System perymetrycznej ochrony infrastruktury krytycznej

mgr inż. Stanisław Dziubak
Państwowy Instytut Badawczy

mgr inż. Paweł Gajewski
Państwowy Instytut Badawczy

dr inż. Andrzej Sobolewski
Polska Agencja Przemysłowo-Obronna

Zapewnienie bezpieczeństwa obiektom infrastruktury krytycznej wymaga oceny ryzyka wystąpienia zagrożenia oraz budowy zabezpieczeń fizycznych, które ewoluowały równolegle z postępem technicznym – od systemów ochrony obwodowej wokół zewnętrznych granic ochranianego obszaru po nowoczesne systemy dozoru perymetrycznego i powierzchniowego.

Infrastrukturę krytyczną stanowią zasoby państwa mające zasadnicze znaczenie dla funkcjonowania społeczeństwa i gospodarki. Można tu wyróżnić zasoby produkcji, transportu, dystrybucji energii i paliw, a przede wszystkim komunikacji elektronicznej stanowiącej nerw całej gospodarki i funkcjonowania państwa. Środki komunikacji elektronicznej to urządzenia teleinformatyczne wraz z magistralnymi, regionalnymi i dostępowymi sieciami światłowodowymi i radiowymi.

1. SIECI TELEINFORMATYCZNE JAKO ELEMENT INFRASTRUKTURY KRYTYCZNEJ

Sieci teleinformatyczne – telekomunikacyjne lub informatyczne (zwane dalej sieciami) – to w rzeczywistości różne elementy infrastruktury technicznej, takie jak:

- linie kablowe miedziane i światłowodowe,
- kanalizacja kablowa i studnie kablowe,
- szafy uliczne sieci dostępowych z zakończeniami kabli i urządzeniami aktywnymi,
- szafki i pomieszczenia techniczne w budynkach mieszkalnych, przemysłowych itp.,
- stacje bazowe sieci bezprzewodowych: LTE, LTE-A, 5G i inne.

Wymienione obiekty są rozmieszczone na całym obszarze pokrytym siecią. Dla linii kablowych, które są obiektami rozległymi, o długości sekcji w sieci światłowodowej do 100–120 km, a w sieci miedzianej dostępowej do ok. 10 km, wymagane jest zachowanie ciągłości torów transmisyjnych i utrzymanie ich parametrów w zakresie narzuconym przez współpracujące urządzenia aktywne. W razie uszkodzenia niezbędne jest szybkie jego wykrycie i lokalizacja. Dla pozostałych obiektów minimalny zestaw wymagań obejmuje:

- zachowanie fizycznej integralności obiektu,
- wykrywanie włamań i nieuprawnionych prac,
- wykrywanie sytuacji grożących przerwą w pracy lub uszkodzeniem, takich jak pożar, zalanie wodą, utrata zasilania i inne.

Zestaw ten może być uzupełniany o wymagania specyficzne dla danego rodzaju obiektu.
Oprócz firm telekomunikacyjnych w podobnej sytuacji są operatorzy lub właściciele infrastruktury energetycznej, kolejowej czy przemysłowej, mający obiekty bezobsługowe oraz związane z nimi sieci kablowe sygnalizacyjne, informatyczne i sterownicze.
Aktywne urządzenia sieciowe są wyposażone w funkcje nadzoru łączy. Mogą one wykryć uszkodzenie toru w linii kablowej, monitorując moc sygnału na wejściu odbiornika, lecz bez jego lokalizacji. Niestety, w przypadku wynajmowania przez właściciela infrastruktury kablowej par miedzianych i „ciemnych" włókien światłowodowych innym użytkownikom nie ma on dostępu do tych danych. W celu zachowania określonych przez umowy z klientami i regulatora parametrów jakości usług – zwykle dostępności (np. 99,99%) i czasu usunięcia uszkodzenia (np. 12 h) oraz sprawnego utrzymania infrastruktury – niezbędne jest ciągłe monitorowanie jej elementów przez dedykowany system autonomiczny.
Rozpatrując opłacalność ochrony, trzeba uwzględnić, że awarie sieci prowadzą często do zakłóceń i przerw w działaniu systemów ważnych dla gospodarki i bezpieczeństwa państwa lub firm, administracji, kolejowych, bankowych, kontroli ruchu lotniczego, policji, numerów alarmowych, przemysłu itd. Związane z tym straty pośrednie są nieporównanie wyższe od kosztów naprawy przeciętego kabla lub rozbitej szafy z aparaturą.

2. ZAGROŻENIA DLA INFRASTRUKTURY TELEKOMUNIKACYJNEJ

2.1. Uszkodzenia losowe i starzeniowe

Najczęściej spotykanymi przyczynami uszkodzeń infrastruktury kablowej są:

- roboty budowlane i drogowe, których skutkiem są przecięcia lub zgniecenia kabli oraz uszkodzenia kanalizacji i studni kablowych,
- kradzieże kabli i osprzętu, dewastacje, włamania, sabotaż,
- wypadki komunikacyjne powodujące uszkodzenia podpór linii napowietrznych i szaf ulicznych, uszkodzenia studni kablowych przez pojazdy,
- warunki zewnętrzne: wichury, szkody górnicze, osuwiska gruntu, oblodzenie, uszkodzenia linii napowietrznych przez złamane drzewa,
- błędy w trakcie prac przy utrzymaniu i eksploatacji sieci: przecięcia kabli, zwarcia przewodów, błędne przełączenia, nadmierne zginanie światłowodów,
- starzenie kabli i osprzętu pod wpływem zmian temperatury, wilgoci i wibracji,
- przegryzanie kabli przez szczury i inne zwierzęta.

Elementy sieci napowietrznych i szafy uliczne muszą sporadycznie wytrzymać temperaturę od –40°C zimą do 70°C latem, uwzględniając ich nagrzewanie wskutek nasłonecznienia. W ostatnim przypadku temperatura wewnątrz szafy z urządzeniami aktywnymi może przekroczyć 80°C, co prowadzi do niestabilności parametrów, szybkiego starzenia i awarii urządzeń. W temperaturze poniżej –25°C dochodzi natomiast do uszkodzenia akumulatorów ołowiowo-kwasowych (VRLA) używanych do zasilania rezerwowego wskutek zamarznięcia elektrolitu w rozładowanym akumulatorze.
Kable zewnętrzne i ich osprzęt pasywny lepiej znoszą działanie zmiennych temperatur i warunków atmosferycznych, ale możliwe są stopniowo postępujące uszkodzenia:

- wnikanie wilgoci i soli oraz korozja złączy wewnątrz osłon złączowych i szaf,
- uszkodzenia kabli z przewodami metalowymi przez wyładowania atmosferyczne,
- korozja i uszkodzenia mechaniczne uchwytów kabli napowietrznych,
- migracja żelu i włókien w kablach światłowodowych napowietrznych,
- kurczenie się tub w kablach światłowodowych po ekspozycji na wysoką temperaturę latem, obserwowane po spadku temperatury zimą poniżej np. –30°C; włókna ulegają silnym zgięciom wewnątrz skróconych tub lub wysuwają się z końca kabla w osłonie złączowej, a ich tłumienność wzrasta,
- luzowanie włókien wklejonych we wtykach złączy światłowodowych po degradacji kleju, połączone ze wzrostem strat i odbiciami promieniowania.

Awarie te są często wynikiem wadliwego montażu lub używania kabli i osprzętu niskiej jakości, względnie zaprojektowanych do pracy w odmiennych warunkach klimatycznych.

2.2. Uszkodzenia celowe

Dużym zagrożeniem dla infrastruktury sieci kablowych są celowe działania przestępcze wymienione poniżej:

- Wandalizm, dywersja i sabotaż. Przecięcie światłowodów w kilku punktach w celu zablokowania mechanizmów protekcji w sieci szkieletowej lub metropolitalnej to tani sposób na sparaliżowanie sieci obsługującej miasto, bank czy przedsiębiorstwo bez używania broni palnej lub materiałów wybuchowych. Danych o lokalizacji i funkcji kabli mogą dostarczyć byli pracownicy firm telekomunikacyjnych. W kraju notowano m.in. przecinanie kabli, by zniszczyć reputację konkurującego operatora w celu przejęcia klientów oraz w wyniku sporów o opłaty za przejście przez nieruchomości lub wynajem kanalizacji kablowej.
- Kradzieże kabli miedzianych w celu ich sprzedaży na złom, często połączone z uszkodzeniami studni kablowych oraz

przecinaniem rur kanalizacji i kabli światłowodowych. Te ostatnie nie mają wartości jako surowiec wtórny, przenoszą natomiast duży ruch i są pracochłonne w naprawie.
- Nielegalne korzystanie z kanalizacji kablowej – układanie kabli przez obce firmy bez zgody właściciela i opłat; możliwe jest uszkodzenie już istniejących kabli.
- Instalowanie odgałęzienia do przechwytywania danych, także ze światłowodów.

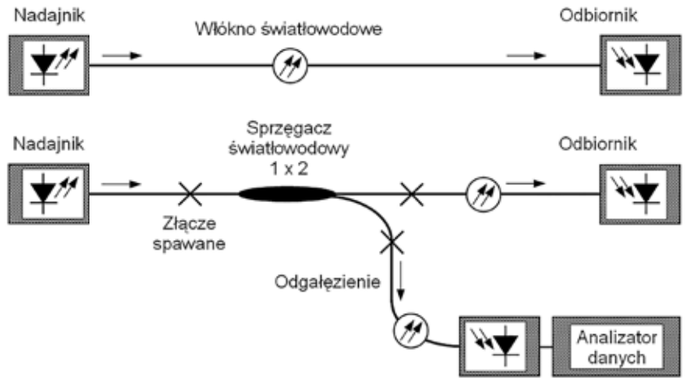
Instalacja odgałęzienia przez rozcięcie włókna światłowodowego i wstawienie pasywnego sprzęgacza odprowadzającego 1–20% sygnału *(rys. 1)* powoduje krótkotrwałą przerwę, a następnie trwały wzrost tłumienności, zwykle o 0,5–1,5 dB, stanowiący sumę strat sprzęgacza i dwóch złączy spawanych. Odgałęzienie umożliwia też zagłuszanie lub wprowadzenie fałszywych danych. Wspólny port sprzęgacza znajduje się wtedy od strony odbiornika atakowanego łącza. Przerwa włókna podczas montażu odgałęzienia trwa 2–4 min. To może uniemożliwić wykrycie tego zdarzenia przez system monitoringu wykonujący okresowe pomiary czynnego włókna za pomocą reflektometru impulsowego (*Optical Time Domain Reflectometer* – OTDR), najczęściej co 10–30 min.

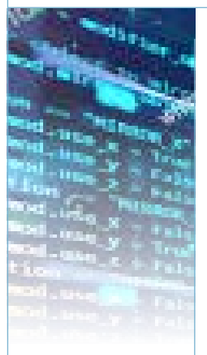
3. MONITORING INFRASTRUKTURY TELEINFORMATYCZNEJ

3.1. Monitoring infrastruktury sieciowej

Przecięcie kabla podczas robót ziemnych, sabotażu lub kradzieży powodu-

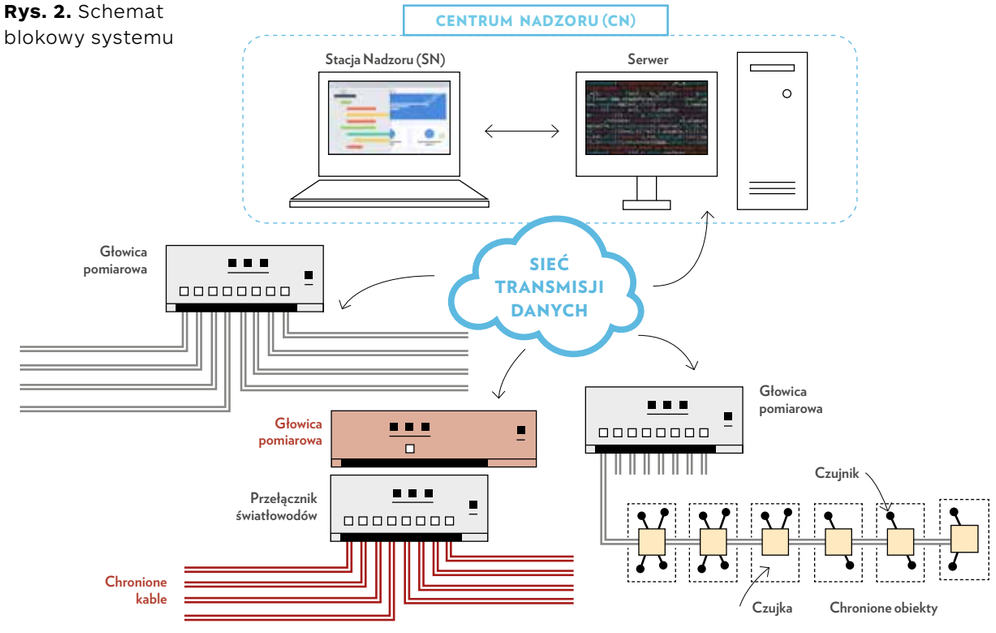
Rys. 1. Odgałęzienie sygnału ze światłowodu przez montaż sprzęgacza. Na górze – łącze w oryginalnej konfiguracji, na dole – łącze z odgałęzieniem





je natychmiast trwałą przerwę wszystkich par przewodów lub włókien światłowodowych. Podobnie jest w przypadku ponad 80% uszkodzeń losowych, stąd do wykrycia i lokalizacji uszkodzenia wystarcza nadzór wybranego włókna lub pary przewodów w linii kablowej.
Nielegalne układanie kabli wymaga wejścia do studni kablowych. Można je wykryć, monitorując włazy i drzwi w obiektach, nie ma natomiast zmian parametrów kabli. Również większość aktów sabotażu i kradzieży rozpoczyna się od włamania do studni kablowych bądź pomieszczeń lub szaf z osprzętem i aparaturą. Podstawową korzyścią z monitoringu po wykryciu i lokalizacji włamania, uszkodzenia lub sytuacji awaryjnej jest szybka reakcja przez interwencję ochrony oraz wysłanie serwisantów. Skuteczne zwalczanie wymienionych wcześniej zagrożeń wymaga scentralizowanego rozwiązania dla

Rys. 2. Schemat blokowy systemu

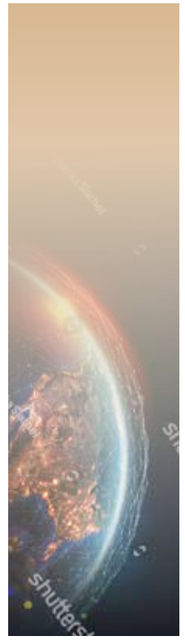


hermetyzacji i ochrony sieci kablowej obejmującego:
- kompletną, na bieżąco aktualizowaną ewidencję (tzw. paszportyzację) elementów sieci,
- fizyczne zabezpieczenia przed włamaniami: zamki, wzmocnione pokrywy studni itp.,
- system monitoringu wykrywający, sygnalizujący, lokalizujący i rejestrujący uszkodzenia elementów sieci, zmiany ich parametrów, włamania do studni i in.

System monitoringu infrastruktury telekomunikacyjnej (zwany dalej „systemem") autorstwa Instytutu Łączności pełni tę ostatnią funkcję. Może też zapewnić integrację wszystkich związanych z eksploatacją i utrzymaniem infrastruktury systemów innych producentów, w tym wymianę danych między systemami i zintegrowane centrum nadzoru. Rozwiązania takie mogą być tworzone według indywidualnych wymagań.

3.2. Funkcje systemu

Zakres funkcji systemu obejmuje:
- monitorowanie kabli z parami przewodów miedzianych,



- monitorowanie kabli światłowodowych z włóknami jednomodowymi,
- sygnalizację i lokalizację uszkodzeń kabli jw.,
- nadzór obiektów za pomocą czujników: otwarcia, pożaru, zalania wodą itp.,
- rejestrację zdarzeń w bazie danych i sygnalizowanie ich obsłudze centrum nadzoru,
- pokazywanie miejsca zdarzenia lub uszkodzenia na mapie,
- prezentację opisu obiektu lub linii kablowej oraz danych kontaktowych (serwisanci obsługujący dany obszar, agencje ochrony, posterunki policji lub innych służb),
- tworzenie raportów z danymi wybranymi według kryteriów wprowadzonych przez operatora (przedział dat, rodzaj obiektu, region, rodzaj zdarzenia),
- eksport wybranych danych.

Zakres funkcji systemu można dostosować do wymagań danego operatora lub użytkownika sieci i charakterystyki chronionej infrastruktury przez dobór lub zaprojektowanie nowych elementów sprzętowych i modułów oprogramowania.

3.3. Architektura systemu

Architekturę systemu przedstawiono na rys. 2. System składa się z komputera centrum nadzoru oraz dołączonych do niego różnego rodzaju głowic i czujek.
Miedziane linie kablowe są nadzorowane bezpośrednio przez głowice pomiarowe do kabli miedzianych, które mają 16 portów pomiarowych – jedna głowica może nadzorować do 16 kabli.

Linie światłowodowe są nadzorowane przez głowice pomiarowe do kabli światłowodowych zawierające reflektometr optyczny (OTDR). Głowica ma jeden port, do którego, za pomocą przełącznika światłowodów są sekwencyjnie dołączane pojedyncze włókna z każdego kabla światłowodowego. Mogą być nadzorowane zarówno włókna wolne, jak i wykorzystywane do transmisji (wymaga to montażu sprzęgaczy WDM na końcach linii).

System, nadzorując kable, wykonuje cyklicznie pomiary parametrów wolnej pary przewodów lub włókna w każdej linii kablowej i porównuje wyniki aktualne z wynikami wzorcowymi zapisanymi wcześniej po pomiarach sprawnego kabla. Zmiana parametrów przekraczająca ustalony zakres tolerancji powoduje alarm w centrum nadzoru i określenie miejsca uszkodzenia.
Monitorowane parametry obejmują:

- dla par przewodów miedzianych: rezystancję pętli przewodów i pojemność między przewodami oraz planowane dodanie charakterystyk reflektometrycznych
- dla włókien światłowodowych: charakterystyki reflektometryczne (amplituda echa w funkcji odległości od głowicy pomiarowej).

Maksymalne długości monitorowanych linii kablowych wynoszą typowo dla kabli miedzianych kilka kilometrów, a dla kabli światłowodowych do 100 km.

Studnie kablowe, szafy oraz inne obiekty w terenie są nadzorowane przez montowane w nich czujki. Stany czujek są odczytywane przez komputer w centrum nadzoru za pośrednictwem odpowiednich głowic, które także zasilają czujki przez kabel transmisyjny. Jedna głowica może obsługiwać do 7 linii z czujkami, a do każdej linii o długości kilku kilometrów można dołączyć do 30 czujek. Wszystkie czujki są co kilka sekund sprawdzane przez komputer centrum, dzięki czemu można szybko wykryć ewentualne uszkodzenia w systemie, zakłócenia transmisji itp.

Centralnym elementem systemu jest jego centrum nadzoru, które stanowi komputer z oprogramowaniem użytkowym oraz opcjonalne terminale.
Głowice pomiarowe do kabli miedzianych i światłowodowych oraz przełączniki światłowodów są dołączane poprzez Ethernet i protokół TCP/IP lub opcjonalnie inny interfejs np. RS-485. Oprogramowanie centrum nadzoru realizuje funkcje związane z:

- instalacją, konfigurowaniem i nadzorem pracy elementów sprzętowych systemu,
- wprowadzaniem danych i opisów chronionych elementów sieci,
- zbieraniem i przetwarzaniem danych pomiarowych,
- wykrywaniem, sygnalizacją i lokalizacją uszkodzeń, włamań i innych zdarzeń,
- utrzymywaniem bazy danych zdarzeń,
- tworzeniem raportów z danymi zdarzeń oraz ich eksportem,
- zarządzaniem użytkownikami system.

4. BEZPIECZEŃSTWO INFRASTRUKTURY INFORMATYCZNEJ

System opracowany przez Instytut Łączności stanowi odpowiedź na potrzeby perymetrycznej ochrony sieci teleinformatycznych, systemów istotnych dla bezpieczeństwa państwa, administracji, policji, kolei, lotnictwa, banków lub przedsiębiorstw przemysłowych, handlowych i usługowych. Ochrona zapewniona przez system umożliwia przede wszystkim:

- stały nadzór nad sieciami teleinformatycznymi miedzianymi i światłowodowymi,
- natychmiastową informację o miejscu i przyczynie zdarzenia (miejsce na mapie),
- powiadamianie nadzoru o zdarzeniu i uruchomienie działań naprawczych,
- raportowanie, statystyki, analizy.

Należy zwrócić uwagę, że nawet proste uszkodzenie sieci może pośrednio wpływać na funkcjonowanie obiektów infrastruktury krytycznej i generować wielokrotnie większe koszty od inwestycji w system monitoringu infrastruktury telekomunikacyjnej.