną obsługę wspomnianych systemów. Zadanie to realizuje wizualizacja i integracja systemów alarmowych. Duża liczba zainstalowanych kamer jak i innych elementów systemów alarmowych, wymusza instalację systemów wspomagających pracę operatora-obszernika. Chociażby poprzez integrację czy możliwość przełączania wyświetlanych obrazów poprzez detekcję ruchu, inteligentną analizę obrazu (przekroczenie wirtualnej granicy lub obszarów, kierunku ruchu, analiza zdarzeń np. zbliżenie na określoną odległość więcej niż 2 osób itp.). Istotną rolę odgrywa tutaj ergonomia stanowiska obserwatora, odpowiedni układ wyświetlanych kamer, brak elementów zakłócających zarówno w obrazie (np. nadmiarowe opisy, dużo obszarów nieistotnych dla obserwacji takich jak widok nieba, sufitu, ścian itp.) jak i w samym pomieszczeniu obserwatora.

Interkomy, w zakładach karnych zainstalowane są w trzech rozwiązaniach, do komunikacji pomiędzy:

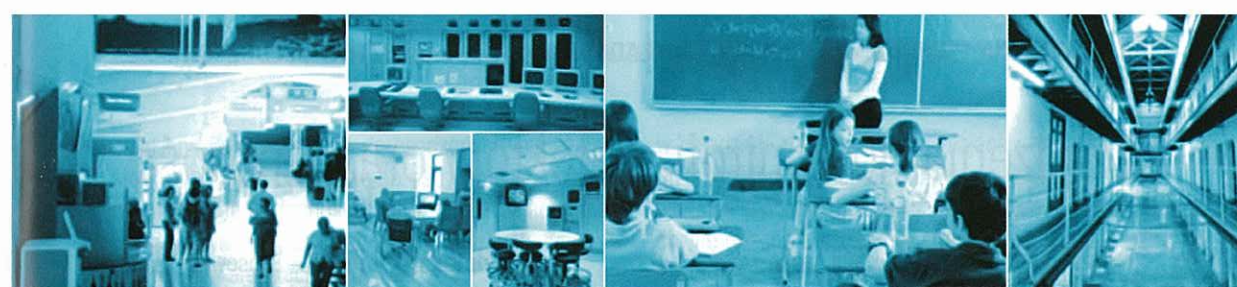
- osadzonymi w celach mieszkalnych, świetlicach a funkcjonariuszem oddziałowym,



- osadzonym a osobą na „widzeniu bezkontaktowym”, czyli widzeniu w sposób uniemożliwiający bezpośredni kontakt z osobą odwiedzającą [10],
- osobą przy przejściach w jednostce, a stanowiskiem operatora.

Są to niezależne systemy, które powinny spełniać określone wymagania: interkomy muszą być wandaloodporne, mogą zawierać dodatkowe funkcje jak np. radiowęzeł z przyciskami głośności. W celi mieszkalnej, na panelu wandaloodpornym mogą znajdować się również przyciski od napędu otwierającego okno (dotyczy np. cel izolacyjnych, dla osadzonych wymagających osadzenia w wyznaczonym oddziale lub celi [2]). Panel powinien posiadać specjalne śruby do których wymagany jest nietypowy klucz. Powinien też zawierać mechaniczne utrudnienia uszkodzenia głośnika oraz mikrofonu.

Wideodomofony, domofony bywają stosowane przy wejściach i bramach wjazdowych na teren jednostki, czasami w wybranych przejściach na terenie jednostki kiedy nie ma wdrożonego systemu kontroli dostępu.



N-8000 | SIECIOWY SYSTEM INTERKOMOWY



the future is **safe&sound**

TOA Poland • www.toa.pl



Urządzenia do kontroli, detektory oraz łączność

Służba Więzienna do realizacji zadań wykorzystuje różnego rodzaju urządzenia do kontroli. Funkcjonariusz wyposażony w urządzenia mechaniczne lub elektroniczne ma obowiązek wykorzystywania ich do każdej kontroli:

- osobistej lub pobieżnej osadzonych, osób z wolności;
- cel i innych pomieszczeń;
- paczek i przedmiotów;
- pojazdów,
- generalnej całego zakładu karnego.

Do ww. kontroli wykorzystuje się także psy [5].

To co może znajdować się na terenie jednostki, to co może do jednostki trafiać z zewnątrz, jak i to co może opuszczać jednostkę, regulują właściwe przepisy [2, 5].

Bramkowe detektory metali – stosowane przy wejściach do jednostek, niekiedy w oddziałach mieszkalnych. Często ze względu na zastane warunki architektoniczne występuje ograniczone miejsce do montażu tego rodzaju urządzeń. Pracują one w wąskich przejściach, często w pobliżu krat przejściowych, skanerów rentgenowskich, narażone są na pobliskie ruchome elementy metalowe. Im bardziej precyzyjnie urządzenie wskazuje miejsce detekcji tym lepiej. Szczególnie sprawdzają się urządzenia posiadające wiele stref detekcji.

Ręczne detektory metali – stosowane bardzo często, wyposaża się w nie funkcjonariuszy realizujących określone zadania/kontrole bądź przypisuje jako stałe wyposażenie posterunku, służą do kontroli osób, paczek, korespondencji, cel i pomieszczeń (materacy, rzeczy posiadanych przez osadzonych). Służba posiada różne modele detektorów, przy czym na uwagę zasługuje kwestia skuteczności oraz na ile taki detektor jest poręczny dla funkcjonariusza. Urządzenia te są intensywnie eksploatowane ze względu na ilość wykonywanych, różnych rodzajów kontroli.

Detektory narkotyków i materiałów wybuchowych

Służba Więzienna poza psami specjalnymi, przeszkolonymi do wykrywania narkotyków (w paczkach, korespondencji, na terenie, w pomieszczeniach, w celach mieszkalnych, jak i przez osoby wchodzące na teren jednostki penitencjarnej) stosuje również elektroniczne detektory narkotyków. Są to chromatografy gazowe, urządzenia przenośne bądź stacjonarne, działają na zasadzie spektrometrii lotnych jonów. Do rozpoznawania substancji, bądź spożycia substancji psychoaktywnych stosowane są testery chemiczne.

Skanery rentgenowskie (X-Ray) paczek – służą do prześwietlania paczek, które mogą otrzymywać

osadzeni, korespondencji do osadzonych jak i jednostek SW, a także bagaży, toreb osób ubiegających się o wstęp na teren jednostki lub je opuszczające. Znajdują się we wszystkich zakładach karnych typu zamkniętego i aresztach śledczych.

Skanery rentgenowskie (X-Ray) osób – służą do prześwietlania osób wchodzących na teren jednostki oraz wychodzących. Doskonałe narzędzie do kontroli, jednak ze względu na cenę występuje tylko w jednej jednostce penitencjarnej.

Skanery rentgenowskie (X-Ray) pojazdów – służą do prześwietlania pojazdów wjeżdżających do jak i wyjeżdżających. Kolejne doskonałe narzędzie do kontroli, jednak ze względu na wysoką cenę Służba Więzienna nie posiada takich urządzeń. W jednym z zakładów pracy gdzie pracują osadzeni stosuje się detektor tężna do wykrywania osób, które mogą znajdować się ukryte w pojeździe.

Detektory przenośne telefonów komórkowych. Rozwój technologii telefonii komórkowej w ostatnich latach jest bardzo intensywny. Należy zadbać, aby detektory telefonów komórkowych wykrywały wszystkie zakresy i technologie. Detektor stosowany w SW musi posiadać wyświetlacz, na którym wyświetli wskazanie maksymalne poziomu odebranego sygnału, powiadomi o detekcji dźwiękiem lub sygnałem świetlnym, zarejestruje w pamięci datę, godzinę i poziom sygnału.

Dobrze jeżeli detektor umożliwia detekcję innych technologii bezprzewodowych niż telefonia komórkowa a wykorzystywanych do komunikacji np. CDMA, Wi-Fi i inne. Użytkownik musi posiadać możliwość wglądu w rejestr bez możliwości kasowania (rejestr samonadpisujący).

System detektorów do lokalizacji telefonów komórkowych – zabudowany w różnych miejscach w pawilonie mieszkalnym np. w interkomach. Należy zadbać, aby detektory telefonów komórkowych wykrywały wszystkie zakresy i technologie. Do obsługi stosowany jest komputer, na którym wyświetlone będzie wskazanie maksymalne poziomu odebranego sygnału w grupie kilku detektorów, co na wizualizacji pokaże obszar gdzie znajdował się nadający telefon. W rejestrze zapisze się data, godzina i poziom sygnału oraz lokalizacja. Użytkownik musi posiadać możliwość wglądu w rejestr bez możliwości kasowania (rejestr samonadpisujący).

Detektory elektroniki – zarówno włączonej jak i wyłączanej. Jest to bardzo obiecujące rozwiązanie

w dziedzinie detektorów pozwalające uniezależnić się od technologii telefonii komórkowej. Pojawiają się rozwiązania w postaci bramek bądź urządzeń ręcznych. Na chwilę obecną Służba Więzienna nie posiada tych detektorów.

Kamery inspekcyjne – pojawiają się ostatnio w zakładach karnych. Służą do realizacji różnych rodzajów kontroli (poza kontrolą osób). Korzystają z nich też funkcjonariusze działów kwatermistrzowskich do konserwacji i remontów np. wglądu w instalacje wentylacyjne, kanały kablowe, nad sufity podwieszane itp.

Kamery taktyczne – pojawiają się ostatnio w jednostkach. Wykorzystywane są w sytuacjach zagrożenia bezpieczeństwa, interwencjach, przy stosowaniu środków przymusu bezpośredniego oraz podczas ćwiczeń.

Łączność przewodowa – dotychczasowa telefonia analogowa i cyfrowa jest obecnie sukcesywnie zamieniana na technologię VoIP, w celu optymalnego wykorzystania zasobów sieci WAN i obniżenia kosztów za połączenia pomiędzy jednostkami organizacyjnymi.

System wideokonferencji – w zestawy wideokonferencyjne wyposażone są Centralny Zarząd Służby Więziennej, Centralny Ośrodek Szkolenia Służby Więziennej, ośrodki szkolenia i doskonalenia, okręgowe inspektoraty i niektóre jednostki podstawowe. System ten wykorzystywany jest do prowadzenia zdalnych odpraw oraz szkoleń, znacząco pozwala ograniczyć koszty delegacji. Pozwala również nagrywać wideokonferencję. Widzą i słyszą się wszyscy uczestnicy, urządzenia umożliwiają podłączenie komputera i wyświetlanie zdalnie multimediów widocznych dla wszystkich uczestników wideokonferencji.

Wideokonferencje z prokuraturą

Służba Więzienna wyposażona jest w zestawy wideokonferencyjne służące do czynności procesowej – przesłuchania na odległość. Osadzony nie musi opuszczać zakładu karnego lub aresztu śledczego, co eliminuje koszty i działania związane z jego konwojowaniem. Osadzony doprowadzony jest do przygotowanego pomieszczenia na terenie jednostki penitencjarnej i dozorowany przez funkcjonariusza, po odbytej czynności procesowej odprowadzany do celi mieszkalnej.

Wideokonferencje dla osadzonych

Uzupełnią do tej pory stosowane aparaty samoinkasujące służące do kontaktu ze światem z wolności. Służba Więzienna wzorem krajów europejskich testu-

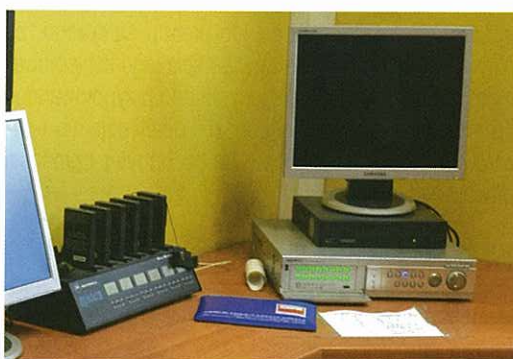


je i przygotowuje się do wdrożenia wideokonferencji dla osadzonych. Może być wykorzystywana jako uzupełnienie dodatku do rozmowy telefonicznej lub jako forma odbycia widzenia z osobami bliskimi przez osadzonego.

Łączność bezprzewodowa wprowadzona jednocześnie w całej Służbie Więziennej w 2000 r. System łączności bezprzewodowej jednostki realizowany jest w technologii analogowej FM z wywołaniem selektywnym CCIR oraz funkcją CTCSS w zakresie VHF, składa się przede wszystkim z:

- radiotelefonu stacji bazowej Radmor,
- radiotelefonów przewodowych Radmor,
- radiotelefonów ręcznych Motorola serii GP,
- cyfrowego rejestratora rozmów,
- anten, masztów, zasilaczy z akumulatorem, zabezpieczeń przepięciowych itp.

Radiotelefony pracują w wydzielonym paśmie częstotliwości, na kilku kanałach: roboczym, alarmowym, zamkniętym i przeznaczonych do połączeń w Krajowej Sieci Współdziałania i Alarmowania (z policją na całym obszarze kraju). Kanały: roboczy i alarmowy są nagrywane. Zasady komunikacji przez radiotelefony regulują wytyczne [13]. Przestrzeganie zasad łączności bezprzewodowej jest szczególnie istotne, ponieważ system pracuje w sympleksie (jeden do jednego, jeden do wielu), gdzie w danym momencie może nadawać tylko jeden nadawca. Dodatkową funkcjonalnością radiotelefonów jest funkcja przycisku napadowego oraz funkcja „czuwak”, czyli po określonym czasie nie używania radiotelefonu włączy się sygnał, który użytkownik zobligowany jest potwierdzić. Jeżeli tego nie zrobi, na stacji bazowej wyświetli się komunikat ALARM i nr radiotelefonu, generując odpowiednią reakcję dowódcy. Służba wykorzystuje łączność przez



radiotelefony na terenie jednostek oraz w czasie realizacji konwojowania (poza terenem jednostki).

Łączność GSM – Służba Więzienna korzysta również z telefonii komórkowej do celów służbowych, telefony posiada kadra kierownicza, dowódcy, kierownicy. Służą przede wszystkim do szybkiego powiadamiania, głosowo jak i SMS.

Aby systemy zabezpieczeń elektronicznych oraz łączności działały prawidłowo w jednostkach zainstalowane są agregaty prądowórcze. Systemy uzupełnione są zasilaczami buforowymi oraz UPS, na czas przełączenia z zasilania podstawowego na agregat. Idealnym rozwiązaniem jest gdy agregat startuje automatycznie, skraca to znacząco czas pracy urządzeń z zasilaczy buforowych i UPS wyposażonych w akumulatory i nie absorbuje funkcjonariuszy do działań związanych z przywróceniem zasilania.

Poza opisanymi powyżej systemami i urządzeniami w zakładach karnych występują też instalacje radiowęzłowe, rtv, multimedialne dla osadzonych.

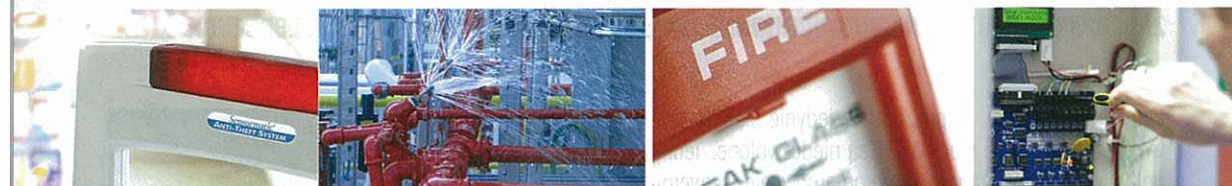
Radiowęzeł doprowadzony do cel mieszkalnych oraz świetlic służy osadzonym. Przygotowują oni audycje, różne informacje związane z życiem więziennym, słuchają radia. Funkcjonariusze posiadają nasłuch radiowęzła, system musi posiadać możliwość zdalnego wyłączenia np. w przypadku próby przekazywania przez osadzonych zabronionych treści. Często radiowęzeł instalowany jest jako zintegrowany z wandaloodpornym interkomem.

System RTV to instalacja radio-telewizyjna rozproszona do cel mieszkalnych (warunkiem jest posiadanie przez osadzonego telewizora lub radia), Służba Więzienna wyposażała w te urządzenia świetlice, biblioteki, wybrane pomieszczenia. Służy on osadzonym do dostępu do telewizji i radia).

Studia telewizyjne i multimedialne, w niektórych jednostkach stworzono takie studia służące osadzonym w celach kulturalno-oświatowych i resocjalizacyjnych. Osadzeni mogą tam tworzyć, nagrywać różne materiały audio-wideo.

Systemy elektroniczne, to nie tylko zabezpieczenia techniczno-ochronne czy środki alarmowania i łączności ale również intensywnie wdrażana informatyzacja Służby Więziennej, należy wspomnieć i o niej.

Systemy informatyczne bazują na sieci strukturalnej w technologii VPN MPLS z łączami światłowodowymi (10MB/s jednostka podstawowa, 50 MB/s okręgowe inspektoraty, 2 x 500 MB/s Centralny Zarząd Służby Więziennej – serwerownia) oraz bekapowymi łączami sateli-



Instalacje Gaśnicze Wodne

- Instalacje mgły wodnej
- Instalacje tryskaczowe i zraszaczowe
- Systemy pianowe
- Systemy gaszenia iskier
- Instalacje hydrantowe

Instalacje Gaśnicze Gazowe

- Mieszaniny gazów obojętnych
- Gazy chemiczne
- CO₂

Instalacje Elektryczne:

- Zewnętrzne i wewnętrzne
- Średniego napięcia
- Rozdział energii
- Oświetlenie

Instalacje Teleinformatyczne (LAN i IT)

Instalacje Teletechniczne:

- Elektroniczne Systemy Przeciwwkradzieżowe (EAS)
- Systemy Kontroli Dostępu (ACC)
- Systemy Sygnalizacji Pożaru (SSP)
- Dźwiękowe Systemy Ostrzegawcze (DSO)
- Systemy Nadzoru Wizyjnego (CCTV)
- Systemy Sygnalizacji Włamania i Napadu (SSWIN)

Instalacje Automatyki Budynkowej i BMS

- Sterowanie wentylacją i klimatyzacją
- Monitoring zużycia mediów (woda, prąd, ciepło)
- Integracja systemów
- Oszczędność zużycia energii

Instalacje dedykowane dla sektora handlu detalicznego

AGIS Fire & Security jest międzynarodowym dostawcą i integratorem rozwiązań w zakresie elektronicznych systemów zabezpieczeń, instalacji elektrycznych, systemów detekcji i gaszenia pożaru, a także **wyłącznym dostawcą** wysokiej klasy rozwiązań przeciwwkradzieżowych marki **Sensormatic**. Kompleksowe usługi AGIS Fire & Security obejmują projektowanie, instalowanie, uruchomienie oraz konserwację i serwis dostarczanych rozwiązań. Klienci AGIS Fire & Security reprezentują sektory rynku takie jak np. przemysł, handel detaliczny, budownictwo, logistyka, telekomunikacja itp. AGIS Fire & Security posiada certyfikaty potwierdzające, że firma spełnia wymagania normy **ISO 9001:2008** i publikacji standaryzacyjnej **AQAP 2110:2009** oraz certyfikat na zgodność z polską normą **PN-N 18001:2004** oraz z normą międzynarodową **BS OHSAS 18001:2007** (British Standard for occupational health and safety management systems). Wymienione certyfikaty umożliwiają AGIS Fire & Security realizację projektów dla klientów z sektora działalności przemysłowej o kategorii wysokiego ryzyka. Więcej informacji: www.agisfs.pl.

AGIS Fire & Security Sp. z o.o. ul. Palisadowa 20/22, 01-940 Warszawa,
tel.: (0-22) 430 83 01, faks: (0-22) 430 83 02,
Infolinia ogólna: 801 801 238, e-mail: agisfs.pl@agisfs.com
Infolinia serwisowa: 800 800 238, e-mail: serwis@agisfs.com
www.agisfs.pl

AGIS
Fire & Security

tarnymi (8/2 MB/s). Dopuszcza się jedynie sieci kablowe, bezprzewodowe sieci Wi-Fi są niedozwolone. Technologia Microsoft zapewnia oprogramowanie serwerowe takie jak Windows Serwer, Hyper-V, MS Exchange, SharePoint, MS SQL oraz klienckie. Usługami sieciowymi zarządza się poprzez Active Directory, jej politykę bezpieczeństwa. Wdrożono nowe komputery, których jest obecnie kilkanaście tysięcy, serwery w liczbie kilkuset. Wprowadzone są wielopoziomowe zabezpieczenia sieci, sprzętowe jak i programowe, obejmujące swym zasięgiem jednostki w całej Polsce. Trwa opracowywanie i wdrażanie Zintegrowanego Systemu Zarządzania w oparciu o system Microsoft Dynamics AX, oprogramowania finansowanego z Norweskiego Mechanizmu Finansowego. Oprogramowanie to będzie obejmowało między innymi moduły: kadry–płace, szkolenia, BHP, czas pracy, magazyny i inne, w systemie klasy ERP.

Poza wspomnianym oprogramowaniem Służba Więzienna użytkuje oprogramowanie Jednostka, portale Zamówienia Publiczne, BIP, Elektroniczna Skrzynka Podawcza i E-Sekretariat, System Informacji Prawnej, Poczta elektroniczna, Intranet, strony www – zarówno internetowe jak i intranetowe. Wdrożono kursy zawodowe i specjalistyczne prowadzone poprzez e-learningu oraz b-learningu, z rozbudowanymi bazami materiałów szkoleniowych w postaci multimedialnej.

Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET jest to system ewidencji, zbudowany na klastrze wielonodowym serwerów z macierzami. Dostęp do systemu dozwolony jest tylko z wewnętrznej sieci, użytkownik wyposażony jest w kartę z certyfikatem elektronicznym, wydawanym przez Punkt Certyfikacji Centralnego Zarządu Służby Więziennej. Do wydzielonego zasobu bazy danych mają też dostęp inne służby, sądy. Baza Noe.NET została zakwalifikowana jako szczególnie ważna dla bezpieczeństwa państwa. Baza ta jest stale rozbudowywana o nowe moduły i funkcjonalności. Modernizowana, zarówno sprzętowo jak i programistycznie.

W Służbie Więziennej wdrażany jest system bezpieczeństwa informacji z certyfikacją na zgodność z ISO 2700-1.

Opisując systemy elektroniczne Służby Więziennej nie sposób nie wspomnieć o dozorcze elektronicznym.

System dozoru elektronicznego (SDE) – wzorem krajów zachodnich gdzie systemy odbywania kary poza więzieniem okazały się skutecznym środkiem na przepelnione więzienia, Polska sukcesywnie wdraża dozór elek-



troniczny. System bazuje na zakładanym na nogę lub ręką nadajniku w bransoletce oraz module do kontaktu z centralą nadzorującą instalowanym w miejscu zamieszkania. Moduł ten komunikuje się z centralą monitorowania w sieci GSM. W centrali zaprogramowany jest harmonogram, kiedy dozorowany ma przebywać w domu, a kiedy poza nim. Ustalono zasady kontaktu, alarmowania i reagowania kiedy harmonogram zostaje naruszany.

Obiekty Służby Więziennej to najczęściej obiekty budowlane i tereny wokół nich. Ze względu na zagrożenia wyładowaniami atmosferycznymi i przepięciami, instalując wszelkiego rodzaju systemy elektroniczne należy pamiętać o połączeniu wyrównawczym metalowych obudów, elementów konstrukcji, koryt itp., nie zapominając o zabezpieczeniach przepięciowych w torach zasilania oraz torach sygnałowych. Wymagane jest stopniowanie zabezpieczeń przepięciowych do wartości odporności jaką posiadają instalowane urządzenia.

Podsumowanie

Przedstawione powyżej informacje zaledwie szcążkowo poruszają tematykę jaką są zabezpieczenia techniczno-ochronne, środki alarmowania i łączności a także systemy informatyczne i inne występujące w zakładach karnych. Z treści przedstawionego materiału jednoznacznie wynika, jak wielki wpływ na zabezpieczenie techniczno-ochronne jednostek penitencjarnych Służby Więziennej, ma intensywny rozwój technologii elektronicznych.

O Autorze



Por. mgr inż. Cezary MECWALDOWSKI – starszy inspektor Zakładu Szkolenia Ochronnego Centralnego Ośrodka Szkolenia Służby Więziennej w Kaliszu.

Autor zajmuje się szkoleniami z zakresu bezpieczeństwa, techniki więziennej, zagadnień związanych z ochroną informacji niejawnych oraz danych osobowych. Specjalizuje się w tematyce zabezpieczeń techniczno-ochronnych, szczególnie systemów alarmowych. Prowadzi zajęcia zawodowe, jak i specjalistyczne, stacjonarne oraz zdalne poprzez e-learning, b-learning czy wideokonferencję.

Absolwent Uniwersytetu Ekonomicznego w Poznaniu, Uniwersytetu Adama Mickiewicza w Poznaniu oraz Politechniki Łódzkiej.

Literatura

- [1] Ustawa o Służbie Więziennej z 9 kwietnia 2010 r.
- [2] Ustawa Kodeks karny wykonawczy z 6 czerwca 1997 r.
- [3] Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r.
- [4] Rozporządzenie Rady Ministrów w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony z 24 czerwca 2003 r.
- [5] Rozporządzenie Ministra Sprawiedliwości w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej z 31 października 2003 r.
- [6] Rozporządzenie Ministra Sprawiedliwości w sprawie rodzaju urządzeń i środków technicznych służących do przekazywania, odtwarzania i utrwalania obrazu lub dźwięku z monitoringu w zakładach karnych z 16 października 2009 r.
- [7] Zarządzenie Dyrektora Generalnego Służby Więziennej nr 43/2010 w sprawie ustalania metod i form działalności w zakresie ochrony jednostek organizacyjnych Służby Więziennej z 13 sierpnia 2010 r.
- [8] Wytyczne Dyrektora Generalnego Służby Więziennej nr 2/2013 w sprawie wymagań dla zabezpieczeń techniczno-ochronnych w jednostkach organizacyjnych Służby Więziennej z 4 czerwca 2013 r.
- [9] Wytyczne Dyrektora Generalnego Służby Więziennej nr 4/2013 w sprawie określenia standardów systemów zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej z 10 czerwca 2013 r.
- [10] Wytyczne Dyrektora Generalnego Służby Więziennej nr 3/2011 w sprawie wymagań technicznych i ochronnych dla pawilonów zakwaterowania osadzonych z października 2011 r.
- [11] Rozporządzenie Ministra Sprawiedliwości w sprawie celi zabezpieczającej i izby izolacyjnej z 4 czerwca 2013 r.
- [12] Statystyka za rok 2013 Biura Informacji i Statystyki Centralnego Zarządu Służby Więziennej
- [14] Wytyczne Dyrektora Generalnego Służby Więziennej w sprawie postępowania się łącznością bezprzewodową w Służbie Więziennej z 14 grudnia 2000 r.
- [15] Rozporządzenie Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych z 23 stycznia 2014 r.
- [16] Rozporządzenie Rady Ministrów w sprawie szczegółowego trybu działań funkcjonariuszy Służby Więziennej podczas wykonywania czynności służbowych z 4 sierpnia 2010 r.
- [17] Rozporządzenie Ministra Sprawiedliwości w sprawie szczegółowych warunków technicznych urządzeń wchodzących w skład środków technicznych w systemie dozoru elektronicznego, a także sposobu organizowania tych urządzeń w systemie oraz sposobu przekazywania danych wewnątrz tego systemu z 27 lutego 2009 r.
- [18] Wytyczne Dyrektora Generalnego Służby Więziennej nr 1/2013 w sprawie wymagań, jakim powinno odpowiadać oświetlenie miejsc pracy na zewnątrz oraz metod poprawy efektywności energetycznej instalacji oświetlenia zewnętrznego w jednostkach organizacyjnych Służby Więziennej z 18 marca 2013 r.
- [19] Zarządzenie Dyrektora Generalnego Służby Więziennej nr 56/2012 w sprawie szczegółowych zasad eksploatacji i rozwoju systemów łączności i zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej z 22 sierpnia 2012 r.
- [20] Zarządzenie Dyrektora Generalnego Służby Więziennej nr 57/2012 w sprawie szczegółowych zasad eksploatacji i rozwoju systemów informatycznych w jednostkach organizacyjnych Służby Więziennej z 22 sierpnia 2012 r.

Technika zabezpieczeń dla jednostek penitencjarnych



Modernizacja obiektów służby więziennej oraz zakładów karnych i aresztów w Polsce trwa od kilku lat. Potrzeby w zakresie wymiany starych i instalacji najnowszych rozwiązań z zakresu zabezpieczenia technicznego pomieszczeń i terenów przyległych nadal są olbrzymie. Argumenty o braku środków na ten cel tracą na mocy, jeśli zestawia się je z kosztami generowanymi codziennie w sytuacji kiedy tego typu rozwiązań jeszcze nie ma.

Chcąc zaprezentować dostępną na rynku ofertę polskich firm rozmawiamy z Dyrektorem Sprzedaży firmy Unicard – Adamem Daniłowiczem.

OMil: Jakie rozwiązania obecnie znajdują się w Państwa ofercie?

Adam Daniłowicz: W ofercie mamy szeroką gamę systemów produkowanych przez naszą firmę. Wszystkie one posiadają cechę wspólną, którą jest autoidentyfikacja. Najważniejszymi rozwiązaniami dla zakładów karnych i aresztów są zintegrowane systemy bezpieczeństwa w tym: system kontroli dostępu do pomieszczeń i wjazdów, system rejestracji czasu pracy, depozytory kluczy i broni, systemy parkingowe.



Unicard nie tylko dostarcza te systemy, ale ma również możliwość ich wdrożenia. Jesteśmy w stanie zaprojektować system z uwzględnieniem indywidualnych potrzeb, zainstalować go, uruchomić, przeszkolić administratorów i serwisować w ramach gwarancji i pogwarancyjnie. Nasza firma powyższe rozwiązania rozwija i dostarcza od ponad 20 lat.

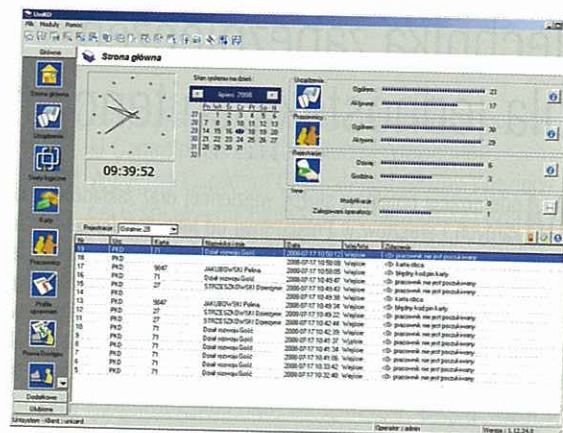
OMil: Czym wyróżnia się dostarczany przez Unicard system kontroli dostępu?

A.D.: Nasze rozwiązanie jest kompleksowe. Produkujemy wszystkie najważniejsze elementy systemu czyli czytniki, kontrolery i oprogramowanie co przekłada się na stabilność pracy. Nasze systemy są skalowalne i łatwe w rozbudowie. Dostarczamy małe rozwiązania zapewniające kontrolę na kilku przejściach, jak również rozwiązania bardzo duże, rozproszone w kilkudziesięciu lokalizacjach, obejmujące setki przejść i tysiące kart. W związku z tym, że jesteśmy producentem możemy dostosować rozwiązanie do indywidualnych potrzeb klienta. System kontroli dostępu jest zintegrowany z innymi dostarczonymi przez nas systemami. Możemy także zintegrować się z systemami posiadanym przez klienta. System kontroli dostępu jest nieustannie rozwijany przez firmę Unicard.

OMil: Jakie korzyści zapewnia wdrożenie systemu bezpieczeństwa państwa firmy?

A.D.: Zapewniamy stabilnie działające i zaawansowane technologiczne rozwiązanie. Możemy świadczyć wsparcie na każdym etapie wdrożenia, a później działania systemu. Nasza firma świadczy bezpośrednio serwis gwarancyjny i pogwarancyjny na terenie całej Polski. Rozbudowujemy i modernizujemy nasze systemy. Zapewniamy, że dostarczone dzisiaj systemy będą wspierane przez naszą firmę przez długie lata. Aktualnie wspieramy co najmniej kilkadziesiąt systemów kontroli dostępu, które były zainstalowane kilkanaście lat temu. Systemy te są rozbudowywane o urządzenia nowej generacji, a wszystko nadzorowane jest przez najnowsze oprogramowanie UniKD.

OMil: Czy dla Służby Więziennej macie Państwo wyspecjalizowaną ofertę? Wiadomo, że jednostki penitencjarne charakteryzują się znacznie wyższym poziomem zabezpieczeń. Czy w związku z tym rozwiązania dostępne na rynku cywilnym są w jakiś sposób dostosowywane do potrzeb Służby Więziennej?



A.D.: W naszej ofercie dla Służby Więziennej kładziemy szczególny nacisk na trzy kwestie. Po pierwsze w takich jednostkach przykładamy najwyższą staranność jeśli chodzi o instalację systemu. Dobrze wykonane instalacje przekładają się na późniejszą stabilną pracę systemu. Po drugie mamy możliwość dostosowania systemu do niestandardowych potrzeb klienta, a także zintegrować go z innymi działającymi systemami w danym obiekcie.



Po trzecie dla takich jednostek jesteśmy w stanie dostarczyć rozwiązanie kontroli dostępu wykorzystujące technologie identyfikacji Mifare Plus (standard ten jest wprowadzony w legitymacjach służbowych SW). Od kilku miesięcy mamy w swojej ofercie kompleksowe rozwiązanie, w skład którego wchodzi karta Mifare Plus, czytniki ASR-804M i koder kart wraz z oprogramowaniem (wszystkie elementy poza kartami są naszymi produktami). Rozwiązanie to zapewnia najwyższy poziom zabezpieczenia kart i transmisji między kartą a czytnikiem. Oprócz tego dzięki dostarczaniu koderowi administrator systemu ma pełną kontrolę nad kartami (kluczami zapisanymi na nich) i ich numeracją. Na dzień dzisiejszy prowadzimy rozmowy o zastosowaniu tego rozwiązania w jednostkach penitencjarnych.

Omii: Spośród licznych Państwa realizacji można wskazać również te bardzo wymagające. Państwa urządzenia instalowane były w szpitalach, zakładach przemysłowych i na obiektach sportowych – czyli dostarczacie rozwiązania do obiektów wymagających najwyższego poziomu bezpieczeństwa.

A.D.: Unicard ma wieloletnie doświadczenie w dostarczaniu systemów bezpieczeństwa do obiektów o szczególnym znaczeniu. Nasze systemy funkcjonują między innymi w Ministerstwie Spraw Wewnętrznych i Ministerstwie Skarbu Państwa. Dostarczyliśmy duże systemy do sądów m.in. w Poznaniu i Stalowej Woli. Nasze systemy działają także w obiektach policji, np. KMP w Płocku, KWP w Poznaniu, Katowicach i Krakowie. Jeśli chodzi o obiekty o znaczeniu strategicznym wdrożyliśmy bardzo duży system bezpieczeństwa w kilkunastu oddziałach Operatora Logistycznego Paliw Płynnych. Ponadto od kilkunastu lat Unicard dostarcza zaawansowane czytniki kart Mifare dla jednostek wojskowych w całym kraju.

Dziękujemy za rozmowę.

Fot. Unicard S.A.

Drzwi do cel firmy DONIMET



Pomimo rozwoju zabezpieczeń i systemów informatycznych oraz teletechnicznych przeznaczonych dla jednostek penitencjarnych i coraz szerzej w nich stosowanych,

nieodzownym atrybutem i cechą więzienia pozostają drzwi do cel, które są jednocześnie częścią składową wyżej wymienionych systemów, ale pełnią też rolę niezależnego zabezpieczenia. To właśnie za zamkniętymi drzwiami celi, więzień odbywa karę, a solidność drzwi daje mu świadomość braku możliwości wyjścia. Firma DONIMET w oparciu o wieloletnie doświadczenie, konsultacje ze służbami więziennymi oraz szereg przeprowadzonych badań, oferuje i produkuje drzwi, których jakość i zgodność ze wszystkimi wymogami stawianymi drzwiami do cel, potwierdził Instytut Mechaniki Precyzyjnej, wydając Certyfikat Zgodności na drzwi DONIMET do cel więziennych i aresztów typu DC3.1/ZK.

Podstawowym kryterium warunkującym możliwość stosowania drzwi w celach więziennych, jest ich odporność na włamanie. Od drzwi więziennych wymagana jest odporność na włamanie klasy RC4 wg PN-EN 1627 i klasy C wg PN-B-92270 oraz spełnienie Kryteriów Technicznych KT/101/IMP:2008, stawianych drzwiom do cel więziennych i aresztów.

Drzwi do cel charakteryzują się wieloma cechami istotnymi dla bezpieczeństwa osadzonych, takimi jak:

- brak jakiegokolwiek możliwości manipulacji w celu otwarcia drzwi (skrzydło i ościeżnica całkowicie gładkie od strony celi),



Drzwi do cel (widok z korytarza / od strony celi)

- wizjer szerokokątny zabezpieczony szkłem antywłamaniowym P6 oraz zamykany metalową kłapką, umożliwiającą podgląd całego pomieszczenia,
- możliwość szybkiego zamknięcia celi poprzez zaryglowanie wewnętrznych zasuw (możliwość zaryglowania dolnej zasuwki nogą),
- brak możliwości zatrzaśnięcia pracownika SW w celi (zamek główny nie jest wyposażony w rygiel klamkowy – zapadkę),
- możliwość szybkiego demontażu zamka od strony korytarza przy zamkniętych drzwiach (w przypadku awarii zamka lub sabotażu),
- wyposażenie drzwi w masywny tańczuch zapewniający brak możliwości zerwania nawet przy użyciu bardzo dużych sił, ograniczający otwarcie skrzydła do kilkunastu centymetrów,
- możliwość pewnego i silnego uchwytu drzwi podczas otwierania przez strażnika, poprzez zastosowanie stalowego, solidnego pochwyty od strony korytarza.

Wszystkie drzwi do cel produkowane w firmie DONIMET malowane są proszkowo w kolorystyce RAL, dostosowanej do kolorystyki każdego zakładu karnego. Poliesterowe powłoki malarskie umożliwiają łatwe i szybkie usunięcie z powierzchni wszelkich zabrudzeń. Drzwi do cel mogą być dodatkowo wyposażone w podajnik więzienny (otwierane drzwiczki), dający możliwość bezpiecznego skucia więźnia, i stanowiący po otwarciu wygodną półkę (np. w celu podania posiłku).



Drzwi do cel – z podajnikiem (widok od strony korytarza)

Drzwi DONIMET do cel mogą być produkowane z zamkiem głównym mechanicznym na klucz (możliwość tworzenia systemu klucza Master key), elektrycznym – wpiętym w system teletechniczny obiektu, jak również z zamkiem głównym na kartę magnetyczną, bez konieczności zasilania (możliwość utworzenia systemu Master key). Dodatkowo drzwi mogą być wyposażone w szereg czujników: kontaktrony

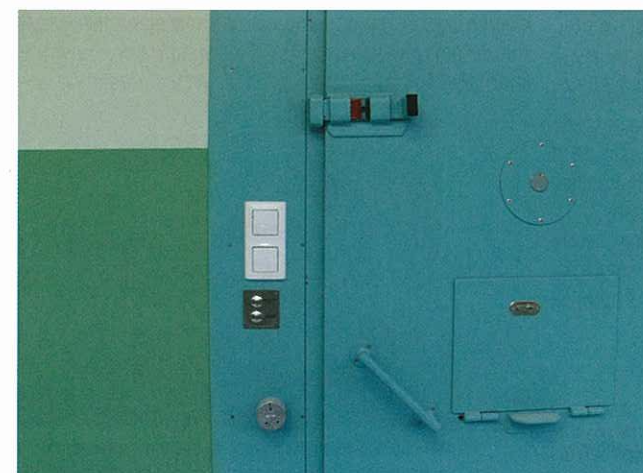


(czujnik otwarcia drzwi), czujnik otwarcia zamka głównego, czujnik sejsmiczny, wizualny sygnalizator otwarcia drzwi itp.

Oprócz cech związanych bezpośrednio z bezpieczeństwem osadzonych, drzwi DONIMET spełniają wiele wymogów zgodnych z przepisami budowlanymi i wymaganymi prawem budowlanym. Podstawowym jest wymóg o dopuszczeniu wyrobu budowlanego do stosowania w budownictwie. Aby wyrob budowlany (drzwi) został dopuszczony do stosowania w budownictwie, musi przejść szereg badań na zgodność z normą lub aprobatą techniczną oraz uzyskać stosowny certyfikat i być odpowiednio oznakowany tabliczką znamionową ze znakiem B lub CE. Ponadto, na drzwi musi być wystawiona Krajowa Deklaracja Zgodności, zawierająca wszystkie zbadane i deklarowane cechy drzwi. Drzwi Donimet spełniają wszystkie obowiązujące w tym zakresie normy. Zostały zbadane przez laboratoria Instytutu Mechaniki Precyzyjnej na odporność na włamanie, jak również przez Instytut Techniki Budowlanej, potwierdzając swoją wysoką odporność na wielokrotne zamykanie i otwieranie – klasa 6, izolacyjność akustyczną $R_w = 40$ dB, wytrzymałość mechaniczną – klasa 4, odporność na korozję – klasa C3, oraz wysoki standard wielu innych cech użytkowych.

Z uwagi na uzyskane wyniki, drzwi DONIMET do cel mogą być stosowane w bardzo ciężkich warunkach pracy. Mogą być również wykonane jako drzwi przeciwpożarowe

(czujnik otwarcia drzwi), czujnik otwarcia zamka głównego, czujnik sejsmiczny, wizualny sygnalizator otwarcia drzwi itp.



dymoszczelne EI30S i EI60S, zgodnie z Aprobata Techniczną ITB AT-15-8513/2013.

Oprócz wyrobów sprawdzonych, przebadanych i posiadających odpowiednie dopuszczenia, rynek wciąż oferuje szereg wyrobów nazywanych drzwiami do cel więziennych, a w rzeczywistości niezbadanych, niecertyfikowanych i nieoznakowanych zgodnie z obowiązującymi przepisami więziennictwa i prawem budowlanym. Stosowanie takich drzwi, oprócz tego, że stanowi naruszenie prawa, naraża zakłady penitencjarne na dodatkowe koszty związane z koniecznością wymiany takich drzwi, zakwestionowanych przez Nadzór Budowlany lub inne organy kontrolne. Na etapie wyboru drzwi w nieznacznie niższych cenach, tylko pozornie wydają się one atrakcyjniejsze. Dopiero dalsze procesy związane z drzwiami (terminowość dostaw, montaż, dokumentacja odbiorowa, odbiory, gwarancja, serwis gwarancyjny i pogwarancyjny, jakość), pokazują przewagę drzwi DONIMET i faktyczne korzyści osiągnięte poprzez ich zastosowanie. Drzwi więzienne do cel produkowane przez firmę DONIMET, od wielu lat „pilnują” więźniów w celach więziennych zakładów karnych m.in. w Opolu Lubelskim, Barczewie, Strzelinie, Bielsku Białej, Sieradzu, Przemyślu, Rzeszowie, Gliwicach, Przywarach, Wejherowie, Pionkach, w Warszawie i w wielu innych więzieniach, aresztach śledczych oraz komendach policji.

Artykuł firmy Donimet Sp. z o.o.
Fot. Donimet Sp. z o.o.

Systemy skrytkowe dla jednostek penitencjarnych



Elektroniczne systemy depozytowe od wielu lat wspomagają pracę służb ochrony w jednostkach penitencjarnych, ułatwiając i porządkując zarządzanie kluczami i depozytami w obiekcie. Są to systemy znane i cenione przez użytkowników, ale... również traktowane jako niezwykle skomplikowane w instalacji oraz bardzo kosztowne. Z drugiej strony, co za chwilę przedstawimy w poniższym artykule, producenci nie ograniczają się tylko do drogiej i trudnej w administrowaniu urządzeń. Oferują również bardzo atrakcyjne cenowo produkty, spełniające wszystkie niezbędne funkcje wspólnego systemu depozytowego.

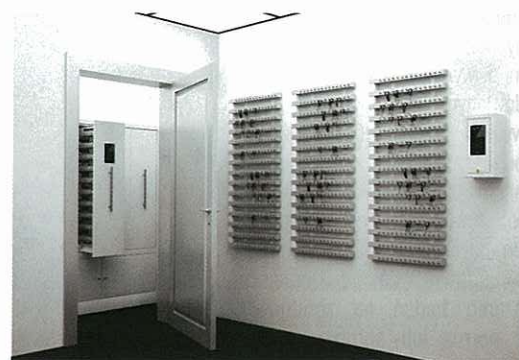
Firma Creone została założona w 1979 roku i od początku swojej działalności cały proces produkcji, konstrukcji oraz projektowania jest realizowany w Szwecji. Działalność firmy, lista i różnorodność oferowanych produktów stale się powiększa.

Inteligentne depozytory
by
CREONE

Dzięki własnemu działowi projektowemu, producent zgodnie z potrzebami rynku wprowadza nowe rozwiązania. Aktualnie systemy szaf do przechowywania kluczy i depozytów są dostarczane do 30 krajów świata. Gamę produktów firmy Creone najlepiej opisuje kilka cech: Pełna Kontrola, Prosta Obsługa, Elastyczność i Uniwersalność.

W ofercie firmy Creone znaleźć możemy cztery rodzaje produktów: KeyRack, KeyBox, ValueBox, KeyWin.

System KeyRack (fot. 1), może się składać z 66 listew połączonych ze sobą przy pomocy wspólnej magistrali komunikacyjnej i nadzorowane przy pomocy wspólnego modułu operatorskiego. Pojedynczy panel operatorski może obsługiwać do 924 gniazd kluczowych. Dzięki takiemu rozwiązaniu Klient w prosty sposób może ustalić czy klucz



Fot. 1. System KeyRack – dopasowany do potrzeb biur przepustek

znajduje się w depozycie lub czy został pobrany. Wybierając ten system unikniemy również problemu z brakiem miejsca na dużą metalową szafę, w które to standardowo wyposażone są elektroniczne systemy depozytowe. Takie rozwiązanie pozwala również na ograniczenie kosztów związanych z budową systemu, dlatego rozwiązania KeyRack cieszy się dużym zainteresowaniem wśród Klientów szukających atrakcyjnych cenowo systemów do zarządzania dużą ilością kluczy.

KeyBox jest rozwiązaniem dedykowanym do przechowywania i zarządzania kluczami i małymi przedmiotami. Jest to seria metalowych szaf wyposażonych w haczyki na klucze lub niewielkie skrytki (fot. 2a i 2b).

Po prawidłowej weryfikacji użytkownika zostają otwarte drzwiczki depozytu i odblokowują się gniazda kluczy do których użytkownik ma dostęp. W celu ułatwienia lokalizacji klucza, gniazda wyposażone są w sygnalizatory optyczne informujące użytkownika o przypisanych kluczach. W pa-



Fot. 2a. System KeyBox seria KeyControl – z nadzorem przechowywanych depozytów



Fot. 2b. System KeyBox seria System – rozwiązanie bardzo atrakcyjne cenowo



Fot. 3a. System ValueBox – dostępne różne wymiary skrytek



Fot. 3b. System Valuebox – w wykonaniu umożliwiającym montaż podtynkowy



Fot. 3c. System Valuebox umożliwia deponowanie prywatnych i służbowych przedmiotów

kiecie tym możemy znaleźć również rozwiązania umożliwiające bezpieczne przechowanie od 14 zestawów kluczy w modelu 9400SC do 924 w modelu 9700SC. Jest to rozwiązanie adresowane do Klientów którzy oprócz uporządkowania i nadzoru nad dostępem do poszczególnych kluczy, wymagają również prostej obsługi i elastycznej rozbudowy.

ValueBox (fot. 3a, 3b i 3c) to seria rozwiązań skrytkowych umożliwiającą przechowywanie przedmiotów takich jak: telefony komórkowe, nośniki danych, prywatne przedmioty pracowników, dokumenty, laptopy, wartości pieniężne, lekarstwa, broń i wiele innych. W grupie tych produktów możemy znaleźć rozwiązania ze skrytkami o wymiarach wewnętrznych od 260x125x255 mm [sxwxg] w modelu 7006S, do 260 x 400 x 255 mm [sxwxg] w modelu 7002S.

Dzięki dużej różnorodności wielkości skrytek i możliwości ich dowolnego łączenia między sobą, każdy użytkownik może zbudować system spersonalizowany zgodnie z jego potrzebami. System Valuebox w ramach pojedynczego modułu operatorskiego może zostać rozbudowany do 15 modułów rozszerzających, z obsługą do 96 skrytek.

KeyWin jest to oprogramowanie zarządzające dla wszystkich powyższych rozwiązań. Wszystkie urządzenia komunikują się z wykorzystaniem protokołu TCP/IP. W ramach jednej wspólnej bazy danych można zbudować system obsługujący do kilku tysięcy gniazd kluczowych lub skrytek depozytowych. Aplikacja umożliwia nadzorowanie do 100 modułów operatorskich w rozproszonych lokalizacjach. W celu łatwiejszego dostępu do systemu, producent wprowadził do oferty rozwiązanie webowe, które pozwala zarządzać systemem przy pomocy smartfonów, tabletów czy laptopów bez konieczności instalacji oprogramowania klienckiego.

Generalnym dystrybutorem na terenie Polski produktów firmy Creone jest firma Volta. W przypadku dodatkowych pytań zapraszamy do odwiedzenia strony www.volta.com.pl lub kontaktu z autorem artykułu.

Artykuł firmy Volta Sp. z o.o.
Fot. Volta Sp. z o.o.

Grzegorz MICHAŁSKI, Specjalista ds. Systemów Depozytowych
creone@volta.com.pl

CASTEL – interkomowe systemy bezpieczeństwa dla więziennictwa

urmet
miwi

Zwiększenie bezpieczeństwa w zakładach karnych i aresztach śledczych to jeden z wielu celów, jakie mają postawione przed sobą jednostki więzienne. Cel ten ma zostać zrealizowany m.in. poprzez ograniczenie możliwości dostępu do obiektów penitencjarnych osób trzecich, a także zintensyfikowanie kontroli zachowania osób podczas pobytu w tego typu jednostce.

W ramach systemów bezpieczeństwa pomocne jest rozwiązanie proponowane przez firmę CASTEL – jednego z producentów systemów oferowanych przez firmę Miwi-Urmet należącą do grupy Urmet od 2010 roku.

CASTEL oferuje jednostkom penitencjarnym interkomowe systemy bezpieczeństwa do cel, korytarzy, wind, czy parkingów. Systemy te umożliwiają komunikację pomiędzy stacjami różnych oddziałów, a centralnym punktem kontroli. System interkomowy do cel wyposażony jest w wandaloodporne stacje, kontrolę oświetlenia, świetlne oznakowanie połączeń oraz identyfikację numeru i funkcję wykrywania hałasu.

Dodatkowo CASTEL oferuje:

- systemy komunikacji interkomowej i dostępu (do budynków, korytarzy, służ),
- systemy interkomowe do pokoi widzeń (z funkcją posłuchu i nagrywania),
- systemy interkomowe do punktów wydawania paczek i dokumentów.

Castel to również wizualizacja systemu komunikacji, dostępu i alarmu z funkcją wideo, zarządzania dźwiękiem, wideo i dostępem (kody, karty lub biometria) poprzez IP.

Stacje przystosowane są do środowiska więziennego, tj. charakteryzują się wysoką jakością dźwięku połączoną z wytrzymałością urządzeń. Produkty Castel to rozwiązania, które można integrować z systemem centralnego zarządzania bezpieczeństwem.

XELLIP/CAP IP oraz Maylis to dwa najnowsze systemy oferowane przez firmę CASTEL i stosowane w obiektach więziennych.

Główną korzyścią XELLIP jest bezpośrednia komunikacja (IP), tzn. jedno połączenie LAN do zarządzania dźwiękiem, obrazem, danymi i zasilaniem stacji (PoE). Ważna jest również jakość obrazu i dźwięku, którą można osiągnąć dzięki dwukierunkowej komunikacji audio (Full-Duplex), pozbawionej szumów i echa oraz wysokiej jakości kolorowych kamer wideo (H.264). Co więcej, użycie protokołu SIP (RFC3261 standard) i najpowszechniejszych kodeków obrazu i dźwięku (G711, H263, H263+, H264) daje możliwość integracji z innymi systemami: telefonicznymi systemami IP, systemami nadzoru, systemami obserwacji wideo, itd. Na uwagę zasługuje również łatwa obsługa tego systemu – przyjazny dla użytkownika interfejs (aplikacja web) służąca do zdalnego programowania stacji i serwerów. System XELLIP uwzględni również potrzeby osób niepełnosprawnych. Stacje i urządzenia wyposażone są w kolorowe kamery wideo, trzy diody LED, pętle indukcyjne dla aparatów słuchowych i przyciski z alfabetem Braille.

Maylis jest kompletnym systemem interkomunikacji wykorzystującym najnowszą technologię cyfrową. System jest owocem 40-letnich doświadczeń firmy CASTEL i spełnia wymagania najbardziej różnorodnych zastosowań.

Wybrane cechy systemu:

- wszechstronne zastosowanie,
- szybka i niezawodna komunikacja,
- system komunikacji pomiędzy różnymi stacjami, który zapewni personelowi pełną ochronę,
- graficzny interfejs użytkownika,
- wizualizacja połączeń, dostępu i alarmów, z funkcją śledzenia i zapisu wydarzeń, a także bieżącego raportowania na wszystkich stacjach interkomu.

CASTEL posiada szerokie doświadczenie i wiele zrealizowanych projektów systemów interkomowych dla obiektów więziennych, co pozwala na oferowanie najwyższej jakości oraz funkcjonalności systemów komunikacji i bezpieczeństwa dla personelu, osadzonych i gości.

Artykuł firmy Miwi Urmet Sp. z o.o.

Marek KOŚMIDER, kierownik Działu SSWIN, KD i SSP w firmie Miwi Urmet Sp. z o.o.



Nedap AEOS – optymalny sposób współdziałania systemów zabezpieczeń w obiektach Służby Więziennej

nedap
technology that matters

Obecnie systemy zabezpieczeń technicznych w obiektach Służby Więziennej coraz częściej współdziałają ze sobą tworząc zaawansowane systemy zintegrowane.

Większość inwestorów planujących modernizację infrastruktury zabezpieczeń zakłada, że systemy chroniące ich budynki będą ze sobą współdziałać i wymieniać wzajemnie informacje dotyczące zdarzeń zachodzących w poszczególnych obszarach zabezpieczeń. Oczekują oni na przykład, że naruszenie uzbrojonej strefy alarmowej systemu sygnalizacji włamania i napadu spowoduje automatyczne wyświetlenie na ekranie stacji operatorskiej w centrum monitoringu obrazu z kamery znajdującej się w pobliżu naruszonej strefy. Dzięki takiemu współdziałaniu systemu sygnalizacji włamania i napadu i monitoringu wizyjnego znacznie prostsze i szybsze staje się właściwe podjęcie reakcji służb ochrony fizycznej.

W innym przypadku chcą, aby po uzbrojeniu strefy, dostęp do pomieszczeń chronionych systemem kontroli dostępu był niemożliwy nawet dla osób, które normalnie posiadają do nich prawo wstępu i odpowiednie uprawnienia przypisane do swojego identyfikatora. Takie proste rozwiązanie dramatycznie zmniejsza liczbę fałszywych alarmów, generowanych przez osoby, które zapomniały, że strefa została uzbrojona i przed wejściem do pomieszczenia należy ją rozbroić. Projektanci systemów zabezpieczeń stają więc przed koniecznością zapewnienia choćby podstawowej integracji podsystemów zabezpieczeń. Nie jest to jednak zadanie łatwe. Sposobów integracji jest bowiem co najmniej kilka, a każdy ma swoje zalety i wady. Ponadto w obiektach, które posiadają już istniejącą infrastrukturę zabezpieczeń projektanci muszą uwzględnić zastane uwarunkowania i potrzebę dopasowania się do elementów dotychczas wykorzystywanych.

Sytuacja komplikuje się jeszcze bardziej, gdy systemy dotychczas wykorzystywane pochodzą od różnych producentów, którzy niekoniecznie widzą swój interes we współpracy z systemem konkurenta. Wprawdzie można sądzić, że jeżeli jeden producent dostarczył system kontroli dostępu, a drugi sygnalizacji włamania i napadu to konkurencji tutaj nie ma, bo to systemy pełniące inne funkcje, ale w praktyce ci dwaj producenci mają w swojej ofercie zarówno kontrolę dostępu jak i systemy alarmowe, więc choć w tym obiekcie nie są konkurentami, to na rynku owszem i nie mają za-

zwyczaj woli współpracy ze sobą. Cierpi na tym rzecz jasna użytkownik, ale na krótką metę dla wielu producentów nie wydaje się to szczególnie istotne.

Warto też wspomnieć o konieczności integracji systemów zabezpieczeń z systemami ochrony pożarowej. Szczególnie istotne jest w tym przypadku zintegrowanie systemu kontroli dostępu z systemem alarmu pożarowego. Oczywiście bezpieczeństwo osób przebywających w chronionym budynku zakłada konieczność odblokowania wszystkich przejść znajdujących się na drogach ewakuacyjnych. Wymóg ten jest jednak narzucony przez przepisy prawa i dopóki nie zostanie on spełniony, budynek nie zostanie dopuszczony do użytku. Ze strony technicznej ten rodzaj integracji nie wiąże się z żadnym szczególnie skomplikowanym mechanizmem integracji i zwykle sprowadza się do zwolnienia napięcia na elementach blokujących przejścia, które w przypadku braku napięcia przechodzą w stan otwarty.

Przyjrzyjmy się zatem podstawowym wykorzystywanym obecnie możliwościom integracji zabezpieczeń.

Większość systemów zabezpieczeń składa się z trzech podstawowych poziomów – poziomu serwera, poziomu kontrolera (centrali) i poziomu elementów wykonawczych.

Poziom serwera. Większość współczesnych systemów zabezpieczeń pracuje w oparciu o serwer, na którym zainstalowane jest oprogramowanie aplikacyjne i bazodanowe. Integracja na tym poziomie zakłada wymianę danych pomiędzy serwerami dwóch lub większej liczby systemów. W tym celu niezbędne jest stworzenie interfejsu pomiędzy systemami. Zazwyczaj odbywa się to na drodze udostępniania przez producentów narzędzi specjalnie opracowanych do wymiany danych z innymi systemami. Przykładem takich narzędzi są SDK (software development kit), API (application programming interface), Web Service czy socket interface. Rzecz jasna nie każda firma dostarcza tego typu narzędzia i w przypadku tych, które tego nie robią, integracja może być bardzo utrudniona.

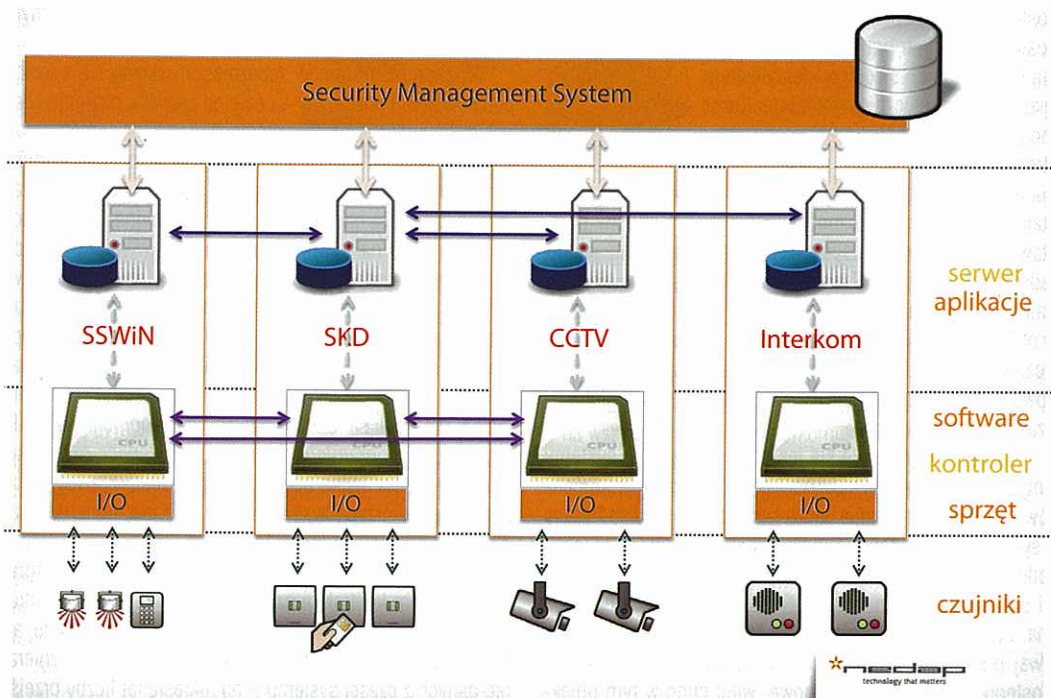
Kolejnym poziomem, na którym możliwa jest integracja to poziom kontrolera czy w innej terminologii – centrali. Większość systemów oprócz serwera posiada w swojej architekturze kontrolery odpowiadające za zarządzanie i zbieranie danych z części systemu – np. określonej liczby przejść czy stref alarmowych.

Najniższym poziomem architektury systemów zabezpieczeń są elementy peryferyjne takie jak czujki PIR, kontaktrony, czytniki kart czy kamery. W tradycyjnym ujęciu te elementy podłączone są do odpowiadających sobie kontrolerów (centralek), a potem wyżej do właściwych im serwerów. I tak odpowiednio czujki PIR podłączone są do centrali SSWiN i do serwera systemu alarmowego, a czytniki kart do kontrolera SKD i serwera SKD. Otrzymujemy wówczas architekturę z kilkoma systemami pracującymi równolegle w stosunku do siebie. Graficznie taki układ przedstawia rys. nr 1.

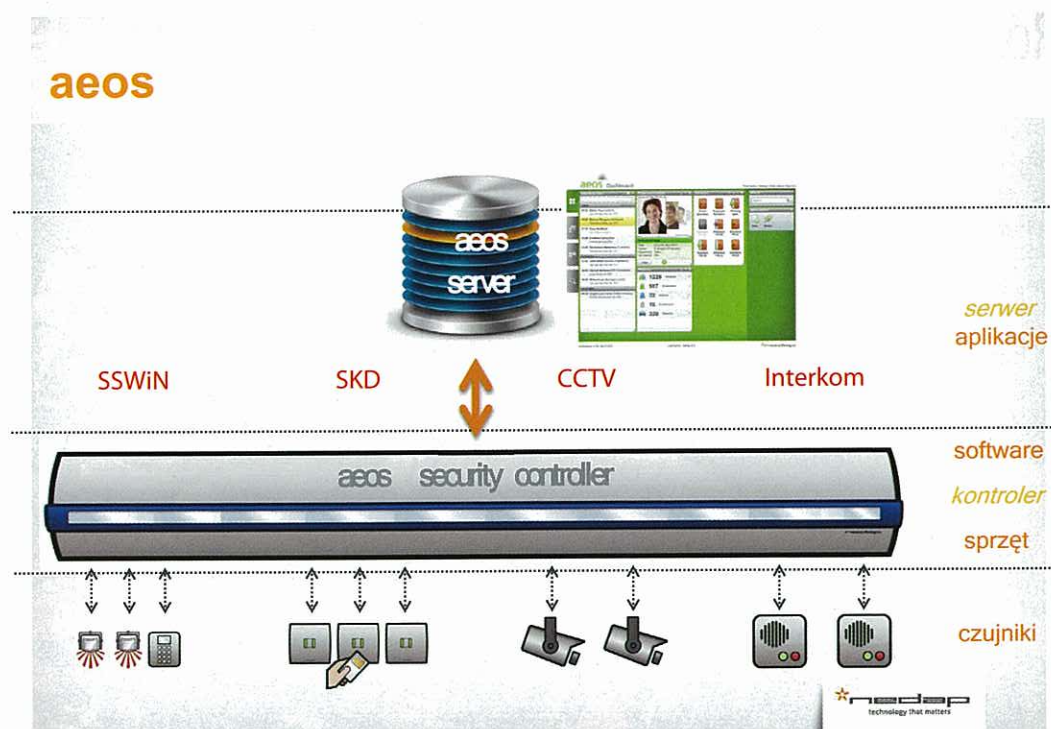
W systemie Nedap AEOS dzięki jego innowacyjnej koncepcji i ogromnym możliwościom sprzętowym możliwe jest podłączenie i pełne zarządzanie elementami peryferyjnymi z różnych podsystemów przez jeden zintegrowany kontroler. Tak więc w przypadku systemu Nedap AEOS zarówno czujki PIR, czytniki kart jak i kamery IP będą zarządzane i obsługiwane przez ten sam, wielozadaniowy kontroler zabezpieczeń. Takie rozwiązanie ma wiele zalet. Przede wszystkim uzyskuje się idealną zgodność czasową zdarzeń we wszystkich podsystemach. Istnieje możliwość dowolnego tworzenia zależności pomiędzy systemami. Zdarzenie w obrębie jednego systemu może determinować dowolne zachowanie w innym systemie lub systemach. Ponieważ ten

sam kontroler zbiera dane z systemu alarmowego, kontroli dostępu i telewizji dozorowej, z jego punktu widzenia jest to jeden zintegrowany system, którym może swobodnie zarządzać. Co więcej w Nedap AEOS kontrolery łączą się ze sobą na zasadzie *peer to peer* (każdy z każdym), mogą więc wzajemnie wymieniać ze sobą dane. Zdarzenie w obrębie jednego kontrolera, może zatem determinować reakcję elementu podłączonego do zupełnie innego kontrolera bez udziału serwera. Dokładnie taka architektura systemu została wykorzystana do zabezpieczenia lotniska w Lublinie (Świdniku), gdzie Nedap AEOS pełni rolę zintegrowanej platformy zabezpieczeń. Ogromną zaletą takiej architektury jest możliwość korzystania przez operatorów i administratorów z jednej zintegrowanej platformy i tym samym z jednego zintegrowanego interfejsu użytkownika, jednej wspólnej aplikacji i tej samej bazy danych.

Oprócz opisanych wyżej struktur systemów zabezpieczeń, w większych i rozbudowanych systemach występuje jeszcze jedna. Jest to struktura systemu nadrzędnego, lub mówiąc inaczej systemu parasolowego. W tej architekturze ponad równoległe pracującymi systemami instaluje się dodatkowy system, który posiada własny serwer i dzięki wielu interfejsom do różnych podsystemów jest w stanie zbierać z nich dane i wpływać na ich



Rys. 1. Serwery systemów bezpieczeństwa zintegrowane w oparciu o SMS lub/i integrację międzyserwerową



Rys. 2. Integracja systemów bezpieczeństwa w oparciu o wielozadaniowy kontroler systemu AEOS

działanie. System taki nazywany jest zintegrowanym systemem zarządzania bezpieczeństwem lub z angielskiego SMS (*Security Management System*). Jest to niekiedy jedyne możliwe rozwiązanie i taki rodzaj integracji pozwala zwykle na łączenie systemów produkowanych przez firmy, które nie są skłonne do bezpośredniej współpracy w zakresie integracji. W odróżnieniu od opisanego wyżej sposobu integracji przy użyciu wielozadaniowych kontrolerów bezpieczeństwa Nedap AEOS, rozwiązanie takie ma jedną wadę – tzw. pojedynczy punkt podatności na awarię – w przypadku awarii serwera systemu SMS utracona zostaje cała integracja. W praktyce jednak w obiektach o szczególnym znaczeniu stosuje się serwery redundantne, które pracując w tle są w stanie natychmiast przejąć działanie serwera uszkodzonego. Obrazowo tego typu architekturę przedstawia rys. nr 2. Również system Nedap AEOS może pracować w tak zorganizowanej strukturze.

Biorąc pod uwagę to krótkie omówienie możliwych sposobów integracji wydaje się, że projektowanie integracji poprzez wielozadaniowy kontroler Nedap AEOS jest optymalnym sposobem współdziałania systemów zabezpieczeń. Problem jednak w tym, że nie zawsze projektan-

ci systemów mają ten komfort, że mogą tworzyć architekturę systemu od zera, a użytkownik dysponuje budżetem pozwalającym na modernizację czy zakup całej infrastruktury bezpieczeństwa za jednym razem. Często projekty budowy czy rozbudowy systemów zabezpieczeń realizowane są etapowo, a istniejąca struktura w dużej mierze musi być ponownie wykorzystana. W takim przypadku inwestorzy skazani są na pewnego rodzaju kompromis pomiędzy potrzebami a możliwościami. Powinni jednak zawsze mieć na uwadze to, że im prostsza architektura i im mniej podsystemów składa się na system zintegrowany, tym integracja jest pełniejsza, a utrzymanie systemu tańsze i prostsze. Nedap AEOS dzięki swojej rewolucyjnej koncepcji integracji i maksymalnemu uproszczeniu architektury wydaje się być rozwiązaniem godnym polecenia w większości projektów, a dzięki przyjaznemu modelowi rozbudowy, możliwe jest tworzenie systemu etapowo, zaczynając np. od kontroli dostępu, a dodając w późniejszym okresie systemu alarmowego czy monitoringu.

Artykuł firmy Nedap Security Manager

Jakub KOZAK, Country Manager Poland Nedap Security Manager
jakub.kozak@nedap.com

Rozwiązania w zakresie bezpieczeństwa



W przypadku wystąpienia pożaru niezbędne jest podjęcie akcji gaśniczej tak szybko, jak to tylko możliwe. Bezpieczeństwo przebywających w obiekcie osób stanowi wartość nadrzędną. Rozwiązania umożliwiające podjęcie natychmiastowej akcji gaśniczej i stłumienie ognia w pierwszej fazie pożaru to stałe urządzenia gaśnicze (SUG), czyli samoczynne instalacje umożliwiające automatyczne wykrycie, sygnalizację pożaru oraz rozpoczęcie procesu gaszenia w chronionych strefach. Można je także stosować w obiektach służby więziennej.

Na rynku dostępna jest szeroka oferta rozwiązań w zakresie ochrony przeciwpożarowej. Wymienić można m.in. systemy gaszenia wodą (tryskaczowe, zraszaczowe, pianowe) oraz systemy gaszenia gazem. Dobór odpowiedniego rozwiązania uzależniony jest m.in. od wymagań Klienta, rodzaju chronionego obiektu (np. zakłady karne), a także przepisów i wymogów firm ubezpieczeniowych.

Urządzenia tryskaczowe są zaprojektowane w taki sposób, aby zadziałały we wstępnej fazie pożaru, przy czym otwierają

się tylko te tryskacze, które przez określony czas poddane zostaną działaniu podwyższonej temperatury – a zatem będą narażone bezpośrednio na działanie pożaru. Z danych statystycznych wynika, że w 97% przypadków do skutecznego ograniczenia rozprzestrzeniania się pożaru wystarczył jeden działający tryskacz, w 93% przypadków było to 5 tryskaczy, a więcej niż 10 działało w 78% przypadków. Powyższe dane potwierdzają fakt o selektywnym działaniu instalacji tryskaczowych, dzięki czemu zniszczenia spowodowane pożarem ograniczają się do niewielkiego obszaru. W przypadku wybuchu pożaru w budynku, w którym zainstalowany został system gaśniczy liczba ofiar śmiertelnych jest mniejsza o 57%, a straty mienia są niższe o 34% – 68%.

W strefach wymagających wyjątkowej ochrony (np. zakład penitencjarny) ważny jest dobór rozwiązania, które pozwoli na wyeliminowanie nie tylko strat spowodowanych działaniem ognia, ale też będących wynikiem przeprowadzonej akcji gaśniczej w sytuacji wystąpienia pożaru (np. zalanie). Idealnie sprawdzą się w tym



przypadku stałe urządzenia gaśnicze gazowe. Aktualnie do najbardziej skutecznych i najczęściej stosowanych należą systemy wykonane w oparciu o wodzące środki gaśnicze takie jak mieszaniny gazów obojętnych.

Korzyści z zastosowania systemów gaszenia gazem jest wiele. Najważniejsze z nich to szybka możliwość przywrócenia pełnej funkcjonalności pomieszczeń lub urządzeń w strefie objętej gaszeniem, możliwość zachowania ciągłości pracy urządzeń i procesów krytycznych w gaszonym obszarze, zapewnienie maksymalnej ochrony i bezpieczeństwa osób przebywających w chronionej strefie, brak negatywnego wpływu na środowisko naturalne, możliwość rozpoczęcia akcji gaśniczej w najwcześniejszym stadium rozwoju pożaru. W dłuższym okresie czasu użytkowania obiektu realne jest uzyskanie określonego zwrotu kosztów instalacji. Stałych Urządzeń Gaśniczych poprzez uzyskanie dzięki temu niższej składki ubezpieczenia.

Warunkiem niezawodności w/w rozwiązań jest przede wszystkim projekt techniczny wykonany precyzyjnie, zgodnie ze sztuką, uwzględniający wszystkie ryzyka i parametry pomieszczeń oraz właściwy montaż systemu. Niezbędne są także regularne przeglądy konserwacyjno-serwisowe, wykonywane przez wyspecjalizowane firmy, co stanowi gwarancję bezpieczeństwa na lata. Ważne jest też upewnienie się, czy producent systemu posiada wszelkie niezbędne aprobaty i certyfikaty uprawniające do wprowadzenia wyrobu do obrotu na terenie Polski.

AGIS Fire & Security jako dostawca i integrator elektronicznych systemów zabezpieczeń, instalacji elektrycznych, rozwiązań przeciwpożarowych swoim Klientom od wielu lat oferuje kompleksową obsługę projektów. Usługi AGIS obejmują doradztwo, projektowanie, instalowanie, uruchomienie oraz konserwację i serwis dostarczanych rozwiązań. W oparciu o specjalistyczną wiedzę i wieloletnie doświadczenie firma jest w stanie dostarczać rozwiązania szyte na miarę potrzeb klientów, uwzględniając ich indywidualne potrzeby, skalę i specyfikę budynku. AGIS Fire & Security dba o wysoką jakość, czego potwierdzeniem są systemowo zintegrowane certyfikaty: ISO 9001, AQAP 2110, PN-N 18001 oraz BS OHSAS 18001 oparte na koncepcji ciągłego doskonalenia.

W zależności od specyfiki, skali danego obiektu oraz profilu prowadzonej działalności zarządcy budynków w celu zapewnienia bezpieczeństwa decydują się na wdrożenie systemów monitoringu wizyjnego (CCTV). System ten umożliwia ciągłą i kom-

pleksową obserwację wielu obszarów chronionego obiektu (zakład karne i areszt śledczy) z jednego lub co najwyżej kilku stanowisk monitorowania.

Rozwiązanie CCTV wspomaga pozostałe systemy bezpieczeństwa i technicznej ochrony mienia, poprzez umożliwienie weryfikacji zaistniałych zdarzeń oraz ich archiwizację, tworząc w ten sposób materiał dowodowy. Podstawowym zadaniem systemu monitoringu wizyjnego jest zapewnienie bezpieczeństwa poprzez podgląd obrazu na żywo. Systemy CCTV umożliwiają również szybkie przeszukiwanie nagrań. Nowoczesne rozwiązania w zakresie monitoringu wizyjnego wyposażone są w dodatkową funkcjonalność w postaci inteligentnej analizy obrazu. Oprogramowanie analizujące obraz na żywo umożliwia np. wykrycie ruchu na terenie monitorowanego obiektu lub przekazanie właściwej osobie odpowiadającej za bezpieczeństwo informacji o nieuprawnionym wtargnięciu na dany teren. Dzięki temu nic nie umknie uwadze operatora, a zdarzenia alarmowe mogą być automatycznie wyświetlane na dodatkowym monitorze.



Obok systemów monitoringu wizyjnego narzędziem wspierającym zarządzanie bezpieczeństwem w obiekcie typu więzienie jest także system kontroli dostępu (ACC), którego głównym zadaniem jest monitorowanie oraz porządkowanie przemieszczania się osób oraz pojazdów w dozorowanych strefach.

W ten sposób system umożliwia zabezpieczenie obiektu przed dostępem osób niepowołanych oraz ogranicza poruszanie się osób nieupoważnionych do wydzielonych stref, jednocześnie pozostawiając swobodę przemieszczania się osobom uprawnionym.

W trosce o zapewnienie najwyższego poziomu bezpieczeństwa wymienione powyżej rozwiązania takie jak m.in. stałe urządzenia gaśnicze, systemy monitoringu wizyjnego, systemy kontroli dostępu mogą być zintegrowane. Instalacja Systemów Automatyki Budynkowej i Zarządzania Budynkami (BAS/BMS), pozwala także na optymalizację kosztów np. poprzez bieżące gromadzenie, przetwarzanie i archiwizowanie danych związanych ze stanem wybranych instalacji w obiekcie oraz sterowanie nimi w sposób automatyczny lub półautomatyczny.

Więcej informacji: www.agisfs.pl

Artykuł firmy AGIS Fire & Security Sp. z o.o.
Fot. AGIS Fire & Security Sp. z o.o.

Inteligentne ogrodzenia – gwarancją bezpieczeństwa i 100% skuteczności



Ogrodzenie obiektu więziennego powinno stanowić gwarancję bezpieczeństwa dla mieszkańców okolicy, w której znajduje się więzienie, personelu więziennego, a jednocześnie gwarantować przyjazne warunki przebywającym w więzieniu penitencjariuszom. Wobec tego można przyjąć, że obiekty więzienne są tak bezpieczne jak ich ogrodzenie.

Wymagania stawiane współczesnym ogrodzeniom więziennym powodują, iż nawet najlepsze fizyczne ogrodzenia składające się z dwóch linii ogrodzenia wykonanego z wysokich siatek lub paneli, zakończonych zwojami ostrzowymi, stają się niewystarczającym zabezpieczeniem. Aby sprostać rosnącym wymaganiom oraz potencjalnym zagrożeniom fizyczne ogrodzenia muszą być zintegrowane z systemami ochrony pozwalającymi na dokładne wykrycie prób ich sforsowania.

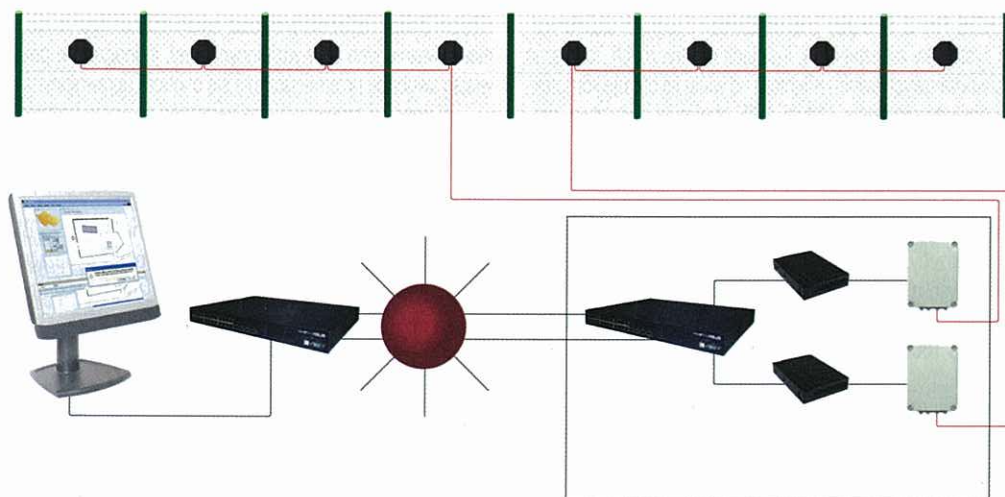
Precyzyjny system detekcji perymetrycznej PERIDECT instalowany na ogrodzeniu zapewnia dokładną i skuteczną ochronę obiektów charakteryzujących się podwyższonym poziomem ryzyka, takich jak obiekty więzienne. System ten – dzięki gęsto rozmieszczonym czujnikom – pozwala na wykrycie drgań ogrodzenia spowodowanych mechanicznym działaniem – wspinaczką, przecinaniem, podnoszeniem. Dokładność działania systemu wynosi około 2,5-3 m.

Czujniki systemu PERIDECT mogą być konfigurowane tak, aby konfiguracja odpowiadała lokalnym warunkom i wymaganiom klienta. System PERIDECT korzysta z unikalnego systemu logiki różnicowej (*Differential Logic*), która pozwala na redukcję fałszywych alarmów spowodowanych przez złe warunki pogodowe (intensywne opady, silny wiatr, grad).



System PERIDECT charakteryzuje się następującymi parametrami:

- pozwala na dokładne wykrycie miejsca wtargnięcia / próby przekroczenia,
- doskonale współpracuje z innymi systemami ochrony np. z systemem telewizji CCTV lub ochroną obwodową,
- system można indywidualnie konfigurować ustawiając jego parametry zgodnie z lokalnymi warunkami chronionego obiektu oraz wymaganiami klienta,



- ilość fałszywych alarmów wywołanych czynnikami zewnętrznymi jest znikoma,
- jest łatwy w instalacji i utrzymaniu,
- łatwość wykrywania defektów, możliwość szybkiej naprawy minimalnymi kosztami,
- szeroki zakres wytrzymałości na temperatury otoczenia (od -55 °C do +85 °C), przy czym odporność na uszkodzenia mechaniczne i promieniowanie UV,
- długa żywotność komponentów elektronicznych,
- odporność na wyładowania atmosferyczne i inne czynniki elektromagnetyczne,
- możliwa rozbudowa systemu o nowe rozwiązania przetwarzające sygnał naruszenia.

Charakterystyka systemu, wysoka jakość instalacji, jak również weryfikacja w trakcie pracy czynią z PERIDECT-u jeden z najbardziej niezawodnych systemów na rynku.

System PERIDECT dostępny jest w czterech wersjach:

1. Standardowej (*Standard*),
2. Ukrytej (*Hidden*), który pozwala na doprowadzenie przewodów wewnątrz słupów ogrodzenia,
3. Antywandalowej (*Antivandal*),
4. Podziemnej (*Underground*).

Zasadą przy stosowaniu systemów alarmowych jest stosowanie ich w kombinacji. Systemy stosuje się z reguły parami, tak aby słabości jednego systemu mogły być kompensowane mocnymi stronami drugiego. Dzięki temu ryzyko fałszywych alarmów można wyeliminować praktycznie w 100%. Oferta systemów, które mogą być stosowane w kombinacji z systemem PERIDECT obejmuje: bariery mikrofalowe, bariery na podczerwień, czujniki wykorzystujące efekt Dopplera.

Japoński producent urządzeń fotoelektrycznych TAKEX już od ponad 50 lat wytwarza bariery podczerwieni stosowane do zewnętrznych systemów ochrony obwodowej, obecnie jest jednym z wiodących producentów tych urządzeń na



świecie. W swojej ofercie oprócz aktywnych barier podczerwieni TAKEX posiada również bariery mikrofalowe oraz pasywne czujniki ruchu.

Bariery podczerwieni, zapewniając bardzo wąską strefę detekcji, szczególnie dobrze sprawdzają się jako uzupełnienie ogrodzenia wykrywając intruza bezpośrednio przed lub po jego sforsowaniu. Bardzo istotnym parametrem barier podczerwieni jest zdolność do pracy w warunkach pogorszonej przejrzystości powietrza (mgła, śnieżyca, silny deszcz). W barierach TAKEX zastosowano dwa rozwiązania – dziesięciokrotny zapas

sygnału oraz algorytm wykrywania zjawisk pogodowych. Dziesięciokrotny zapas sygnału umożliwia poprawną pracę bariery nawet wówczas, gdy mgła lub śnieżyca absorbuje 90% energii wiązek podczerwieni, algorytm wykrywania zjawisk pogodowych odróżnia całkowite przerwanie wiązki spowodowane pogorszeniem przejrzystości powietrza od jej przerywania przez intruza.

Wszystkie produkty TAKEX wytwarzane są w Japonii i objęte pięcioletnią gwarancją.

Więcej informacji na temat systemów firmy DIRICKX oraz TAKEX można uzyskać u Autoryzowanego Dystrybutora – firmy ICS POLSKA, ul. Poleczki 82, 02-822 Warszawa lub na stronie: www.ics.pl.

Artykuł firmy ICS Polska i Dirickx Bohemia
Fot. ICS Polska



PRENUMERATA ROCZNA

**Czytaj
nas
w 2014!**

**Ochrona
Mienia
i Informacji**



Prenumerata:

- drukowana **80 zł**
- cyfrowa **56 zł**
- pakietowa (drukowana + cyfrowa)

~~136 zł~~ **110 zł**

**Źródło profesjonalnej wiedzy
dla fachowców.**

Zamów prenumeratę

- wypełniając formularz na stronie: www.e-czasopismo.pl
- e-mailem: prenumerata@instalatorpolski.pl
- telefonicznie: 22 678 38 05