4.3 Elementy kontroli dostępu

Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- **czym są i jak działają szyfratory i kontrolery dostępu;**
- **jaka jest zasada działania urządzeń opierających się na niepowtarzalnym identyfikatorze;**
- **jak działają systemy biometryczne;**
- **do czego służą elektrozwory i elektrozaczepy;**
- **jak zabezpieczyć się przed próbami niedozwolonego dostępu do tych urządzeń.**

Elementami kontroli dostępu są urządzenia pozwalające na uzyskanie dostępu do danej sfery oraz uniemożliwiające dostęp do stref chronionych. Taki sprzęt może być bardzo prosty i składać się zaledwie z dwóch elementów: pojedynczego kontrolera i zwory zamka elektromagnetycznego albo tworzyć zaawansowane systemy przechowujące dane o tysiącach osób i zarządzające setkami stref.

4.3.1. Szyfratory i kontrolery dostępu

Szyfrator – nazywany również klawiaturą lub manipulatorem – to urządzenie umożliwiające wprowadzenie hasła (zazwyczaj w formie liczbowej), a czasem także bezpośrednie sterowanie elektrozworą lub elektrozamkiem. Zazwyczaj pracuje w połączeniu z centralą alarmową.

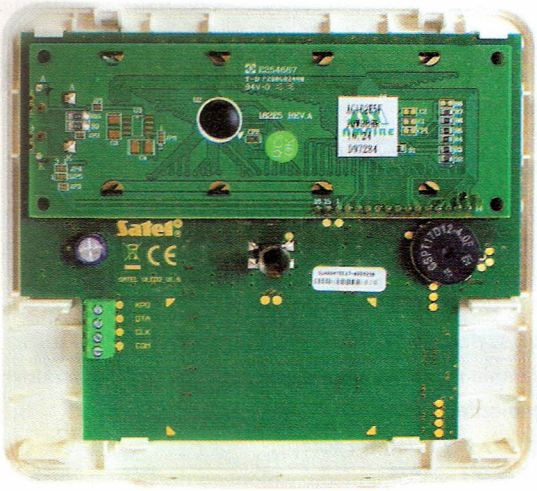
Kontrolery – zwane też sterownikami dostępu – to urządzenia autonomiczne, sterujące elektrozworami i zamkami. Często można je łączyć w sieć, co umożliwia wymianę informacji o logowaniu, lub łączyć z centralą alarmową w celu integracji z system zarządzania dostępem.

Niezależnie od pełnionej funkcji urządzenia tego typu powinny przechodzić okresową kontrolę i być zabezpieczone przed możliwością manipulacji lub podejrzenia wpisywanych kodów przez osoby niepowołane. Najczęstszym **błędem** jest używanie krótkich, długo niezmienianych kodów. Po pewnym czasie zużycie niektórych przycisków lub zabrudzenia na klawiaturze mogą umożliwić złamanie hasła.

W manipulatorach i sterownikach dostępu często integruje się **czytniki kart inteligentnych** działających zbliżeniowo. Rzadziej są to czytniki kart czipowych bądź magnetycznych. W zależności od ustawień urządzenia jest wymagana kombinacja szyfru i użycia karty bądź każdy z tych sposobów rozbrojenia systemu może być stosowany zamiennie.

WARTO WIEDZIEĆ

Jeśli szyfratora używa kilka osób, można ograniczyć się do krótkich haseł, np. czterocyfrowych. Jeśli jednak jest ich więcej, hasła powinny być pięcio- lub sześciocyfrowe, aby zwiększyć poziom bezpieczeństwa.



Rys. 4.18. Wnętrze manipulatora (widoczne: zaciski do połączenia z centralą, na górze – płyta wyświetlacza LCD, na środku – sprężyna umieszczona na mikroprzełączniku antysabotażowym, po prawej – brzęczyk piezoelektryczny)

W czasie przeglądów technicznych należy zwracać szczególną uwagę, czy na manipulatorze lub sterowniku nie widać śladów, które mogłyby wskazywać na próby niedozwolonego dostępu, takich jak próby otwarcia obudowy czy odczytania haseł przez zastosowanie mikrokamery lub nakładki na klawiaturę.

Główne **przyczyny awarii** tego typu urządzeń to:

- uszkodzenia mechaniczne,
- zużycie elementów przycisków,
- awarie elektroniki.

4.3.2. Karty, klucze, piloty

Wprowadzanie haseł i szyfrów przez manipulator jest prostym i stosunkowo tanim rozwiązaniem, wymaga jednak zapamiętania haseł. Istnieje też niebezpieczeństwo poznania hasła przez osobę postronną. Rozwiązaniem tych problemów jest **element identyfikujący** wręczony uprawnionej osobie. Może to być:

- pilot radiowy,
- karta kodowa,
- karta zbliżeniowa,
- brelok zbliżeniowy.

Wszystkie te systemy opierają się na elemencie z zapisanym **niepowtarzalnym identyfikatorem**, który jest odczytywany w czytniku manipulatora lub kontrolera dostępu.

Producenci kart i breloków dbają o niepowtarzalność numerów, dlatego zazwyczaj nie ma możliwości uzyskania duplikatu karty.

Najczęstszymi problemami związanymi z działaniem tego sposobu zabezpieczeń są:

- uszkodzenia mechaniczne i elektryczne kart dostępowych,
- zakłócenia elektromagnetyczne niepozwalające na odczytanie kart,
- błędy w oprogramowaniu,
- bliskość kilku kart, które jednocześnie próbują wysłać swoje identyfikatory.

ZAPAMIĘTAJ

Systemy oparte na niepowtarzalnym identyfikatorze są bardzo wygodne w obsłudze, ale istnieje niebezpieczeństwo zgubienia lub kradzieży karty, klucza czy pilota. Dlatego często łączy się je z koniecznością wprowadzenia hasła, co znacznie zwiększa bezpieczeństwo, gdyż dostęp jest możliwy po spełnieniu dwóch warunków:

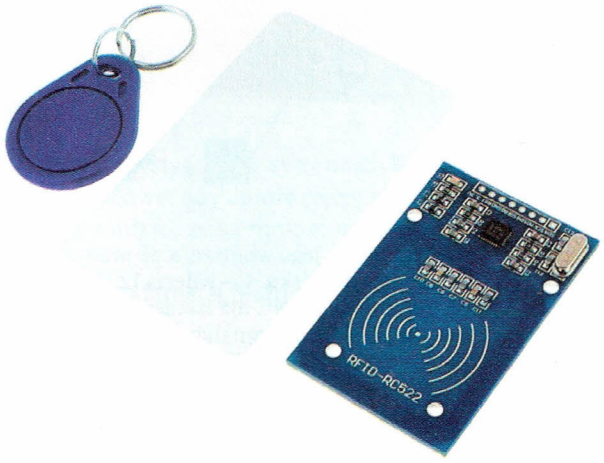
- coś wiem (hasło),
- coś mam (karta).

Wadą systemów wykorzystujących takie zabezpieczenia jest możliwość:

- skopiowania kart przy użyciu specjalnych urządzeń,
- zakłócenia ich pracy,
- przechwycenia kluczy w czasie próby użycia karty.

WARTO WIEDZIEĆ

Część kart działających na podstawie technologii zbliżeniowej można skopiować przy użyciu smartfona obsługującego technologię NFC. Może się to odbyć nawet z odległości kilkudziesięciu centymetrów. Dlatego tak ważne jest, by trzymać karty w bezpiecznym miejscu. Dotyczy to również kart bankowych.



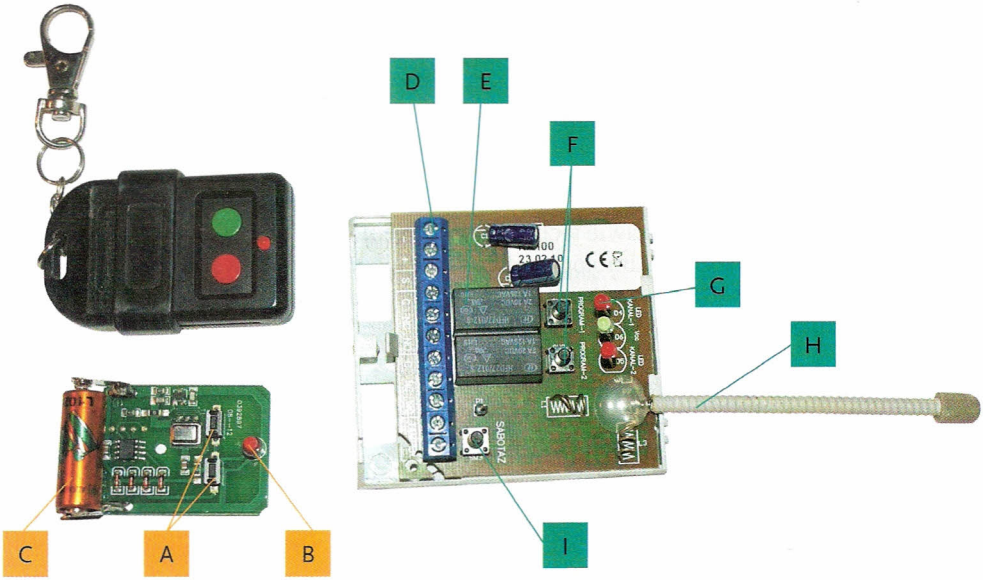
Rys. 4.19. Karta i brelok zbliżeniowe

Na podobnej zasadzie działają **piloty** służące do wysyłania informacji do systemu alarmowego. Ich odbiorniki mogą obsługiwać bezpośrednio zamki i rygle lub być włączone do centrali alarmowej. Zaletą tego rozwiązania jest możliwość sterowania urządzeniami ze znacznej odległości oraz to, że pilot może służyć jako osobisty przycisk antynapadowy. Główna wada to możliwość złamania, skopiowania lub przechwycenia klucza szyfrującego przez osobę niepowołaną.

Nawet piloty o zmiennym kodzie są podatne na technikę przechwycenia. Dlatego – o ile to możliwe – należy ograniczać moc nadajników, aby utrudnić przechwycenie klucza. Powinno się również używać pilota dyskretnie, by nie ułatwiać przestępcy wychwycenia momentu, w którym wykorzystuje się klucz.

ZAPAMIĘTAJ

Prawie wszystkie piloty, w których wykorzystuje się zmienny kod, stosują rozwiązanie KeeLog. Niestety, w 2007 roku udało się znaleźć sposób na ominięcie zabezpieczeń, w 2008 – całkowicie je złamano. W kolejnych latach doszło do wycieku kluczy typu master używanych do tworzenia kluczy w pilotach. Obecnie ten system uważa się za niezapewniający bezpieczeństwa.



Rys. 4.20. Pilot w wersji dwukanałowej, niżej – jego wnętrze, a po prawej – odbiornik (A – przyciski pilota, B – dioda sygnalizująca naciśnięcie przycisku, C – bateria 12 V, D – terminale połączeniowe, E – przekaźniki zapewniające pracę w trybie NO/NC dla każdego z kanałów, F – przycisk uczenia się pilota odpowiednio dla 1. i 2. kanału, G – diody sygnalizujące stan i pracę odbiornika, H – antena, I – mikroprzełącznik antysabotażowy)

Programowanie takich pilotów jest bardzo proste, polega na naciśnięciu wybranego przycisku, przytrzymaniu go i wciśnięciu programu pierwszego lub drugiego w zależności od tego, który kanał ten przycisk ma obsługiwać.

Każdy z kanałów może zapamiętać od kilku do kilkunastu pilotów.

Najczęstsze problemy związane z użytkowaniem pilotów to:

- zakłócenia elektromagnetyczne,
- wzajemne zakłócanie się pilotów,
- rozładowane baterie,
- metalowe przedmioty blisko odbiornika lub nadajnika ograniczające zasięg,
- uszkodzenia mechaniczne przycisków pilota.

Podczas przeglądu systemów, w których stosuje się piloty, należy skupić się na stanie technicznym pilotów oraz stanie zasilającej je baterii.

4.3.3. Biometria

Czytniki biometryczne uchodzą za najdoskonalszą formę identyfikacji osób uprawnionych. Niestety, jest to rozwiązanie najdroższe. Biometria opiera się na kilku technikach:

- skanowaniu oka,
- skanowaniu linii papilarnych,
- skanowaniu układu naczyń krwionośnych,
- skanowaniu twarzy.

Wszystkie systemy biometryczne muszą mieć czyste i nieuszkodzone sensory, dlatego nie stosuje się ich raczej w przestrzeniach publicznych, w których dodatkowym zagrożeniem jest wandalizm.

Sensory biometryczne występują wyłącznie w połączeniu z systemami mikroprocesorowymi analizującymi dane.

Za najdoskonalsze uznaje się **systemy skanujące układ naczyń krwionośnych**, ponieważ tego parametru nie można podrobić. Urządzenia sprawdzają także przepływ krwi w arteriach, więc człowiek, którego poddaje się badaniu, musi żyć. Zmniejsza to ryzyko przestępczych prób złamania zabezpieczenia. Do badania używa się kamery działającej w paśmie podczerwieni, więc nie jest wymagany bezpośredni kontakt czytnika z obiektem. Optymalna odległość skanowania wynosi od kilku do kilkunastu centymetrów, jednak niektóre rozwiązania umożliwiają uzyskanie dobrych wyników skanowania z odległości prawie metra. Skuteczność poprawnego rozpoznania przy jednorazowym skanowaniu przekracza 99%.

Podczas serwisowania systemów biometrycznych szczególny nacisk należy położyć na czystość i stan techniczny sensorów, gdyż to od nich zależy niezawodność systemu.

WARTO WIEDZIEĆ

Pasmo widma światła, wykorzystywane w systemach biometrycznych, pozwala na poprawne rozpoznanie układu żył, nawet gdy dłonie (ręce) są mocno zabrudzone. Nie ma również znaczenia ich temperatura lub to, że są mokre, np. od deszczu.

Najczęstsze problemy w systemach biometrycznych:

- zabrudzony obiektyw kamery,
- wadliwe działanie elektroniki,
- zakłócenia od silnych pól elektromagnetycznych.

Systemy oparte na zeskanowaniu **odcisku palca** są dość zawodne i podatne na manipulacje, nawet gdy mają sensor pulsu. Ponadto wymagają fizycznego kontaktu obiektu z czytnikiem, co prowadzi do szybszego zużywania się sensora lub brudzenia układu optycznego. Trudności z rozpoznaniem osoby pojawiają się także, gdy palec jest brudny lub mokry. Skuteczność systemów korzystających z rozpoznawania odcisku palca przy jednorazowym skanowaniu wynosi około 85%.

Najczęstsze problemy w systemach skanujących palec:

- uszkodzenie mechaniczne sensora,
- zabrudzenie sensora lub układu optycznego,
- zużycie się sensora,
- wadliwe działanie układu elektronicznego,
- zakłócenia elektromagnetyczne.

Rys. 4.21. Skaner naczyń krwionośnych

Systemy **skanujące oko** są dość popularne. Badają tęczówkę lub układ naczyń krwionośnych na dnie oka. O ile istnieją sposoby na oszukanie systemu opartego na analizie tęczówki, o tyle pozostałe systemy biometryczne są na razie w pełni bezpieczne. Proces skanowania jest szybki i bezbolesny, ale stwarza problemy u osób noszących okulary lub szkła kontaktowe. Również duże wady wzroku, w tym astygmatyzm, mogą zaburzać pracę systemów. Skuteczność przy jednorazowym skanowaniu wynosi ok. 95%, gdy skanowany obiekt nie ma wady wzroku lub jest ona niewielka.

Najczęstsze problemy w systemach skanujących oko:

- uszkodzenie mechaniczne sensora,
- zabrudzenie sensora lub układu optycznego,
- wadliwe działanie układu elektronicznego,
- zakłócenia elektromagnetyczne.

Systemy **skanowania twarzy** w kontroli dostępu są używane dość rzadko, częściej wykorzystuje się je w systemach CCTV do rozpoznawania osób. Jest to spowodowane dość niską skutecznością rozpoznawania twarzy, sięgającą 80–95%, gdyż pojawiają się np. problemy ze zidentyfikowaniem kobiet mających ostry makijaż. Takie systemy wymagają też dobrej jakości kamer o wysokiej rozdzielczości. Nie radzą sobie – w przeciwieństwie do wcześniej omówionych – z odróżnianiem np. bliźniąt.

Rys. 4.22. Skaner odcisku palca

Rys. 4.23. Skaner oka

Rys. 4.24. Skaner twarzy

Pozostałe systemy – oparte na próbkach głosu, sposobie naciskania klawiszy, poruszania się – są tak niszowe, że stanowią raczej ciekawostkę, niż dają możliwość praktycznego i niezawodnego wykorzystania.

4.3.4. Zwory i zaczepy

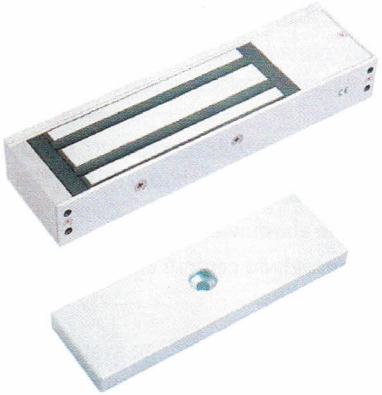
Ostatnim elementem systemów kontroli dostępu są urządzenia fizycznie sprawdzające możliwość dostępu do stref chronionych, czyli zamki i zwory. Najczęściej wykorzystują one **pole magnetyczne**, rzadziej – siłowniki elektryczne lub pneumatyczne.

Urządzenia tego typu można podzielić na takie, które zastępują istniejące zamki mechaniczne, uzupełniają je lub pracują jako niezależny system oprócz zamka mechanicznego.

Elektrozwory działają jak elektromagnes przyciągający do siebie metalową sztabę. Podczas poboru prądu rzędu kilkuset mA potrafią udźwignąć ciężar nawet kilkuset kilogramów. Niestety, po zaniku zasilania chronione drzwi zostają otwarte.

Najczęstsze problemy z elektrozworami:

- źle przylegająca sztaba zwory, przez co do otwarcia drzwi potrzeba dużo mniejszej siły;
- źle dobrana wielkość zwory (jej siły trzymającej).



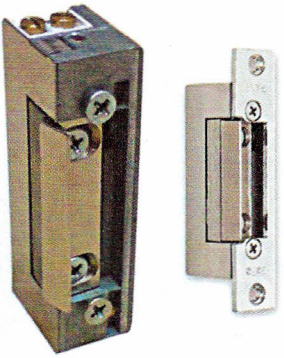
Rys. 4.25. Przykładowa elektrozwora

Elektrozaczep jest elementem współpracującym z zamkiem mechanicznym, konkretnie z „języczkiem" klamki. Umożliwia automatyczne zatrzaśnięcie się drzwi nawet przy braku zasilania.

Elektrozaczepy często stosuje się do kontroli dostępu, gdyż – w przeciwieństwie do elektrozwór – nie wpływają na wygląd drzwi i ościeżnic, są dyskretniejsze. Zapewniają bezpieczeństwo także przy braku zasilania.

Najczęstsze problemy z elektrozaczepami:

- przegrzewanie się cewek, zwłaszcza w drewnianych futrynach;
- brzęczenie spowodowane poluzowaniem się uzwojenia lub rdzenia;
- zła regulacja elementów mechanicznych.



Rys. 4.26. Przykładowy elektrozaczep

SPRAWDŹ SWOJĄ WIEDZĘ

1. Na co należy zwracać uwagę podczas konserwacji systemów kontroli dostępu?
2. Czy wszystkie systemy biometryczne zapewniają taki sam poziom bezpieczeństwa?
3. Jakie znasz elementy kontrolujące otwieranie drzwi?
4. Czy używanie pilotów do obsługi systemów kontroli dostępu jest w pełni bezpieczne?
5. Jakie są najczęściej spotykane problemy z systemami kontroli dostępu?