Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 66

LI Międzyuczelniana Konferencja Metrologów

MKM 2019

Opole - Moszna, 23-25 września 2019

doi: 10.32016/1.66.11

BEZPIECZEŃSTWO PRZYRZĄDÓW POMIAROWYCH – TRANSMISJA DANYCH

Michał MOSIĄDZ, Janusz SOBIECH, Jacek WÓJCIK

Główny Urząd Miar, Zakład Metrologii Interdyscyplinarnej (ZMI)
tel.: +48 22 681 93 93 e-mail: zmi@gum.gov.pl

Streszczenie: Zabezpieczenie transmisji danych urządzeń pomiarowych jest ważnym obszarem bezpieczeństwa cyfrowego determinującym rzetelność pomiaru. Metody ochrony takie jak ograniczenie dostępu do zasobów systemu, czy techniki uwierzytelnienia i kodowania informacji utrzymują ryzyko transmisji cyfrowej w akceptowalnych granicach. Jednakże w praktyce wciąż wykrywane są elementarne luki zabezpieczeń sieciowych w przyrządach pomiarowych. Temat zabezpieczeń transmisji danych w rozwiązaniach metrologicznych jest więc aktualny. W nowych urządzeniach wprowadzanych na rynek, przesyłanie wyników pomiarów jest pożądaną funkcjonalnością. W entuzjazmie korzystania z dostępu online nie można zapomnieć o testowaniu bezpieczeństwa, badaniach oraz kontroli. Na straży wiarygodności pomiaru, poza rozwiązaniami informatycznymi, stoją regulacje prawne, normy oraz wytyczne organizacji metrologicznych. Zawarte w nich wymogi i zalecenia opisują metodykę testów wyszczególniając ochronę transmisji danych w przyrządach pomiarowych.

Słowa kluczowe: przyrządy pomiarowe, transmisja danych, bezpieczeństwo informacyjne, testy bezpieczeństwa.

1. WSTĘP

Współczesne przyrządy pomiarowe podlegające prawnej kontroli metrologicznej mają być zgodne z wymogami m.in. bezpieczeństwa cyfrowego. Dotyczy to również urządzeń wykorzystywanych w laboratoriach pomiarowych stosujących normy jakości (np. ISO 17025) [1]. Zastosowanie technik informatycznych, sieci komputerowych i różnych kanałów przesyłania danych wymusza potrzebę zabezpieczenia transmisji danych urządzeń pomiarowych i zapewnienia rzetelności pomiaru. Włamania do sieci i systemów teleinformatycznych mogą zachwiać zaufanie do wiarygodności wyników pomiarów. Dlatego należy mieć na uwadze czy użyte rozwiązania w przyrządach pomiarowych faktycznie zabezpieczają przesyłane wyniki pomiarów? Jak zapewniono weryfikację niezmienności przesyłanych informacji oraz jak zabezpieczono dostęp do systemu oraz zebranych danych?

Występujące ryzyka definiowane są głównie jako nieuprawniony dostęp do danych, przejęcie kontroli nad układem pomiarowym, fałszowanie i utratę danych. Koniecznością są wiec środki ochrony takie jak ograniczenia dostępu do zasobów systemu (np. odpowiednia konstrukcja urządzenia, stosowanie polityki bezpieczeństwa) oraz techniki uwierzytelnienia i kodowania informacji.

Ochrona transmisji danych metrologicznych jest uwzględniana w wymaganiach prawnych, które warunkują dopuszczanie przyrządów do użytkowania. Przykładowo dla urządzeń do pomiaru prędkości pojazdów w ruchu drogowym stwierdzono: „Zarejestrowane dane, jeśli są transmitowane powinny zawierać dodatkowo sumy kontrolne lub pieczęcie elektroniczne i mogą zawierać dodatkowo podpisy elektroniczne osób dokonujących pomiaru, umożliwiające potwierdzenie przez przyrząd i przez oprogramowanie zewnętrzne współpracujące z przyrządem niezmienności tych danych po ich transmisji do systemów ogólnodostępnych.” [2].

Podobnie w innych wytycznych i normach dotyczących sprzętu pomiarowego zawierającego oprogramowanie, wiele uwagi poświęcono połączeniom między elementami układu pomiarowego i bezpieczeństwu transmisji danych. Zapisy dokumentów OIML D31 2008 [3], WELMEC 7.2 Software Guide [4] przedstawiają zagadnienia transmisji danych pomiarowych i zabezpieczeń kryptograficznych. Również norma ISO 17025 odnosząc się do zarządzania informacjami laboratoryjnymi (7.11.3) zwraca uwagę na ochronę danych przed nieuprawnionym dostępem (manipulacją i usunięciem) oraz na integralność informacji [1]. W szczególności wyróżnia przesyłanie danych w laboratorium z używanych komputerów oraz urządzeń pomiarowych przez sieć teleinformatyczną (LAN, Wi-Fi).

Pomimo że techniki zabezpieczeń transmisji danych są powszechnie znane i stosowane w urządzeniach sieciowych nie związanych z metrologią – w praktyce okazuje się, że cześć przyrządów pomiarowych przed wprowadzeniem ich na rynek w trakcie badań wykazuje niepokojące podatności informatyczne i luki bezpieczeństwa. Spotykane jest w nich korzystanie z nieszyfrowanych protokołów, jak FTP, HTTP, czy używanie aplikacji sieciowych bez ochrony systemem kont i haseł. Rosnąca konkurencja na rynku sprawia, że niektórzy dostawcy urządzeń pomiarowych działając w pośpiechu, jakby zapominają o zabezpieczeniu swych urządzeń przed atakami z sieci. Przedstawiane do badań oprogramowania przyrządy pomiarowe, niemal na ostatnim etapie przed wprowadzeniem ich do użytkowania, muszą być poprawiane, gdyż nie zapewniają ochrony sieciowej zgodnej z obowiązującymi przepisami, zaleceniami metrologicznymi, czy nawet wytycznymi bezpieczeństwa informatycznego, pomimo że są one bieżąco publikowane i najczęściej ogólnie dostępne.

2. OCHRONA URZĄDZEŃ PRACUJĄCYCH W SIECI

Ochrona przyrządów pomiarowych pracujących w sieci korzysta z zasad ochrony innych urządzeń informatycznych

i dotyczy trzech obszarów: kontroli dostępu, uwierzytelniania (authentication) i kodowania (szyfrowania) informacji. Wymienione płaszczyzny stanowią bazę nie tylko rozwiązań technicznych transmisji danych, ale też dla konstruowanych wymogów prawnej kontroli metrologicznej, od których zależy dopuszczenie przyrządów do obrotu i użytkowania.

2.1. Kontrola dostępu

Pod względem samej informatyki, kontrola dostępu ma zapewniać ochronę danych przed nieuprawnionymi użytkownikami i polega na zabezpieczeniu dostępu do systemu teleinformatycznego. W tym celu nakładane są ograniczenia na poszczególne warstwy urządzeń, zasobów i systemów. Ochrona jest realizowana dwutorowo, przez poziomy kontroli dostępu w systemie operacyjnym oraz zabezpieczenia sprzętowe. W systemach rozproszonych, wymieniających informacje metrologiczne poprzez otwarte i zamknięte sieci transmisyjne (zob. [4]) ochronę wspiera ustalona polityka bezpieczeństwa, zarządzanie uprawnieniami, kontami użytkowników, a także sieciowe zapory ogniowe, odpowiednia konfiguracja routerów oraz ochrona antywirusowa [5].

W przyrządach pomiarowych kontrola dostępu winna chronić oprogramowanie urządzenia, jego parametry konfiguracyjne oraz dane pomiarowe przed dostępem poprzez interfejsy komunikacyjne oraz przed fizycznym dostępem do wewnętrznych elementów przyrządu.

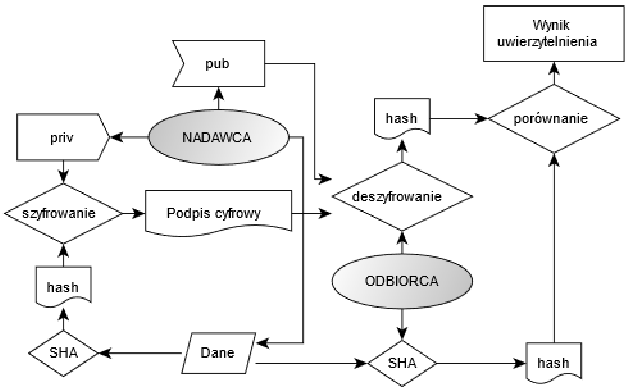
2.2. Uwierzytelnianie

Obszar uwierzytelniania wynika z potrzeby weryfikacji autentyczności obiektów zawierających dane w sieci. Wiadomo, że autentyczność kogokolwiek lub czegokolwiek w sieci nie może być z góry gwarantowana. Niespodziewane incydenty bezpieczeństwa wzmagają potrzebę kontroli, audytów bezpieczeństwa i zwykłego przypominania o ciągłym ryzyku, że pojawiający się w sieci użytkownicy, wiadomości, dokumenty, oprogramowanie, serwery, czy inne elementy nie zawsze muszą być tymi, za jakie się podają. Mechanizmy uwierzytelniania pozwalają potwierdzać niezmienność danych (plików, wiadomości) wytworzonych przez dane źródło wraz z jego autentycznością.

Często stosowanym mechanizmem uwierzytelniania są techniki podpisu cyfrowego oparte na kryptografii [6]. Podpis cyfrowy wymaga od nadawcy wygenerowania pary kluczy publicznego i prywatnego oraz dostarczenia odbiorcy swego klucza publicznego. Następnie nadawca za pomocą odpowiedniej funkcji tworzy skrót (hash) z danych, które zamierza przesłać i generuje podpis (digital signature) poprzez zaszyfrowanie utworzonego hasha swoim kluczem prywatnym, zgodnie z tym jak przedstawiono na rysunku 1. Otrzymany wynik jest właściwym podpisem elektronicznym, który nadawca przekazuje odbiorcy wraz z danymi, których użył do wygenerowania podpisu.

Odbiorca chcąc zweryfikować nadawcę oraz otrzymane dane, najpierw odszyfrowuje podpis cyfrowy korzystając z klucza publicznego nadawcy, uzyskując pierwszy hash. Następnie z otrzymanych danych odbiorca tworzy drugi hash i porównuje go z pierwszym odszyfrowanym hash'em. Ich zgodność gwarantuje autentyczność (authentication), niezaprzeczalność (non-repudiation) oraz integralność (integrity) danych.

Podpis cyfrowy poręcza, że nikt nie „podszyje" się pod nadawcę, bo tylko on dysponuje prywatnym kluczem nadawcy. Z kolei nadawca nie może zaprzeczyć, że wysłane dane pochodzą od niego, gdyż tylko on zna klucz prywatny, którym posłużył się do podpisania danych. Dane nie mogły zostać też zmienione (np. przez niepowołane osoby), gdyż ich modyfikacja spowodowałaby zmianę wyliczonego przez odbiorcę hash'a oraz jego niezgodność z hash'em zawartym w podpisie elektronicznym nadawcy [5].



Rys 1. Uwierzytelnianie przesyłanych danych

Należy zwrócić uwagę, że o stopniu bezpieczeństwa podpisu, wykorzystywanego m.in. przy przesyłaniu danych pomiarowych, decyduje prawidłowe stosowanie kryptografii klucza publicznego. Ważna jest ochrona i nieudostępnianie klucza prywatnego wraz z wiarygodnym rozpowszechnianiem kluczy publicznych. Klucze powinny być dostępne jako certyfikaty wydawane przez zaufaną instytucję CA (Certification Authority), która zajmując się ich dystrybucją dba o weryfikację danych przynależnych do użytkownika [6]. Urządzenia pomiarowe z uwierzytelnianiem powinny być zabezpieczone przed możliwością skopiowania klucza prywatnego z przyrządu lub jego podmiany. Skuteczność ochrony danych pomiarowych podczas transmisji przed ich przekłamaniem lub zmianą zależy od zachowania prawidłowych zasad uwierzytelniania.

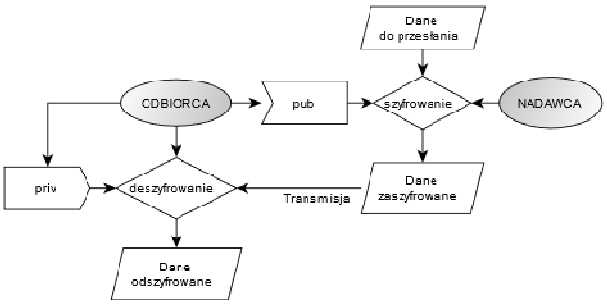
2.3. Kodowanie (szyfrowanie) informacji

Celem szyfrowania informacji jest umożliwienie jedynie upoważnionego odczytu danych i ograniczenie do nich dostępu. W obszarze tym, tak jak przy uwierzytelnianiu, stosuje się podobne standardy i rozwiązania kryptograficzne wraz z algorytmami szyfrowania blokowego i strumieniowego [5, 6]. Różnica polega na tym, że dane nie są przesyłane jawnie, ale wcześniej są zakodowane i w ukrytej formie są albo przechowywane są na nośnikach danych, albo przekazywane dalej podczas transmisji na odległość.

Przy przesyłaniu danych pomiarowych wymagany poziom zabezpieczeń uzyskuje się przez szyfrowanie asymetryczne, gdzie istotą jest stosowanie par kluczy: prywatnego i publicznego pamiętając, jak przy uwierzytelnianiu, o należytej ochronie i wiarygodnej dystrybucji kluczy. Dane przed przesłaniem są szyfrowane kluczem publicznym odbiorcy, co przedstawiono na ryunku 2. Dostęp do informacji po ich dostarczeniu jest możliwy wyłącznie z użyciem klucza prywatnego.

Kodowanie informacji ma szczególne zastosowanie również przy szyfrowaniu samego kanału w transmisji danych. Chociaż teoretycznie może ono być realizowane na dowolnej warstwie protokołów modelu komunikacyjnego OSI, to praktycznie najczęściej kodowanie odbywa się albo w warstwie fizycznej na poziomie łącza transmisyjnego, albo na warstwach najwyższych w węzłach końcowych. Zaletą szyfrowania w warstwie fizycznej, na poziomie połączeń, jest szybkość i prosta obsługa, bo szyfrowane są

wszystkie przesyłane dane. Jednak w takim rozwiązaniu zabezpieczone informacje są narażone na ujawnienie w każdym z węzłów pośredniczących, gdyż przed kolejnym przesłaniem muszą zostać odkodowane i zaszyfrowane ponownie do dalszej transmisji. Wady tej nie mają metody szyfrowania w węzłach końcowych, ponieważ transmitowane dane pozostają zaszyfrowane podczas całej drogi i zostają rozkodowane dopiero, gdy osiągną miejsce przeznaczenia. Problemem w tej metodzie jest jednak potencjalna możliwość śledzenia drogi pakietów i określania punktów krańcowych połączenia, a także podatność na analizę ruchu w sieci [6]. Systemy mające zapewnić większe bezpieczeństwo wymagają więc zastosowania obu tych metod łączenie, co eliminuje opisane wady.



Rys 2. Kodowanie (szyfrowanie) informacji

Transmisję danych w przyrządach pomiarowych, podobnie jak w innych urządzeniach, zabezpiecza się przez przez wybór i stosowanie odpowiednich, szyfrowanych protokołów komunikacyjnych, np. protokołu SSL, który jest rozwiązaniem kryptograficznym odrębnym od aplikacji [7]. Zapewnia on, poza uwierzytelnieniem serwera, również autoryzację klienta oraz szyfrowanie przesyłanych danych. Dobór zastosowanych metod zależy od poziomu bezpieczeństwa ochrony danych pomiarowych przed dostępem osób nieupoważnionych.

3. BADANIA BEZPIECZEŃSTWA TRANSMISJI DANYCH W PRZYRZĄDACH POMIAROWYCH

Badania przyrządów pomiarowych pod względem bezpieczeństwa transmisji danych oparto na przepisach określających wymagania dla danej grupy typów przyrządów. Uwzględnia się też wytyczne, zalecenia i normy organizacji oraz instytucji metrologicznych jak: OIML, WELMEC, PKN, ISO i liczne standardy dla bezpiecznych systemów w IT, np. BS 7799, CIS, NIST, COBIT, ITIL.

3.1. Metodyka badań

Badanie zabezpieczeń transmisji danych można oprzeć na metodach testów akceptacyjnych i bezpieczeństwa oprogramowania. Adaptacja takiej metodyki została wdrożona w Pracowni Badań Oprogramowania ZMI Głównego Urzędu Miar (GUM) przyczyniając się do rozwoju i modernizacji regulacji w zakresie certyfikacji przyrządów pomiarowych, w tym wytycznych dotyczących transmisji danych. Przykładem mogą być zmiany w przepisach dotyczących przyrządów do pomiaru prędkości pojazdów w ruchu drogowym [2] oraz współudział w aktualizacji przewodnika WELMEC WG7.2. Obszary badań bezpieczeństwa: oprogramowania, przechowywania i transmisji danych, wskazane w przewodniku WELEMC WG 7.2 [4] stosowane są w GUM w zakresie oceny zgodności przyrządów pomiarowych z dyrektywą MID i adoptowane do krajowych przepisów, które dotyczą poszczególnych rodzajów przyrządów pomiarowych podlegających ocenie zgodności.

Współczesne układy pomiarowe mają zwykle konstrukcję modułową, w której między elementami przesyłane są sygnały sterujące, parametry etapów procedury pomiarowej, cząstkowe wyniki pomiarowe. Ostateczny wynik pomiaru jest eksportowany do zewnętrznych systemów przetwarzania i przechowywania danych. W pierwszym etapie badań należy zdefiniować zakres i obszary wymaganej ochrony uwzględniając ocenę istotności przesyłanych danych dla bezpieczeństwa i wiarygodności wyników pomiaru. Zazwyczaj w systemach metrologicznych zabezpieczenia kryptograficzne i logiczne uzupełniane są przez tradycyjne mechaniczne ograniczenia dostępu. Zabezpieczenia przed dostępem do konstrukcji wewnętrznej przyrządu przez system plomb eliminują konieczność zabezpieczeń transmisji danych pomiędzy ich podzespołami zamkniętymi we wspólnej obudowie. Weryfikacji na poziomie badań funkcjonalnych (czarnoskrzynkowych) wymagają zaimplementowane wewnątrz przyrządu mechanizmy wykrywania błędów transmisji przed przekłamaniami i zakłóceniami.

W przypadku sygnałów przepływających poza zabezpieczoną przed dostępem częścią układu pomiarowego, pozostają kwestie związane z autentycznością i poufnością danych, a także uwierzytelniania dostępu. Należy skontrolować prawidłową implementację i działanie mechanizmów uwierzytelniania i szyfrowania danych.

Problematykę badań komplikuje różnorodność stosowanych kanałów transmisji danych. W literaturze [4] zastosowano szerszą ich klasyfikację, pod względem różnych cech: sieci otwarte (ogólnodostępne) i zamknięte, interfejsy przewodowe i bezprzewodowe itp.

Wśród najpowszechniej stosowanych w przyrządach pomiarowych interfejsów komunikacyjnych, możemy wyróżnić komunikację via Internet, zarówno przez przewodowe medium transmisji (przewód miedziany bądź światłowód) oraz bezprzewodowe (Wi-Fi), komunikację lokalną w standardzie BT, IR, USB, RS-232. Wszystkie wymienione rodzaje kanałów transmisji danych wymagają innych stopni ochrony, posiadają wbudowane różne metody zabezpieczeń (BT, kanał SSL i VPN, bity parzystości, SHA). W badaniach należy uwzględnić wszystkie zewnętrzne porty i protokoły przyrządu oraz możliwe dostępy bezprzewodowe i kanały zdalnego sterowania przyrządem.

3.2. Obszary regulacji oraz badań

Regulacje w przepisach prawa oraz zalecenia zabezpieczeń przyrządów pomiarowych, w szczególności WELMEC 7.2 Software Guide [4], podają wymagania dotyczące bezpieczeństwa przesyłania danych w urządzeniach pomiarowych, będąc jednocześnie wskazaniami dla testowania tego typu przyrządów. Zawierają zidentyfikowane ryzyka, a także wytyczne dotyczące poziomu akceptacji rozwiązań oraz używanych metod badań (analiza dokumentacji, testy funkcjonalne, testy strukturalne, analiza kodu źródłowego itp.).

W zakresie kompetencji badacza jest weryfikacja poziomu i istotności ww. ryzyk w przewidywanym zastosowaniu przyrządu pomiarowego i dobór metod badań, celem sprawdzenia akceptowalnego poziomu bezpieczeństwa przyrządu pomiarowego.

W obszarze badań bezpieczeństwa transmisji danych dokument WELMEC wyszczególnia następujące zakresy

wymagań: (T1) Kompletność transmitowanych danych. (T2) Ochrona przed przypadkowymi i nieumyślnymi zmianami. (T3) Integralność danych. (T4) Autentyczność przesyłanych danych. (T5) Poufność kluczy i danych. (T6) Obsługa uszkodzonych danych. (T7) Opóźnienie transmisji. (T8) Dostępność usług transmisji.

Wymagania kompletności transmitowanych danych (T1) dbają aby przesyłane dane zawierały wszystkie istotne informacje niezbędne do prezentacji i późniejszego przetwarzania wyników w jednostce docelowej.

Konieczna jest też ochrona przed możliwymi zmianami przesyłanych danych (T2). Urządzenie pomiarowe powinno chronić dane pomiarowe przed nieumyślną zmianą lub ich usunięciem, a oprogramowanie powinno wykrywać możliwe przekłamania transmisji.

Przesyłając informacje metrologiczne w sieci należy zapewnić ich integralność (T3) oraz autentyczność (T4). Wyniki pomiarów powinny być chronione metodami uwierzytelniania danych przed możliwością dokonywania celowych zmian.

Należy także uwzględniać poziom ryzyka, który jest wyższy jeśli urządzenie pracuje w sieci otwartej. Przyrządy narażone na pracę w podwyższonej klasie ryzyka powinny być odporne na próby włamań przeprowadzane nawet za pomocą specjalistycznych narzędzi informatycznych. Gdy ryzyko jest minimalne, wystarcza zastosowanie prostszej ochrony przed celowymi zmianami i falsyfikacją danych.

Przesyłane dane pomiarowe w sieci powinny zawsze być chronione. Dlatego przyrządy pomiarowe wykorzystujące transmisję muszą być wyposażone w mechanizmy weryfikacji autentyczności przesyłanych informacji oraz umożliwiać przypisanie wartości pomiarowych do określonego pomiaru.

W zależności od klasy ryzyka należy zapewnić odpowiednią ochronę i poufność kluczy kryptograficznych oraz szyfrowanie danych i wyników pomiarów (T5).

Zalecenia WELMEC podają, że przyrządy pomiarowe mają uniemożliwiać przetwarzanie uszkodzonych danych powstałych w wyniku błędów transmisji (T6). Użytkownik nie powinien otrzymywać uszkodzonych, mylnych wyników pomiaru. Urządzenie winno prezentować jasny komunikat o wystąpieniu błędu transmisji i uszkodzeniu danych.

Również opóźnienie lub zerwanie transmisji (T7) nie może wpływać na pomiar i jego wyniki.

Należy zapewnić odporność na zanik dostępu do sieci komunikacyjnej (T8), zebrane dane pomiarowe muszą być przechowane do czasu przywrócenia łączności, a potem zostać przesłane do zamierzonego punktu docelowego.

4. PODSUMOWANIE

Szerokie zastosowanie technik przesyłania danych wprowadza nieznane wcześniej zagrożenia bezpieczeństwa przyrządów pomiarowych. W celu zmniejszenia ryzyka uzyskania nieupoważnionego dostępu i zmiany transmitowanych danych stosuje się szereg środków ochrony polegających na ograniczeniu dostępu do zasobów systemu urządzenia pomiarowego, uwierzytelnieniu danych oraz kodowaniu informacji za pomocą metod kryptograficznych. Przyrządy pomiarowe wyposażone w dostępne dla użytkownika interfejsy komunikacyjne powinny być badane pod względem zabezpieczeń transmisji danych pomiarowych i weryfikacji przesyłanych informacji. Regulacje w przepisach prawa oraz wytyczne dla przyrządów pomiarowych podają szczegółowe wymogi i zalecenia odnośnie wykorzystywania cyfrowego przesyłania danych i są wskazaniami dla testowania tego typu przyrządów. Obowiązujące wytyczne oraz metodyka badań powinny być aktualizowane ze względu na rozwój i stosowanie nowoczesnych technologii w przyrządach pomiarowych.

5. BIBLIOGRAFIA

1. Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących, PN-EN ISO/IEC 17025: 2018-02.
2. Rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 10 stycznia 2019 r. zmieniające rozporządzenie w sprawie wymagań, którym powinny odpowiadać przyrządy do pomiaru prędkości pojazdów w ruchu drogowym, oraz szczegółowego zakresu badań i sprawdzeń wykonywanych podczas prawnej kontroli metrologicznej tych przyrządów pomiarowych (Dz.U. 2019 poz. 151), § 1 pkt. 8 lit. c.
3. General requirements for software controlled measuring instruments, OIML D 31, 2008 (E).
4. WELMEC 7.2, 2018: Software Guide (Measuring Instruments Directive 2014/32/EU), European Cooperation in Legal Metrology.
5. Anderson R.: Inżynieria zabezpieczeń,, Wyd. Naukowo-Techniczne, Warszawa 2005, s. 59–134, 437–464.
6. Schneier B.: Kryptografia dla praktyków: Protokoły, algorytmy i programy źródłowe w języku C, Wyd. Naukowo-Techniczne, Warszawa 2002.
7. Stokłosa J., Bliński T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych, Wyd. Naukowe PWN, Warszawa 2001, s. 354–355.

SAFETY OF MEASURING INSTRUMENTS – DATA TRANSMISSION

Securing data transmission in measuring instruments is the important area of digital security, which determines the reliability of measurement. Methods of protection such as limited access to system resources or the use of authentication and information encoding techniques keep the risk of digital transmission in acceptable limits. However, in practice elementary security gaps are still detected in measuring instruments. The subject of securing data transmission is up-to-date in metrological solutions. In new devices placed on the market, sending measurement results is a desired functionality. In enthusiasm over using online access, we cannot forget about testing security, researches and control. IT solutions, legal regulations, standards and guidelines of metrological organizations uphold the reliability of measurement. Requirements and recommendations contained in them, describe the methodology of tests, specifying the protection of data transmission in measuring instruments.

Keywords: measuring instruments, data transmission, IT security, security tests.