Obiekty logistyczne
Systemy bezpieczeństwa
System SSWiN i KD

Joanna ĆWIRKO[1]
Robert ĆWIRKO [2]

ROZWAŻANIA O SYSTEMACH OCHRONY W OBIEKTACH I CENTRACH LOGISTYCZNYCH

Rynek systemów bezpieczeństwa oferuje wiele różnorodnych systemów alarmowych i ich podzespołów. Poprawność projektowania i instalowania systemów alarmowych jest codziennie weryfikowana przez przestępców. Celem artykułu jest omówienie zabezpieczeń wybranych elementów systemu bezpieczeństwa. Przedstawiono krytyczne rozważania dotyczące konieczności zabezpieczeń torów transmisji sygnałów alarmowych, systemów kontroli dostępu oraz mechanicznych i elektromechanicznych systemów ochrony w obiektach logistycznych.

DISCUSION ON SECURITY SYSTEMS IN LOGISTIC CENTERS AND OBJECTS

The market of securities is offering many alarm systems and their components. Validity of designing and installation of security system is examine by buglers, every day. The aim of this article is showing protection of chosen compound security systems. The paper presents analyses of protection of alarm transmission systems, access control, mechanical and electromechanical security systems in logistic centers and building.

1. WSTĘP

Systemy inżynierii bezpieczeństwa powinny być bezwzględnie optymalizowane nie tylko pod kątem zastosowanych rozwiązań technicznych, ale też z uwzględnieniem specyfiki obiektów, które mają chronić. I tak w przypadku obiektów objętych nadzorem konserwatorskim [1] (zabytkowe kościoły, muzea, pałace itp.) ważnym elementem jest takie zaprojektowanie połączeń między poszczególnymi modułami systemu bezpieczeństwa, żeby zminimalizować liczbę nawierzchniowych połączeń kablowych. W takim przypadku dobrym rozwiązaniem może się okazać przyjęcie bezprzewodowej struktury połączeń (drogą radiową).

W przypadku obiektów logistycznych jednym z ważnych kryteriów projektowych jest odporność systemu bezpieczeństwa na wszelkie próby ze strony nieuprawnionych użytkowników np. sabotażu i próby zakłóceń poprawnej pracy [2]. W takim przypadku

[1] Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, Polska 00-908 Warszawa; Gen. S. Kaliskiego 2.Tel: +48 22 6839-626, E-mail: joanna.cwirko@wat.edu.pl
[2] Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, Polska; 00-908 Warszawa; Gen. S. Kaliskiego 2.Tel: +48 22 6837-123, E-mail: robert.cwirko@wat.edu.pl

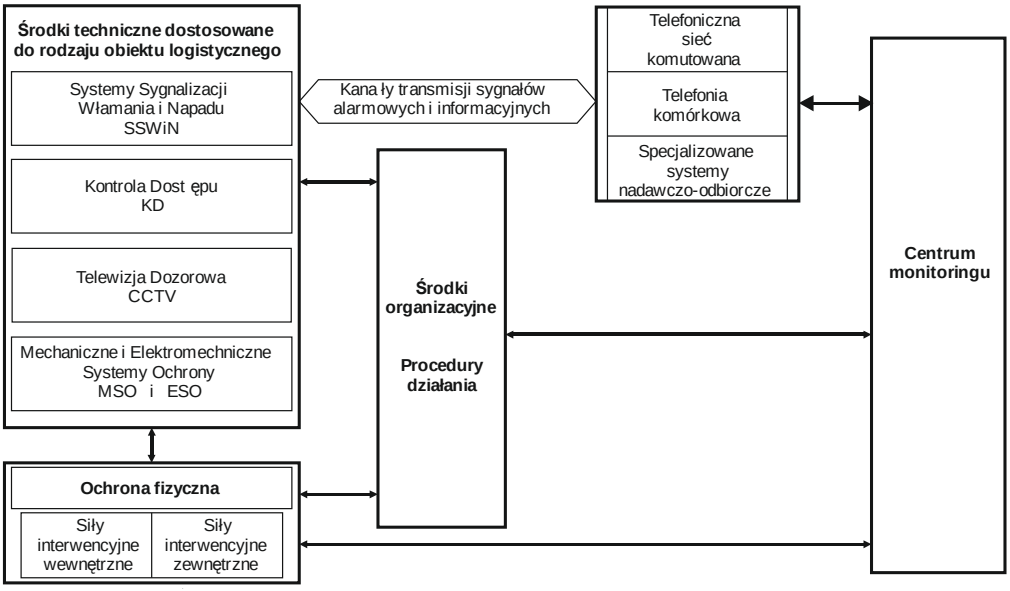
systemy łączności bezprzewodowej w systemie sygnalizacji włamania i napadu mogą się okazać gorszym rozwiązaniem w stosunku do połączeń przewodowych.

Na terenie obiektów logistycznych z natury rzeczy w czasie zwykłej pracy oprócz pracowników przebywa wielu kontrahentów, czyli osób postronnych. Ograniczenie ruchu tych osób w przypadku zastosowania klasycznego systemu kontroli dostępu może być kłopotliwe. Różnorodność rodzajów obiektów logistycznych jest bardzo duża i dla każdego z nich należy zastosować optymalną strukturę systemu bezpieczeństwa.

2. SYSTEM BEZPIECZEŃSTWA OBIEKTÓW LOGISTYCZNYCH

Na rysunku 1 przedstawiono typową strukturę systemu bezpieczeństwa przeznaczonego dla obiektów logistycznych.

Na tym poziomie prezentacji struktura ta jest bardzo podobna do struktury systemów bezpieczeństwa stosowanych w przypadku innych rodzajów obiektów, jednakże pozwala ona na pokazanie problemów odgrywających decydującą role przy projektowaniu zabezpieczeń dla obiektów logistycznych [3].



Rys. 1. Typowa struktura systemu bezpieczeństwa przeznaczonego dla obiektów logistycznych

W historii rozwoju systemów bezpieczeństwa struktura ochrony fizycznej przechodziła różne fazy rozwoju. W pierwszym etapie dominowały systemy zabezpieczenia obiektów z wykorzystaniem głównie wykwalifikowanych służb, przy niewielkim wsparciu środków technicznych np. punktów kontrolujących prawidłowe patrolowanie terenu przez wartowników. W następnych latach wzrastała rola środków technicznych realizujących

głównie funkcje systemów sygnalizacji włamania i napadu (SSWiN) oraz systemów kontroli dostępu (KD) przy wsparciu telewizji dozorowej (CCTV) oraz mechanicznych (MSO) i elektromechanicznych (ESO) systemów ochrony [4][5].

Nieprawidłowa analiza ekonomiczna (oczekiwane oszczędności na wynagrodzeniu pracowników itp.) była w wielu przypadkach przyczyną całkowitej eliminacji ochrony fizycznej i projektowania systemów bezpieczeństwa tylko w oparciu o środki techniczne. Okazało się jednak, że funkcjonowanie systemów bezpieczeństwa w tej postaci ma wiele mankamentów. Zminimalizowany został efekt odstraszający, przykładowo w postaci uzbrojonego strażnika. Brak personelu nadzorującego powodował, że elementy SSWiN i CCTV były dewastowane. Ponadto wiele elementów systemów KD nie realizowało prawidłowo swojej funkcji bez współdziałania z odpowiednimi służbami. Przykładowo, mechaniczne zapory przejść w metrze są łatwe do przeskoczenia przez bardziej wysportowanych ale niezdyscyplinowanych pasażerów. Mimo stosowania coraz bardziej zawansowanej techniki systemy SSWiN oraz KD nie są w 100% niezawodne. W zależności od sytuacji generują znaczną liczbę fałszywych sygnałów alarmowych i informacyjnych odbieranych przez obsługujące je centra monitoringu. Przeważnie centra monitoringu są to firmy zewnętrzne (np. Juventus, Solid Security), które obciążają użytkowników systemów bezpieczeństwa znacznymi kosztami nieuzasadnionych interwencji. Okazuje się w wielu przypadkach, że koszty tych interwencji przewyższają koszty zatrudnienia odpowiednich pracowników, którzy mogą m.inn. rozpoznać fałszywy alarm i natychmiast odwołać telefonicznie rozpoczęcie interwencji sterowane z centrum monitoringu.

Dobrze zaprojektowany system bezpieczeństwa dla konkretnego obiektu to system, w którym prawidłowo określono proporcje między poszczególnymi elementami składowymi przedstawionymi na rys. 1. Poszczególne elementy takiego systemu muszą być powiązane między sobą za pomocą odpowiednich procedur działania

2. SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU

Przyjęcie przez centralę sygnału alarmowego z czujki może powodować różnorodne działania, na przykład: uruchomienie sygnalizatora akustycznego z jednoczesnym wysłaniem odpowiedniego komunikatu do stacji monitoringu, wysłanie komunikatu do centrum monitoringu bez włączania sygnalizatora akustycznego, tzw. cichy alarm, wykorzystanie wyjść funkcyjnych centrali do opcjonalnego uruchomienia oświetlenia terenu itd.

2.1 Czujki a niezawodność SSWiN

Struktura systemu SSWiN bazuje na module centrali alarmowej, do której podłączone są różne rodzaje czujek [6][7]. Najczęściej wykorzystywane typy czujek to: czujki piroelektryczne (PIR), magnetyczne czujki kontaktronowe i czujki sygnalizujące stłuczenie szyby. Stosuje się też czujki mikrofalowe bazujące na zjawisku Dopplera, czujki reagujące na przerwanie toru podczerwieni lub mikrofal, czujki światłowodowe reagujące na nacisk, czujki ultradźwiękowe, czujki sejsmiczne, czujki pojawienia się gazu, wody itp.

Sposób podłączenia czujki do centrali alarmowej zależy od zastosowanych w czujce rozwiązań konstrukcyjnych mających za zadanie przekazanie informacji o zmianie jej

stanu z czuwania w stan alarmu. Najczęściej następuje to po zmianie wysterowania przekaźnika na wyjściu czujki, który przełącza swoje zestyki, na przykład ze zwarcia (NC) w stanie czuwania, do rozwarcia w stanie wykrycia alarmu. Zestyk przekaźnika czujki można podłączyć w sposób bezpośredni do danego wejścia linii dozorowej centrali alarmowej, ale preferowane jest jego podłączenie za pośrednictwem rezystorów parametryzujących (konfiguracje EOL lub 2EOL), gdyż pozwala to wykryć dodatkowo sytuacje związane z próbą przecięcia linii dozorowej lub próbą zwarciowego obejścia zestyku przekaźnika czujki.

Do każdego wejścia dozorowego centrali alarmowej podłącza się jedną czujkę. Typowo, płyta główna średniej klasy centrali alarmowej posiada 16 wejść linii dozorowych, przy czym liczba może być na zwiększona przez dołączenie dodatkowych modułów rozszerzeń do 64 wejść czy więcej. Możliwe jest także, chociaż nie zalecane, wykorzystanie jednej linii dozorowej centrali alarmowej do szeregowego podłączenia kilku czujek.

Dla rozwiązania z użyciem klasycznych konfiguracji linii dozorowych, uszkodzenie czujki lub linii transmisyjnej łączącej czujkę z wejściem dozorowym centrali eliminuje tylko tą czujkę i po uaktywnieniu przez użytkownika funkcji „bypass" ta linia dozorowa zostaje wyłączona elektrycznie ze struktury centrali i nie zakłóca działania pozostałych czujek.

Niektóre centrale alarmowe posiadają wydzieloną magistralę dwuprzewodową, do której można dołączyć równolegle do kilkudziesięciu czujek adresowalnych. Każda z tych czujek posiada nadany przez producenta niepowtarzalny adres, za pomocą którego jest ona identyfikowana po przyłączeniu do magistrali. Zaletą tego rozwiązania jest możliwość dołączania kolejnych czujek bez prowadzenia dodatkowego okablowania lub zwiększania linii dozorowych za pomocą dodatkowych modułów. Jednakże w przypadku uszkodzenia takiej magistrali dwuprzewodowej, centrala alarmowa przestaje widzieć wszystkie dołączone do tej magistrali czujki.

2.1 Możliwość uszkodzenia toru transmisji do stacji monitorigu

Często centrala alarmowa jest konfigurowana tak, aby sygnały alarmowe a także informacyjne były przekazywane z centrali alarmowej do stacji monitoringu za pośrednictwem komutowanej linii telefonicznej. Testowanie linii komutowanej, celem wykrycia ewentualnego przecięcia linii przez włamywacza odbywa się w określonych interwałach czasowych i dopiero powtórzenie informacji o sabotażu w kilku kolejnych chwilach czasowych powoduje wygenerowanie przez system sygnału alarmu. Ma to zapobiec generowaniu fałszywych alarmów w przypadku zdarzających się krótkotrwałych zaników napięcia stałego w centrali telefonicznej, do której przyłączona jest linia komutowana. Obeznany z zagadnieniami telekomunikacji przestępca może przeciąć linię telefoniczną i szybko dołączyć na odcinku do centrali alarmowej odpowiednie urządzenie elektroniczne symulujące sprawność linii transmisyjnej.

W przypadku obiektów o wyższej klasie ochrony, gdy wymagane są dwa niezależne tory transmisji, lub gdy brak jest linii telefonicznej w chronionym obiekcie, stosuje się jako moduł nadawczo-odbiorczy telefon komórkowy z odpowiednim interfejsem. Po wykryciu alarmu przez centralę alarmową telefon komórkowy wybiera najpierw numer stacji monitoringu, potem czeka na zestawienie połączenia a następnie przesyła odpowiedni kod informacji.

Przestępca chcąc zagłuszyć transmisję przez sieć komórkową ma do wyboru głównie następujące możliwości: włączyć urządzenie zagłuszające przed wejściem do chronionego obiektu lub prowadzić nasłuch początku transmisji komunikatu alarmowego i dopiero po tym włączyć zagłuszanie. Ten drugi sposób zmniejsza prawdopodobieństwo wykrycia włączenia urządzenia zagłuszającego. Na rysunku 2a przedstawiono wykrywacz telefonów komórkowych WKT-2000 [8].

a) *b)*

Rys. 2. Wykrywacz telefonów komórkowych WKT-2000 i zagłuszarka GS-200

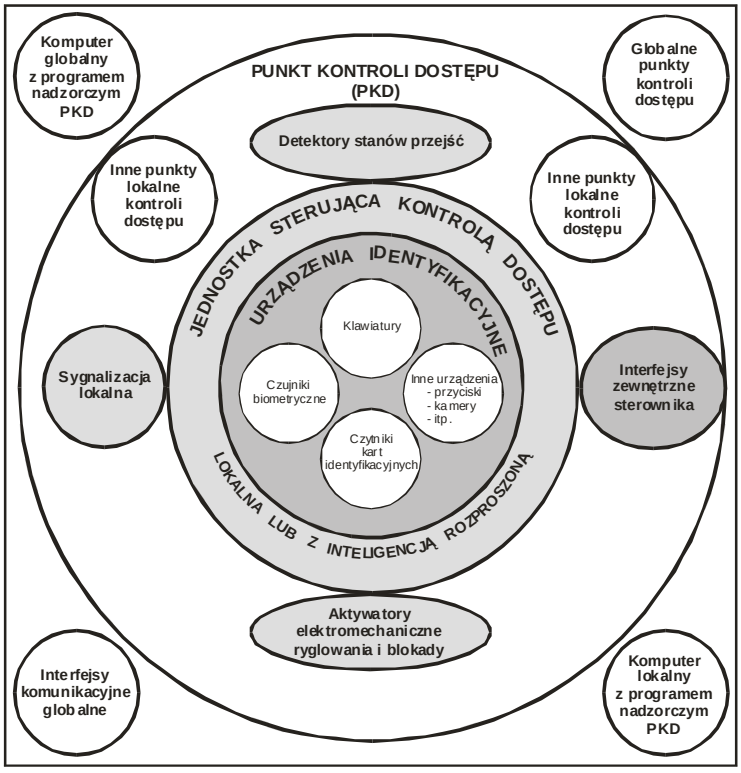
Wykrywacz może współpracować z urządzeniem zagłuszającym, na przykład GS-200 (rys. 2b). W momencie wystąpienia jakiegokolwiek sygnału transmisji radiowej, na przykład rozpoczęcia przez telefon komórkowy systemu centrali alarmowej wybierania numeru stacji monitoringu, urządzenie zagłuszające zostanie aktywowane przez WKT-2000 w czasie nie dłuższym niż 20 ms. Urządzenie GS-200 zagłusza systemy łączności cyfrowe oparte o standardy : IDEN, TDMA, CDMA, GSM, UTMS oraz analogowe: AMPS, NMT, N-AMPS, TACS [9]. Maksymalna moc wyjściowa wynosi 12 W, co pozwala to na zagłuszenie nadajnika radiowego centrali alarmowej z odległości 40-50 metrów. Zagłuszarki służą także do zakłócenia kontaktu między centralą alarmowa a czujkami bezprzewodowymi, w tym kamerami bezprzewodowymi. W przypadku alarmów samochodowych silny sygnał zagłuszarki blokuje działanie pilota, co powoduje, że nie zadziałają siłowniki zamykające drzwi.

W przypadku obiektów logistycznych bezwzględnie należy zwielokrotniać tory transmisyjne, którymi mają być przesyłane sygnały alarmowe i informacyjne, czyli umożliwić przykładowo transmisję za pomocą telefonicznej linii komutowanej i GSM lub GPRS. Przy zabezpieczeniu obiektów specjalnych, lub braku zasięgu telefonii komórkowej, korzysta się często z wydzielonej sieci łączności radiowej

2. SYSTEMY KONTROLI DOSTĘPU W OBIEKTACH LOGISTYCZNYCH

Celem systemów kontroli dostępu (KD) jest wyłączne dopuszczenie uprawnionych osób do określonych miejsc chronionych. Rozpoznawanie i identyfikacja osób może odbywać się na różnych poziomach: od zadeklarowania głosowego przez daną osobę chęci wejścia do chronionej strefy (np. domofon), poprzez podanie kodu identyfikacyjnego, okazanie karty identyfikacyjnej, po rozpoznanie określonych cech biometrycznych (linie papilarne, kształt dłoni, tęczówka oka itp.) [10].

Wybierając techniki rozpoznania i identyfikacji w systemach KD w obiektach logistycznych trzeba mieć na uwadze głównie następujące uwarunkowania: przepustowość zastosowanego rozwiązania (proces rozpoznania i identyfikacji może trwać od kilku do kilkudziesięciu sekund), jakość rozpoznania (kartą identyfikacyjną lub kodem PIN może posługiwać się inna osoba), minimalny poziom inwazyjności zastosowanego systemu KD (np. wykluczenie skanowania siatkówki oka wiązka laserową), łatwość zaadaptowania systemu kontroli dostępu do rejestracji czasu pracy, możliwość integracji z pozostałymi systemami (SSWiN, ochrony p-pożarowej, automatyki budynku inteligentnego itp.).



Rys. 3. Struktura globalnego systemu kontroli dostępu

W wielu przypadkach systemy KD mają strukturę autonomiczną np. zamki biometryczne. Coraz częściej systemy KD obejmują jednak swoim zasięgiem działania nie tylko jeden budynek, z podziałem na ulokowane w nim jednostki organizacyjne, ale mogą mieć charakter globalny (rys. 3). Przykładowo, kierownictwo koncernu w Nowym Jorku może mieć dostęp, przez przeglądarkę internetowa, do danych z lokalnych systemów KD firm zlokalizowanych w Polsce, Korei itd.

Systemy KD nie ograniczają się tylko do zabezpieczenia budynków, urządzeń technologicznych i pojazdów samochodowych. Coraz większą uwagę przywiązuje się do zabezpieczenia informacji, szczególnie przekazywanych drogą komputerową. Dlatego też tworzone są coraz bardziej skomplikowane systemy identyfikacyjne w połączeniu z metodami kryptograficznymi dla szyfrowania informacji. Wiąże się to między innymi coraz powszechniej używaniem podpisu elektronicznego w różnorodnych operacjach np. parafowanie umów i operacje bankowe. Ze względu na wprowadzanie na rynek coraz wydajniejszych systemów komputerowych, średni czas bezpiecznej stosowalności danej techniki zabezpieczeń informacji szacowany jest na 3-4 lata, po czym algorytm pracy musi zostać zmieniony na bardziej rozbudowany.

4. MECHANICZNE I ELEKTROMECHANICZE SYSTEMY OCHRONY

W systemach kontroli dostępu KD powiązanie z różnorodnymi modułami mechanicznych (MSO) i elektromechanicznych (ESO) systemów ochrony jesto wiele bardziej naturalne niż w systemach SSWiN. Systemy KD współpracują z zaporami przejść, elektroryglami, zamkami elektrycznymi itp.

Jednakże w wielu aplikacjach moduły MSO i ESO są stosowanie samodzielnie bez współpracy z SSWiN lub KD. Przykładowo są to różnorodne kraty i systemy zamknięć począwszy od zamków drzwiowych ogólnego zastosowania a skończywszy na zabezpieczeniu sejfów i skarbców [11]. Należy jednak zdawać sobie sprawę, że brak współpracy MSO i ESO z innymi systemami ochrony obniża znacznie poziom zabezpieczenia obiektu. Załóżmy sytuację, że przestępca na pokonanie zamka w drzwiach potrzebuje 10 minut. Sygnał alarmowy zostanie wygenerowany przez SSWiN dopiero w momencie otwarcia skrzydła drzwi, na skutek naruszenia czujki kontaktronowej. Gdyby alarm pojawił się w momencie, gdy przestępca rozpocznie manipulacje w zamku, służby interwencyjne zareagowałyby wcześniej.

Niestety na dzień dzisiejszy tylko niewiele typów zamków ma rozwiązania techniczne pozwalające na bezpośrednie sprzężenie z systemem alarmowym. Niektóre z tych zamków mają co prawda w swojej obudowie lokalne systemy alarmowe, uruchamiające niewielki sygnalizator akustyczny (aż do czasu wyczerpania się baterii), ale bez wyprowadzenia sygnału alarmu do centrali alarmowej pozwalającej na transmisję alarmu do stacji monitoringu.

Ze względu na zastosowanie i kryteria oceny systemy zamknięć możemy podzielić na grupy: zamki drzwiowe ogólnego stosowania, zamki specjalne zwane zamkami o wysokim stopniu zabezpieczenia (ZWSBP) lub zamkami o wysokiej skuteczności bezpiecznego przechowywania HSL (*ang. High Security Lock*), zamki specjalne znajdujące zastosowanie w urządzeniach do przechowywania dokumentów niejawnych zgodnie z dyrektywami NATO, do obiektów o specjalnej ochronie - konstruowane do konkretnych celów w oparciu o cechy biometryczne człowieka np. linie papilarne, siatkówka oka, głos. Ze względu na

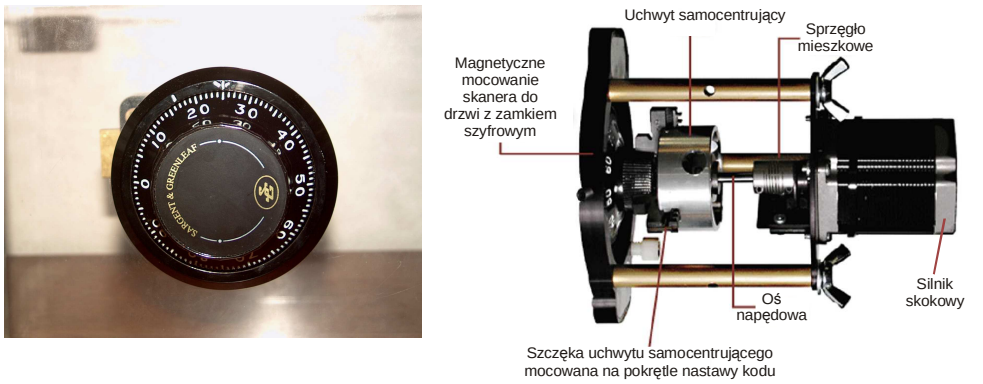
konstrukcję zamki dzielimy na grupy: zamki bębenkowe i wkładki bębenkowe, zamki zapadkowe, zamki szyfrowe, zamki elektryczne, zamki biometryczne.

Przy doborze typów zamków do ochrony obiektów logistycznych trzeba uwzględnić wysokie umiejętności przestępców. I tak zamki ogólnego zastosowania są klasyfikowane do najwyższej grupy jeżeli ich otwarcie typowymi metodami stosowanymi przez przestępców nie nastąpi wcześniej niż w ciągu 5 minut. Jednakże czas ten można zwiększyć do 20 minut montując wraz z zamkiem odpowiednie tarcze ochronne utrudniających dostęp przestępcy do newralgicznych elementów zamka.

Niezależnie od konstrukcji zamka jego mocowanie powinno być zgodne z zaleceniami producenta. Większość przestępców rozpoczyna zmagania z zamkiem od próby jego siłowego wyważenia. Średniej klasy wkładka bębenkowa jest otwierana przez przestępców w ciągu kilku minut. Zamki z wkładkami źle zamontowanymi, tak że wystają one ponad powierzchnie drzwi powyżej 3 mm są otwierane przez przestępców w czasie poniżej 20 sekund.

Z kolei zamki szyfrowe mechaniczne (rys. 4a), zaliczające się do grupy zamków o wysokiej skuteczności bezpiecznego przechowywania HSL, są stosowane przykładowo do zabezpieczania sejfów, skarbców, drzwi do kancelarii tajnych itp. W zależności od konstrukcji ich ceny wahają się od kilkuset do kilku tysięcy złotych [12]. Te najdroższe posiadają największą liczbę kombinacji szyfrowych (do ok. 170 mln) i są odporne na próby otwarcia z wykorzystaniem nasłuchu akustycznego, prześwietlenia promieniowaniem rentgenowskim itp. Zamki mechaniczne szyfrowe ze średniego przedziału cenowego nie są zabezpieczone między innymi przed nasłuchem akustycznym i mogą być otworzone w ciągu około 1 godz. za pomocą skanera [13] przedstawionego na rys. 4b.

a) *b)*



Rys. 4. Szyfrowy zamek mechaniczny typ 6730 firmy Sargent & Greenleaf (a) i skaner do otwierania zamków szyfrowych mechanicznych (b)

Trójszczękowy uchwyt skanera połączony z pokrętłem zamka szyfrowego jest napędzany według odpowiedniego algorytmu silnikiem skokowym sterowanym z laptopa. Program laptopa analizuje także sygnały z systemu mikrofonów przymocowanych do drzwi np. sejfu.

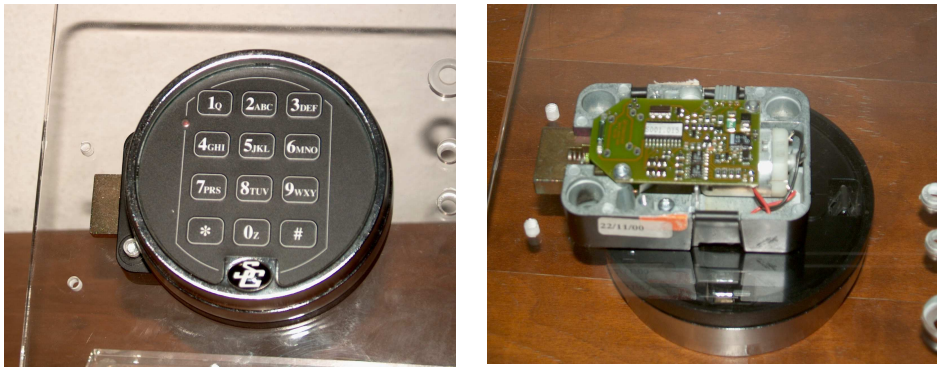
Z niektórymi konstrukcjami mechanicznych zamków szyfrowych mogą współpracować

oddzielne urządzenia zegarowe blokujące możliwość otwarcia zamka, na przykład w godzinach nocnych, mimo znajomości kombinacji szyfrowej.

Przy montowaniu zamków szyfrowych w obiektach logistycznych, należy najpierw zwrócić uwagę czy nie istnieje możliwość podejrzenia kombinacji liczb otwierających zamek np. przy pomocy miniaturowej kamery. Może to mieć miejsce, gdy zamek szyfrowy jest montowany w drzwiach wychodzących na ogólnie dostępny korytarz. Funkcje szyfrowego zamka mechanicznego sprowadzają się tylko do otwierania i zmykania chronionego obiektu.

Zamki szyfrowe elektroniczne (rys. 5) pozwalają na realizację wielu dodatkowych funkcji jak na przykład: wprowadzenie zbioru kodów dostępu o różnych poziomach hierarchii (kod główny, kasowania, kody użytkowników, wprowadzenie zwłoki czasowej itp.).

a) *b)*



Rys. 5. Zamek szyfrowy elektroniczny typ 6124 firmy Sargent & Greenleaf, widok z przodu (a), widok wnętrza z tyłu (b)

Należy zauważyć, że mimo mniejszej ilości funkcji ważniejsze banki szwajcarskie preferują mechaniczne zamki szyfrowe jako mniej zawodne. Do zadziałania mechanicznego zamka szyfrowego wystarczy prawidłowa praca około 10 elementów mechanicznych. W elektronicznym zamku szyfrowym na samej płytce drukowanej elektroniki może znajdować się kilkaset przelotek i lutów. Każdy z tych punktów może by potencjalnym źródłem niesprawności zamka.

4. WNIOSKI

W artykule przedstawiono uwagi odnośnie projektowania systemów ochrony w obiektach logistycznych. Nie istnieje idealny system ochrony, lecz zachowanie odpowiednich proporcji między poszczególnymi częściami składowymi systemu może zapewnić wymagany poziom bezpieczeństwa.

Należy szeroko uwzględniać aspekt współdziałania wszystkich systemów ochrony – SSWiN, SKD, CCTV, nie lekceważąc systemów MSO i ESO.

Przy projektowaniu struktury systemów bezpieczeństwa dla obiektów logistycznych należy zwrócić szczególną uwagę na kanały transmisyjne, którymi będą przekazywane

automatycznie informacje do zewnętrznych centrów monitoringu. Jest to bardzo wrażliwy punkt każdego systemu bezpieczeństwa, gdyż zablokowanie działania tych kanałów transmisyjnych przez przestępców, w większości przypadków drastycznie obniża skuteczność zabezpieczenia obiektu.

Przestępcy próbując unieszkodliwić działanie systemu ochrony wyszukują słabych punktów w poszczególnych jego elementach składowych lub procedurach wiążących te elementy. Dlatego też tak ważna jest na poziomie projektowania systemu ochrony krytyczna analiza zastosowanych rozwiązań technicznych i organizacyjnych. Błędy popełnione na tym etapie ujawniają się niestety w wielu przypadkach dopiero po popełnieniu przestępstwa a ich usunięcie jest przeważnie bardzo kosztowne

4. BIBLIOGRAFIA

[1] Polewiak S., Ogrodzki P., Rulewicz J.: *Vademecum zabezpieczenia muzeów.* Wydawnictwa PAGINA i DYSKRET, ISBN 83-86351-41-1
[2] Cumming N.: *Security. A Guid to Security System Design and Equipment Selection and Instalation*. Butterworth-Heinemann, ISBN 0-7506-9624-9
[3] Schaub J. L., Biery Jr. K. D.: *The Ultimate Security Survey*. Butterworth-Heinemann, ISBN 0-7506-7091-6
[4] Matchett A. R.: *CCTV for Security Professional*. Butterworth-Heinemann, ISBN 0-7506-7303-6
[5] Praca zbiorowa pod red. Wójcika A.: *Mechaniczne i elektroniczne systemy zabezpieczeń*. Velgad Dashofer, 2008
[6] PN-EN 50131-1:2009/A1. *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*
[7] PN-EN 50131-2-2. wrzesień 2009. *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 2-2: Czujki sygnalizacji włamania. Pasywne czujki podczerwieni*
[8] Materiały firmy Elektronik-System, *www.elektronik-system.pl*
[9] Materiały firmy Euro-Soft, *www.euro-soft.pl/gsm.php*
[10] Bolle R., M., Connell J. H., Pankanti S., Ratha N. K., Senior A. W.: *Biometria*. WNT. ISBN 978-83-204-3332-6
[11] Konicek J., Little K,: *Security, ID Systems and Lock. The Book on Electronic Acces Control*. Butterworth-Heinemann, ISBN 0-7506-9932-9
[12] Strona internetowa firmy Pol-Ital, www.polital.com.pl
[13] Strona internetowa firmy Intralock Tools Ltd, www.intralocktools.com