Bezpieczeństwo cyfrowe a rzetelność pomiaru

Digital security and measurement reliability

Michał Mosiądz, Janusz Sobiech, Jacek Wójcik (Główny Urząd Miar)

Zadaniem metrologii jest zapewnienie wiarygodności pomiarów. Nowoczesne przyrządy pomiarowe używają oprogramowania sterującego. Oprogramowanie ma wpływ na rzetelność i jakość pomiaru. Ryzyko obniżenia wiarygodności pomiarów powoduje konieczność stosowania zasad bezpieczeństwa cyfrowego w metrologii. Wytyczne dotyczące przyrządów pomiarowych powinny uwzględniać te zasady.

The goal of metrology is to ensure the reliability of measurements. Modern measuring instruments use control software. The software affects the reliability and quality of measurement. The risk of lowering the reliability of measurements requires the use of digital security principles in metrology. Guidelines for measuring instruments should include these principles.

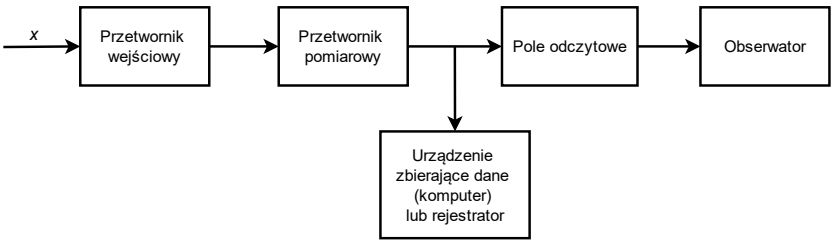
Wstęp

Wszystkie przyrządy pomiarowe, niezależnie od sposobu ich konstrukcji i zastosowanych technologii, muszą zapewnić wiarygodność pomiaru. Znajduje to odzwierciedlenie w budowie i wykonaniu przyrządu, który ma z zamierzoną dokładnością zapewnić wskazanie wartości wielkości fizycznej, która została zmierzona. Przyrząd, gwarantując akceptowalną zgodność kolejnych wyników pomiaru w tych samych oraz zmienionych warunkach pomiarowych, poza wynikiem pomiaru, powinien również miarodajnie rejestrować inne dane pozwalające na identyfikację procedury pomiarowej, poprzez wskazanie m.in. czasu, miejsca, egzemplarza przyrządu bądź układu pomiarowego, osoby mierzącej.

Celem artykułu jest przedstawienie problematyki, związanej z wpływem rozwiązań informatycznych (w szczególności szeroko rozumianego oprogramowania) na rzetelność pomiaru w przyrządach i systemach pomiarowych. Począwszy od przedstawienia wpływu oprogramowania na środowisko i proces pomiarowy, autorzy pokazują problem wiarygodności pomiaru w związku z trudnością rzetelnego oszacowania poziomu ryzyka cyfrowego. W artykule zostaną pokrótce przedstawione wypracowane metody szacowania ryzyka informacyjnego oraz standardy bezpieczeństwa cyfrowego, ze szczególnym uwzględnieniem wytycznych, dotyczących przyrządów pomiarowych, w których zastosowano rozwiązania teleinformatyczne. W końcowej części przedstawiono ogólnie nowe tendencje wykorzystania nowoczesnej informatyki w metrologii.

Oprogramowanie w urządzeniach pomiarowych

Na kluczową rolę oprogramowania w komputerowych systemach pomiarowych zwracano już uwagę w latach 90., kiedy to opisywano rozwój metrologii. Zastosowanie informatyki w metrologii ukazywano wtedy jako odrębną fazę rozwoju, która nastąpiła po okresie stosowania metod pomiarowych, opartych na bezpośrednim porównaniu i korzystaniu z mierników mechanicznych, elektromechanicznych oraz po etapie rozwoju przyrządów elektronicznych. Zastosowanie czujników elektrycznych oraz przetworników analogowo-cyfrowych do pomiarów wielkości elektrycznych i nieelektrycznych umożliwiło późniejszą cyfryzację pomiarów. Opisując fazę wprowadzenia informatyki do metrologii stwierdzono: *Umożliwiło to włączenie do pomiaru praktycznie dowolnie skomplikowanych operacji obliczeniowych oraz automatyczne sterowanie pomiarem;* […] *Komputerowy system pomiarowy może bowiem spełnić wiele złożonych funkcji związanych zarówno z przetwarzaniem informacji pomiarowej, jak i z obsługą obiektu pomiaru – z jednej strony – oraz odbiorcy wyników pomiaru – z drugiej* [1]. Przedstawiając możliwości, jakie daje zastosowanie technologii informatycznych w metrologii, w następujący sposób zwracano uwagę na znaczenie oprogramowania: *O jego [komputerowego systemu pomiarowego] możliwościach w coraz większym stopniu decyduje oprogramowanie (software), w mniejszym zaś – konstrukcja (hardware). Opisane przemiany w dziedzinie instrumentacji umożliwiły podjęcie przez metrologię nowych zadań.* […] *Pojawiła się potrzeba równoczesnego mierzenia wielu współzależnych wielkości opisujących obiekty i zjawiska*



Rys. 1. Dawny schemat funkcjonalny przyrządu pomiarowego

fizyczne. Pomiar wyszedł poza ramy inżynierii, nauk ścisłych i wymiany towarów. Pomiary zaczęto wykorzystywać do celów nietechnicznych (przykładem: złożone pomiary w medycynie). […] Rewolucja komputerowa w metrologii […] co prawda zmniejszyła różnorodność stosowanych rozwiązań konstrukcyjnych, ale w jej miejsce wprowadziła nieporównywalnie większą rozmaitość oprogramowania [1].

Opisywane przemiany wynikają również z dynamicznego rozwoju metrologii ogólnej, która dawniej nazywana miernictwem, stała się interdyscyplinarną dziedziną nauki [1, 2].

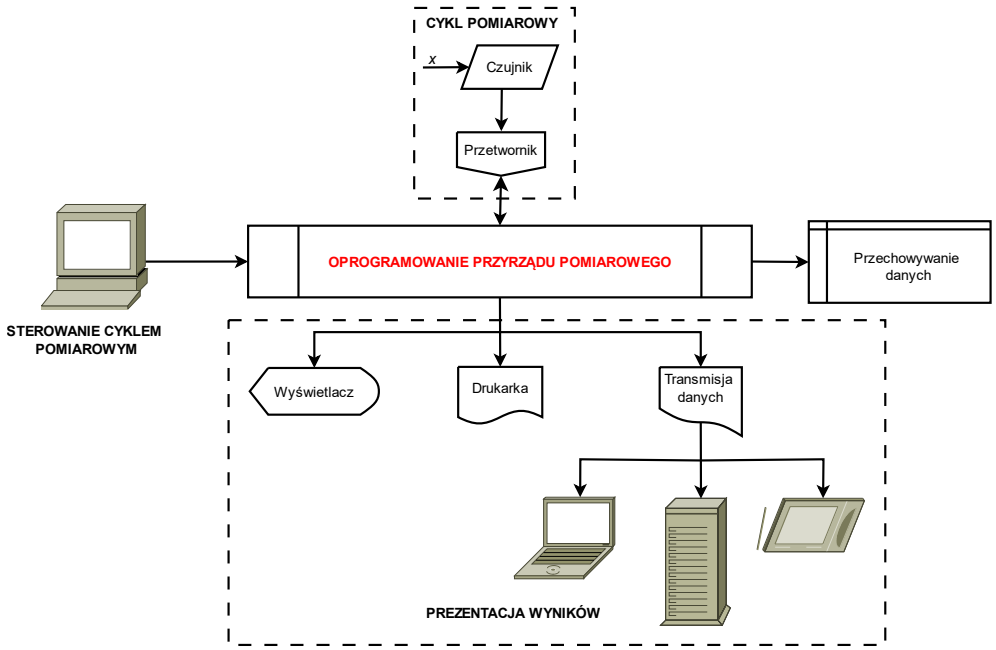
Początkowo rolę komputera sprowadzano do urządzenia zbierającego dane i biorącego udział w opracowaniu wyników lub do urządzenia, które tylko współpracuje z jedną bądź wieloma specjalistycznymi kartami pomiarowymi (przyrządy wirtualne), a jego monitor pełnił funkcję pola odczytowego (rys. 1) [2].

Z czasem urządzenie zbierające dane (komputer lub rejestrator) zaczęło być traktowane jako część przyrządu pomiarowego, a nie tylko dodatek do niego.

Zmiany wynikające z włączenia do konstrukcji przyrządów pomiarowych zdobyczy informatyki i telekomunikacji sprawiły, że stajemy przed koniecznością innego spojrzenia na przyrząd pomiarowy. Przykładem może być nie tylko włączenie do metrologii technologii informatycznej, ale również implementacja wcześniej niedostępnych rozwiązań technicznych z użyciem techniki światłowodowej, czy zjawisk kwantowych i nadprzewodnictwa. W rezultacie dalszych przemian wspominane wcześniej oprogramowanie stało się nie tylko elementem składowym przyrządu pomiarowego, ale jego centralną częścią (rys. 2), mającą często krytyczny wpływ na pomiar i jego rzetelność.

Podobnie wcześniej marginalnie traktowany sprzęt komputerowy [1] stał się stałym i ważnym elementem urządzenia lub układu pomiarowego, który ma wpływ na niezawodność przyrządu.

Na rzetelność wyników badań i ich bezpieczeństwo znaczący wpływ ma oprogramowanie, które wraz z czujnikiem i przetwornikiem pomiarowym stanowi jądro przyrządu. Oprogramowanie, pracujące na sprzętowej



Rys. 2. Współczesny schemat blokowy przyrządu pomiarowego na bazie oprogramowania

części przyrządu (hardware), steruje całym cyklem pomiarowym, zarządza danymi odebranymi od przetwornika oraz decyduje o dalszym przetwarzaniu i wykonywaniu obliczeń. Oprogramowanie kontroluje również prezentację wyników oraz zarządza gromadzeniem i przesyłaniem danych pomiarowych.

Proces i rzetelność w nowoczesnych przyrządach

Wpływ oprogramowania i technik teleinformatycznych na metrologiczną wiarygodność powinien być również brany pod uwagę ze względu na prezentowany w literaturze algorytm procesu pomiarowego [2]. Zazwyczaj wyróżnia się w nim trzy podstawowe elementy:

1) czynności przygotowawcze,
2) realizację techniczną pomiarów (pomiary właściwe i prezentacja wyniku),
3) opracowanie i interpretację wyników pomiaru.

W zastosowaniu przyrządów pomiarowych z oprogramowaniem sterującym wpływ ten jest szczególnie istotny na wymienioną realizację techniczną pomiarów (2), a wraz z nią na prezentację wyników. Oprogramowanie może wspomagać też proces opracowywania i interpretacji wyników pomiaru (3). Z tego powodu wymieniony algorytm pomiarowy można bardziej uszczegółowić o takie elementy, jak: przetwarzanie sygnału, rejestrację i wskazanie wyniku, przechowywanie danych pomiarowych oraz ich odtwarzanie i cyfrową transmisję (rys. 3).

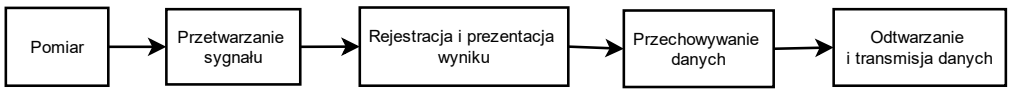
Wymienione składniki biorą udział w pomiarze właściwym i mają istotny wpływ na jego wiarygodność, ponieważ bezpośrednio (chociaż w niewidoczny dla użytkownika sposób) operują na uzyskanych z przetwornika danych pomiarowych. Ponadto oprogramowanie zazwyczaj steruje częścią lub całością cyklu pomiarowego, będąc realizacją założonego modelu pomiaru we wcześniej zaprojektowanym systemie pomiarowym [1, 3]. W literaturze metrologicznej, przy okazji omawiania realizacji technicznej pomiarów w procesie pomiarowym, coraz częściej mówi się o automatyzacji i cyfryzacji. Przykładowo, w jednej z pozycji pojawia się ogólne stwierdzenie: *Na pomiar właściwy składają się: wybór zakresów pomiarowych, porównanie z wzorcem, odczyt pomiaru. Czynności te coraz częściej wykonywane są automatycznie bez udziału człowieka* [2].

Przy ocenie wiarygodności pomiaru automatyzacja nie zwalnia nas jednak z uwzględniania zachodzących w urządzeniu pomiarowym procesów, które w urządzeniach informatycznych zazwyczaj przebiegają w sposób niewidoczny dla zwykłego użytkownika. Warstwa informatyczna przyrządu bierze bowiem udział w procesie pomiarowym i stanowi część środowiska pomiarowego wraz z zastosowanym w urządzeniu pomiarowym systemem operacyjnym, programem BIOS, sterownikami, interfejsami komunikacyjnymi oraz elementami sprzętowymi i ich stabilnością pracy [3]. Znajduje to również swój wyraz w omówionych dalej zbiorach wymagań i wytycznych dla przyrządów pomiarowych, działających pod kontrolą oprogramowania.

Problem wyznaczenia poziomu bezpieczeństwa informatycznego

Przedstawione rozważania prowadzą do wniosku, że w procesie metrologicznym, przy zapewnieniu wiarygodności pomiaru, konieczne jest uwzględnienie zagadnień bezpieczeństwa cyfrowego i określenia ryzyka, wynikającego z użycia oprogramowania w przyrządach pomiarowych. W różny sposób definiowane bezpieczeństwo cyfrowe jest związane z ogólnym pojęciem bezpieczeństwa informacji. Przykładowo podawane jest, że: *Bezpieczeństwo informacyjne, niejednokrotnie […] rozważa się jako element systemu informatycznego, jako synonim bezpieczeństwa komputerowego, telekomunikacyjnego, czy bezpieczeństwa sieciowego* [4]. W określaniu bezpieczeństwa cyfrowego używana jest zamiennie różna terminologia, np. bezpieczeństwo komputerowe, bezpieczeństwo sieci i systemów oraz inżynieria bezpieczeństwa. Mają w nim szerokie zastosowanie zagadnienia ogólnie definiowanego bezpieczeństwa informacji.

Pomimo dużego znaczenia problemu, dziedzina bezpieczeństwa informacyjnego na gruncie polskim od wielu lat jest zaniedbana i *zagadnienia bezpieczeństwa informacyjnego nadal nie doczekały się formalnego uznania – z perspektywy nauki polskiej nie są* [one] *dostrzegalne, a postulat włączenia bezpieczeństwa informacyjnego do dyscypliny naukowej „nauka o bezpieczeństwie" jako odrębnej specjalności naukowej nie został zrealizowany* [5]. Próbując znaleźć przyczyny takiego stanu rzeczy zauważono, że: *Być może przyczyną trudności ze znalezieniem miejsca w formalnej nauce dla bezpieczeństwa informacyjnego jest*



Rys. 3. Proces pomiarowy w przyrządach z oprogramowaniem sterującym

fakt, że jest to problematyka interdyscyplinarna. Mogłoby się wydawać, że we współczesnym społeczeństwie informacyjnym wszyscy powinni być zainteresowani informacją dobrej jakości, w szczególności informacją bezpieczną. Jednak postrzeganie tego zagadnienia przez techników i nie techników jest znacząco różne [5].

Widzimy więc, że temat ten jest różnie, a nawet selektywnie postrzegany i jak to zostanie dalej przedstawione, problematyka interdyscyplinarności zagadnień dotyczących bezpieczeństwa informacji i uwzględniania ich w metrologii polega faktycznie na trudności z precyzyjnym określeniem poziomu bezpieczeństwa cyfrowego w odniesieniu do urządzeń pomiarowych i samych wyników pomiarów. Liderman zauważa, że *bezpieczeństwo nie jest ani stanem, ani zdarzeniem, ani procesem – to imponderabilia z dziedziny psychologii, co swoje implikacje ma na przykład w możliwościach pomiaru bezpieczeństwa* [5]. Stwierdzenie to wydaje się bardzo trafne, gdyż pomimo tego, że stosuje się różnorodne metody oceny ryzyka cyfrowego, to jednak poziomu bezpieczeństwa informacji nie daje się ani dokładnie zmierzyć, ani obliczyć. Bezpieczeństwo informacyjne (w tym przetwarzanych, przechowywanych i przesyłanych danych pomiarowych) ze względu na cyfryzację i coraz większe wykorzystanie transmisji, przechowywania i przetwarzania danych, a także przez rozbudowane nowoczesne środki techniczne, jest wrażliwe na różnej postaci zagrożenia. Są to znaczne problemy, wiążące się z awarią sprzętu, błędami w oprogramowaniu, w szczególności błędami wynikającymi z niedostatecznego testowania i pospiesznego jego wdrażania oraz zagrożenia związane z tzw. cyberprzestępczością.

Ocena ryzyka cyfrowego w świetle rzetelności pomiaru

Korzystając z rozwiązań informatycznych w przyrządach pomiarowych i w przetwarzaniu danych cyfrowych, ze względu na konieczność zapewnienia wiarygodności pomiaru, metrologia musi korzystać z wypracowanych przez informatykę rozwiązań na określenie ryzyka. Dodatkowo, metrologia powinna podejmować próby tworzenia nowych metod i testów, które poprzez analizę jakościową, ilościową lub mieszaną pozwoliłyby porównywać ryzyko cyfrowe i uwzględniać je w ocenie wyników pomiaru.

Pojęcie ryzyka w jednej z norm, dotyczących technik informatycznych, ogólnie zdefiniowano jako *wpływ niepewności na cele* [6], co odnosi się również do ryzyka związanego z wykorzystaniem technologii cyfrowej w przyrządach pomiarowych i jego związku z rzetelnością pomiaru.

Jedną z prób usystematyzowania procesu zarządzania ryzykiem w bezpieczeństwie informacji są wytyczne, dotyczące technik bezpieczeństwa w informatyce, zawarte w normie PN-ISO/IEC 27005. Szacowanie ryzyka podzielono tam na etapy, w których można wyróżnić: identyfikację, analizę i ocena ryzyka [6]. Dla następstw i prawdopodobieństwa zidentyfikowanych zagrożeń, w zależności od przyjętej metodyki jakościowej lub ilościowej, norma w analizie ryzyka stosuje skale opisowe lub numeryczne, za pomocą których określany jest poziom ryzyka i dokonywana jest ocena. Oceny ryzyka mogą być wielokrotne i jeśli dochodzi się do niesatysfakcjonującego wyniku, proces szacowania jest ponawiany i bardziej uszczegóławiany. Ma to na celu podjęcie dodatkowych działań (postępowań), zmierzających do zminimalizowania ryzyka do ostatecznie akceptowalnego poziomu [6]. Wymieniony standard pozwala na dużą elastyczność w wyborze metodyki. W jej wyniku osiąga się przybliżoną wartość poziomu ryzyka na bazie szacowanych prawdopodobieństwem ocen i danych.

Mając na względzie faktyczną niemierzalność opisywanego ryzyka, przy ocenie bezpieczeństwa warto również korzystać z metod opartych na podejściu niesformalizowanej dowolności. Podejście tego typu oferuje doraźne metody ad hoc i eksploracyjne [7], które pozwalają lepiej uwzględnić użycie najnowszych rozwiązań w aparaturze pomiarowej, w obliczu dynamicznych zmian i nowych rozwiązań w technologii informatycznej. Bieżące tworzenie testów na potrzeby badania konkretnego urządzenia daje większą szansę wykrycia poważnych luk bezpieczeństwa i znacząco uzupełnia systemową metodologię badań, opartą na dużo wcześniej przygotowanych założonych testach i procedurach.

Szacowanie ryzyka w metodach opartych na modelowaniu

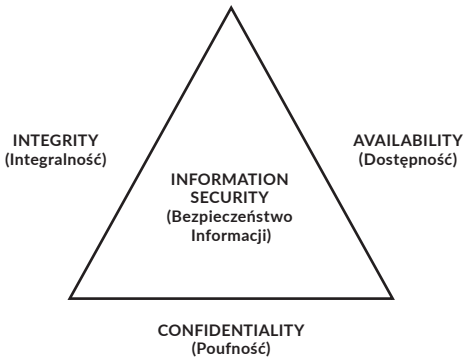
Przy dążeniu do określenia przybliżonego wskaźnika ryzyka często wykorzystywane są również metody oparte na modelowaniu ochrony informacji. Naukowcy z Krajowego Instytutu Metrologicznego w Niemczech (PTB) zwracają uwagę, że wymieniona norma [6] nie narzuca modelu odniesienia do obliczeń poszczególnych liczbowych prawdopodobieństw dla rozpatrywanych zagrożeń i wybór modelu jest pozostawiony użytkownikowi standardu [8]. Wybór i dostosowanie właściwego modelu do zaistniałej badanej sytuacji wydaje się więc kwestią dość istotną i mającą wpływ na wynik szacowania ryzyka. Można również zwrócić uwagę, że samo sięganie po uproszczone modele uzmysławia ukazywaną trudność rzetelnego oszacowania bezpieczeństwa informatycznego, które w praktyce okazuje się zadaniem bardzo złożonym.

Modele tego rodzaju opisują zwykle organizację i sterowanie dostępem do informacji, z czym spotykamy się

w schemacie Grahama–Denninga, operującym na zbiorach podmiotów, obiektów, poleceń i na macierzach dostępu. W opartym na nim innym modelu Harrisona–Ruzzo––Ullmana (HRU) mamy do czynienia ze skupieniem się wyłącznie na zagadnieniu ochrony samej informacji. Kolejny, podobny model BLP (Bella–LaPaduli), poza sterowaniem dostępem, szerzej uwzględnia ochronę danych w zakresie tajności. W systemach komputerowych z kluczową integralnością informacji zazwyczaj wykorzystywane są reguły nakreślone w modelach Biby oraz Clarka–Wilsona. W przemyśle, dla oceny bezpieczeństwa systemów komputerowych stosowany jest model Brewera–Nasha. Jest to model oparty na koncepcji tzw. „chińskiego muru", w którym uprawnienia dostępu zmieniają się dynamicznie i podlegają weryfikacji po każdej zmianie [5, 9].

W modelowaniu systemów intensywnie korzystających z oprogramowania wymienia się model SRAM (Software Risk Assessment Model) oceniający ryzyko oprogramowania za pomocą rozbudowanego kwestionariusza oraz model SRAEP (Software Risk Assessment and Evaluation Process) bazujący na modelowaniu i identyfikowaniu ryzyka za pomocą drzewa błędów w oprogramowaniu. Wymienione modele są tylko bardziej znanymi przykładami różnorodnych podejść i mają tylko ilustrować złożoność problemu.

Jak widać, dla różnych systemów i specyficznych potrzeb ochrony informacji tworzone są własne, przystosowane modele. Dodatkowo, co stwierdził Liderman, modele formalne mają swe teoretyczne ograniczenia i *same w sobie nie zapewniają bezpieczeństwa, mogą co najwyżej dostarczyć wskazówek, jak to bezpieczeństwo budować* [5]. Podczas szacowania ryzyka najczęściej wychodzi się od ogólnych wyznaczników jakości, związanych z ochroną informacji, takich jak: tajność, integralność, dostępność, rozliczalność, niezaprzeczalność, autentyczność [5]. W celu opisania podstawowego standardu oceny i wdrażania bezpieczeństwa informatycznego przyjęło się, niezależnie od systemów, stosować tzw. triadę CIA (Confidentiality, Integrity, Availability), określającą zabezpieczenia



Rys. 4. Bezpieczeństwo informacji

informacji w obszarach poufności, integralności (nienaruszalności) i dostępności (rys. 4).

Wymienione atrybuty bezpieczeństwa odnoszą się również do urządzeń pomiarowych z oprogramowaniem, które powinny zapewnić ochronę informacji przed nieautoryzowanym ujawnieniem (poufność), ochronę informacji przed zmodyfikowaniem przez podmioty, które nie mają do nich uprawnień (integralność) oraz umożliwić stabilne korzystanie z danych i zasobów przez osoby uprawnione (dostępność) [10].

Użyteczna w swej prostocie triada jest także opisem pewnego podstawowego modelu, który w zależności od potrzeb może być modyfikowany i uzupełniany [11, 12].

Do powyższego odnosi się praktyka administratorów systemów informatycznych, która wykazuje, że bezpieczeństwo cyfrowe nie jest stabilnym stanem. Jest raczej procesem, w którym wciąż potrzeba wykonywać pewien zespół określonych czynności, co wyrażono następująco: *Z punktu widzenia administratora systemu lub sieci sprawa jest relatywnie prosta, z perspektywy osoby, która zarządza procesem lub działaniem całość staje się bardziej skomplikowana. […] Do pomocy istnieje wiele narzędzi, zarówno na poziomie administracji, jak i na poziomie zarządzania. […] Na poziomie zarządzania skorzystać można z literatury i norm opracowanych specjalnie w celu wyznaczenia ram dla procesów bezpieczeństwa oraz aplikacji komputerowych wspomagających zarządzania* [10].

Podobnie Liderman zauważa, że *zapewnienie bezpieczeństwa zawsze będzie sztuką, ale też zawsze powinno być oparte na solidnych podstawach inżynierskich* [5].

Można przyjąć, że szacowanie ryzyka dla przyrządów pomiarowych jest możliwe dwutorowo. Po pierwsze, poprzez analizę potencjalnych zagrożeń, z wykorzystaniem wektorów ataków analogicznych do stosowanych w rozwiązaniach informatycznych, stosowanych w innych obszarach. Przykładem mogą być naruszenia ograniczeń dostępu, ataki obciążeniowe (Denial of Service, DoS), zdobycia uprawnień umożliwiających ingerencję w konfigurację bądź sposób działania przyrządu, a także dostęp do danych poufnych i manipulacja nimi. Zagrożenia takie mogą być analizowane teoretycznie, a wskaźniki ryzyka szacowane na podstawie powszechnie użytkowanych systemów teleinformatycznych, w sposób uwzględniający techniczne, psychologiczne i inne metody włamań.

Po drugie, poprzez analizę ryzyka, na podstawie rzeczywistych incydentów zidentyfikowanych w trakcie czynności kontrolnych służb metrologicznych, analiz rejestrów zdarzeń i obserwacji zachowań użytkowników przyrządów. Oczywiście podejście takie wymaga stworzenia narzędzi rejestrujących incydenty oraz systemu nadzoru nad przyrządami pomiarowymi, uwzględniającego weryfikację zagrożeń cyfrowych.

Połączenie tych dwóch podejść w analizie ryzyka może wskazać pełny obraz sytuacji i zagrożeń, z jakimi mamy do czynienia w środowisku pracy cyfrowych przyrządów pomiarowych. Eliminacja wystąpienia ryzyka o wysokim prawdopodobieństwie bądź wysokim poziomie istotności jest możliwa, ale dopiero na podstawie zgromadzonych długookresowo danych.

Standardy i normy bezpieczeństwa informacyjnego

Wymagany poziom bezpieczeństwa cyfrowego urządzeń metrologicznych można zapewnić poprzez zachowanie ustalonych standardów informatycznych. Standardem można nazwać pewne zdefiniowane uzgodnienia, zatwierdzone albo przez instytucję normalizacyjną, albo przyjęte nieformalnie, poprzez ich znaczące upowszechnienie i uznanie w środowiskach zajmujących się daną dziedziną. Standardy bezpieczeństwa teleinformatycznego zasadniczo można podzielić na dwie grupy [5]. Pierwszą stanowią tzw. „miary gwarantowanej odporności", do których przypisuje się standardy: Common Criteria (CC) [13] (również jako norma [14]), TCSEC [15], ITSEC [16]. Zazwyczaj służą one certyfikacji systemów i produktów teleinformatycznych.

Drugą grupą są standardy tzw. „dobrych praktyk", określające cechy bezpiecznych systemów informacyjnych, z których najbardziej znane są następujące: BS 7799 [17, 18] i oparte na nim normy ISO/IEC 2700x, rekomendacje NIST (serii SP-800) [19] oraz dokumenty: CAG/CIS [20], COBIT [21], ITIL [22], SSE-CMM [23], w tym norma ISO/IEC 21827. W tej grupie możemy również wymienić wytyczne, dotyczące przyrządów pomiarowych z oprogramowaniem sterującym, publikowane przez organizacje metrologiczne, jak OIML i WELMEC oraz niektóre opracowania norm PKN, w których uwzględniono aspekty bezpieczeństwa informatycznego dla urządzeń pomiarowych.

Odnośnie do urządzeń metrologicznych, warto zwrócić uwagę na ogólne wymagania dla oprogramowania kontrolującego przyrządy pomiarowe zawarte w dokumencie D31 OIML [24] oraz na odnoszący się do dyrektywy MID [25] przewodnik oprogramowania WELMEC 7.2 [26], jak również na normy branżowe, dotyczące urządzeń pomiarowych (np. wag nieautomatycznych PN EN 45501).

Odzwierciedlenie tych standardów można znaleźć również w krajowych przepisach, dotyczących wymagań technicznych dla poszczególnych rodzajów przyrządów pomiarowych [27].

Nawet krótkie przedstawienie każdego z wymienionych standardów wykracza poza cele i zakres niniejszego artykułu, gdyż są one obszernymi i szczegółowymi opracowaniami zagadnień, związanych z ochroną i oceną bezpieczeństwa informacji w systemach informatycznych i pomiarowych. W celu zapoznania się z nimi najlepiej bezpośrednio zwrócić się do wymienionych wytycznych oraz dodatkowej literatury.

Przykładowo, odnośnie do przyrządów pomiarowych możemy ogólne stwierdzić, że dokument D31 OIML podaje wymagania dotyczące takich podstawowych zagadnień, jak: identyfikacja oprogramowania, ochrona przed niewłaściwym użyciem i oszustwami, kontrola prawidłowości zastosowanych algorytmów i funkcji, a także prawidłowe wykrywanie błędów i ich obsługa. Poza tym dokument D31 określa specyficzne wymagania, odnoszące się do konfiguracji i budowy przyrządu, w których uwzględnia się aspekty separacji składowych części oprogramowania i podzespołów, automatycznego zapisu i zabezpieczenia przechowywania danych, zagadnienia związane z bezpieczną transmisją danych pomiarowych oraz weryfikacją i rejestracją aktualizacji oprogramowania.

Zarys wymagań standaryzowany przez Software Guide 7.2 WELMEC przedstawiono w uproszczeniu w tabeli 1, gdzie dodatkowo wyszczególniono ich znaczenie dla wiarygodności pomiaru.

Można zauważyć, że wytyczne przewodnika WELMEC koncentrują się na zabezpieczeniach w trzech kategoriach: bezpieczeństwa oprogramowania, bezpieczeństwa przechowywania danych oraz na zabezpieczeniach transmisji danych pomiarowych, co jest kluczowe dla ochrony oprogramowania i danych w celu zapewniania rzetelności urządzenia pomiarowego.

Wykorzystanie nowoczesnej informatyki w metrologii

Nawet bardzo ogólne przedstawienie wielu dość złożonych zagadnień, jakie należy uwzględnić, chcąc wykorzystywać zdobycze informatyki i telekomunikacji w dziedzinie metrologii, może powodować wrażenie, że użycie oprogramowania i sprzętu cyfrowego w budowie i wykorzystaniu przyrządów i systemów pomiarowych rodzi wiele trudnych do przezwyciężenia problemów, z którymi należy się zmierzyć. Dlatego, na zakończenie powinno się wspomnieć o szerokich możliwościach wykorzystania tego typu urządzeń w nowoczesnych laboratoriach pomiarowych, przemyśle i możliwościach, które bez informatyki byłyby niedostępne.

Rozwój ICT przyczynił się do praktycznej realizacji koncepcji urządzeń, które za pomocą sieci elektrycznej lub komputerowej mogą bezpośrednio gromadzić, przetwarzać i wymieniać dane (Internet of Things – IoT, Internet of Everything – IoE). Przyrządy pomiarowe wyposażane w interfejsy i oprogramowanie, umożliwiają pracę w sieci i automatyczne przesyłanie danych

Tabela 1. Obszary regulacji w Software Guide 7.2 WELMEC

Wymagania szczegółowe w obszarach regulacji	Wpływ na wiarygodność Cel regulacji
BEZPIECZEŃSTWO OPROGRAMOWANIA – Jednoznacznie identyfikowalne oprogramowanie – Niezależność programu sterującego od innego oprogramowania	OPROGRAMOWANIE Niezmienność programu
– Automatyczna aktualizacja oprogramowania z zachowaniem zabezpieczeń – Autoryzacja autentyczności i sprawdzenie integralności aktualizacji – Nieusuwalny rejestr zmian oprogramowania	Zarządzanie aktualizacjami
– Zabezpieczenie przed przypadkowymi zmianami i celową modyfikacją	DANE – Niezmienność
– Brak możliwości zmiany i wiarygodna prezentacja wyników – Rozróżnienie wyników pomiaru od informacji dodatkowych	INTERFEJSY Interfejs użytkownika (GUI)
– Brak wpływu na zawartość i działanie programu, konfigurację i dane – Bezpieczna wymiana danych metrologicznych	Zabezpieczenie interfejsów i komunikacji
– Inne oprogramowanie nie może zaburzać pomiaru – Ciągłość pracy programu w sytuacjach awaryjnych i zaburzeń działania – Wewnętrzne zasilanie, zapewniające odpowiednio długą ciągłą pracę	POMIAR Odporność na awarie
– Zabezpieczenie przed nieautoryzowaną zmianą	Parametry konfiguracyjne
BEZPIECZEŃSTWO PRZECHOWYWANIA DANYCH – Przechowywanie wszystkich wymaganych danych – Zabezpieczenie przed przypadkowymi zmianami i celową modyfikacją	DANE Zapewnienie niezmienności danych
– Zachowane dane zapewniają identyfikowalność pomiaru – Poufność kluczy kryptograficznych i zabezpieczonych danych	Poufność i uwierzytelnienie danych
– Prezentacja i weryfikacja niezmienności zapisanych danych – Automatyczny zapis i odpowiednia pojemność nośnika danych – Okresowa kopia zapasowa danych pomiarowych w pamięci nieulotnej – Brak możliwości skasowania liczników kumulacyjnych	Odtwarzalność danych
– Zapewnienie ciągłego i poprawnego wskazywania wyniku pomiaru	INTERFEJS (GUI)
– Wykrywanie i raportowanie przekroczenia parametrów pracy	POMIAR – Niezawodność
BEZPIECZEŃSTWO TRANSMISJI DANYCH – Przesyłanie wszystkich niezbędnych danych do dalszego przetwarzania – Zabezpieczenie transmitowanych danych przed przypadkowymi zmianami – Zabezpieczenie przed celową modyfikacją przesyłanych danych	DANE Zapewnienie niezmienności danych
– Weryfikacja autentyczności przesyłanych danych – Poufność kluczy kryptograficznych i zabezpieczonych danych	Poufność i uwierzytelnienie danych
– Obsługa i uniemożliwienie przetwarzania uszkodzonych danych – Opóźnienie transmisji nie może wpływać na przebieg pomiaru – Zachowanie danych w przypadku niedostępności sieci komunikacyjnej	POMIAR Niezawodność i odporność na awarie

pomiarowych. Powoduje to, że pomimo istniejących zagrożeń cybernetycznych coraz szerzej zaczynają być stosowane sieciowe rozwiązania metrologiczne. Nawet tymczasowe połączenie sprzętu pomiarowego np. ze smartfonem daje ogromne możliwości. Podobnie perspektywę poszerza zbieranie, analizowanie i monitorowanie danych pomiarowych z wielu rozproszonych czujników poprzez sieć teleinformatyczną, oferując tych możliwości jeszcze więcej.

Równocześnie, w przypadku komunikacji z urządzeniami o otwartej architekturze (np. przytoczony smartfon, wyposażony w system operacyjny z rodziny Android), mogą pojawić się dodatkowo nowe i trudne do zdefiniowania ryzyka, mające wpływ na rzetelność pomiaru i wiarygodność wyników, gdyż są to systemy podlegające ciągłym zmianom i dające potencjalną możliwość manipulacji i niezdefiniowanego wpływu na oprogramowanie i na cykl pomiarowy.

W świecie trwają prace nad powszechnym wdrożeniem sieci inteligentnych (Smart Grids) do pomiaru dostarczonej energii i zarządzaniem jej dystrybucją [28]. Przez zastosowanie nowoczesnych liczników (Smart Meters), które umożliwiają dwukierunkową komunikację, następuje przesyłanie wyników pomiaru do centralnych systemów informatycznych. Przykładowo, omawiając temat bezpieczeństwa informatycznego w sieciach inteligentnych, Billewicz zwrócił uwagę, że zwiększenie automatyzacji i komunikacji, przy zastosowaniu tego typu sieci, boryka się z problemem zwiększonej podatności na ataki i możliwej ingerencji cyberprzestępców. Spośród najczęstszych zagrożeń systemów informatycznych wymienił on następujące: *zablokowanie dostępu do usługi, włamanie do infrastruktury systemu informacyjnego, utrata danych, kradzież danych, ujawnienie poufnych danych, zafałszowanie informacji, kradzież kodu oprogramowania, kradzież sprzętu, uszkodzenia systemów komputerowych* [29]. Pomimo pojawiających się trudności w zabezpieczeniach, technologia jest wciąż udoskonalana.

Rozwój technik teleinformatycznych, związanych z wprowadzeniem najnowszych systemów, opartych na Cloud Computing i Big Data, otwiera nowe możliwości również dla metrologii. Pojęciem Cloud Computing określa się skalowalną platformę, zawierającą sprzęt IT wraz z oprogramowaniem, która jest dostępna dla zewnętrznego operatora i jako usługa jest dostarczana za pośrednictwem Internetu. *Cloud Computing oznacza również system rozproszenia, zdolność uruchamiania programu lub aplikacji na wielu połączonych komputerach w tym samym czasie lub dynamiczną obsługę danego żądania, polegającą na przydzieleniu zadania do jednego z dostępnych serwerów* [30]. Użytkownik, przykładowo firma lub instytucja, nie musi posiadać w swoich zasobach urządzeń (np. serwerów) ani oprogramowania, natomiast wszystko podnajmuje od innych firm. Rozwiązanie takie wygląda dość korzystnie i mogłoby mieć zastosowanie również w systemach metrologicznych, o ile udałoby się rozwiązać pojawiające się w związku z tym dylematy (np. prawne). Trzeba byłoby zapewnić właściwą ochronę uwierzytelnienia danych pomiarowych i zagwarantować należytą ochronę oprogramowania pracującego na odległym serwerze, który jest administrowany przez zewnętrznego dostawcę usługi.

Rozwiązania takie opierają się na sposobach zabezpieczeń trudnych do technicznej weryfikacji i opartych na pozametrologicznych standardach bezpieczeństwa, stosowanych w branży ICT. Dodatkowo, fakt osadzenia elementów infrastruktury pomiarowej w lokalizacjach, niepodlegających lokalnym rozwiązaniom prawnym i nadzorowi metrologicznemu, stwarza szereg problemów formalno-prawnych oraz technicznych, związanych z możliwościami weryfikacji zabezpieczeń w stosunku do rozwiązań lokalnych. Związane jest to z rozmytą odpowiedzialnością za bezpieczeństwo pomiędzy użytkownikiem usługi a jej dostawcą. Środowisko metrologiczne stoi więc przed wielkim wyzwaniem, dotyczącym wiarygodności nowoczesnych technologii IT w urządzeniach i systemach pomiarowych, a także przed wypracowaniem filozofii zaufania i narzędzi, umożliwiających walidację niezawodności i bezpieczeństwa nowoczesnych przyrządów i rozwiązań.

Wydaje się, że czarnoskrzynkowe metody testowania oprogramowania są tutaj optymalnym rozwiązaniem (również ze względu na brak dostępu do szczegółów technicznych konfiguracji tych rozwiązań). Jednakże z uwagi na uwarunkowanie bezpieczeństwa przyrządu od konfiguracji programowo-sprzętowej, zależnej wyłącznie od operatora udostępnianej platformy, konieczne jest oparcie zaufania o pozametrologiczne standardy i system certyfikacji bezpieczeństwa, powszechnie stosowane w środowisku ICT (np. stosowanie standardowych kanałów komunikacji – sieć Internet, kanały VPN, NFC, Bluetooth, RS232). Dylemat ten występuje również w przypadku konieczności oparcia bezpieczeństwa na systemach operacyjnych o odpowiedniej konfiguracji, wysokim stopniu złożoności i nieokreślonym kierunku rozwoju i aktualizacji.

Również rozwiązania dostępne poprzez najnowsze techniki analizy i składowania dużych ilości danych o wysokiej złożoności (Big Data) dają nadzieję na wykorzystanie ich przy zbieraniu i analizie wyników pomiarów w skali dotąd nieosiągalnej. Próbując zdefiniować tę nową dziedzinę podaje się, że *Big Data to określenie stosowane dla takich zbiorów danych, które jednocześnie charakteryzują się dużą objętością, różnorodnością, strumieniowym napływem w czasie rzeczywistym, zmiennością, złożonością, jak również wymagają zastosowania innowacyjnych technologii, narzędzi i metod informatycznych w celu wydobycia z nich nowej i użytecznej wiedzy* [30].

W 2013 r. firma IBM, odnosząc się do budowy takich usług, w których należy obsługiwać wiele danych, pochodzących z różnych źródeł i generowanych z dużą prędkością, opisała Big Data za pomocą czterech głównych atrybutów: objętości (volume), szybkości przetwarzania (velocity), różnorodności danych (variety) oraz, na co warto zwrócić uwagę, wiarygodności (veracity) [30]. Wykorzystanie powyższych technologii wiąże się z zamiarem opracowania skutecznych metod przetwarzania Big Data, pochodzących z rozproszonych źródeł, z czego oczekuje się osiągnięcia możliwości reakcji na napływ danych w czasie rzeczywistym. Wydaje się, że metody te mogą znaleźć zastosowanie w rozproszonych systemach pomiarowych i podobnie jak w innych rozwiązaniach, będą wymagały wypracowania przez metrologię odpowiedniego podejścia.

Podsumowanie

Zastosowanie oprogramowania metrologicznego w przyrządach pomiarowych stało się powszechne. Oprogramowanie i elementy realizujące funkcje przetwarzania danych we współczesnych urządzeniach pomiarowych są integralnymi i ważnymi częściami składowymi przyrządów, mającymi wpływ na niezawodność i rzetelność pomiaru. Wykorzystanie rozwiązań informatycznych przyczyniło się do rozszerzenia procesu pomiarowego o cyfrowe i programowe przetwarzanie sygnału, rejestrację i wskazanie wyniku, przechowywanie danych pomiarowych oraz odtwarzanie i transmisję wyników pomiaru.

Mając na uwadze, że istnieje związek bezpieczeństwa informatycznego z rzetelnością pomiaru, należy określić poziom ryzyka cyfrowego. Zadanie to okazuje się dość skomplikowane, gdyż bezpieczeństwa informacji faktycznie nie daje się ani dokładnie zmierzyć, ani obliczyć. Ocena ryzyka cyfrowego wymaga więc opracowywania i zastosowania systemowych metod przybliżonych. Przy tym warto również korzystać z metod doraźnych i eksploracyjnych, gdyż pozwalają na wykrywanie dodatkowych zagrożeń bezpieczeństwa i uzupełniają systemową metodologię badań, opartą na wcześniej opracowanych testach i procedurach. Narzędziem dla przybliżonych metod szacowania poziomu ryzyka cyfrowego są liczne metody oparte na uproszczeniu i modelowaniu, wypracowywane przez instytucje zajmujące się bezpieczeństwem informacji.

Ważną rolę w zapewnieniu bezpieczeństwa informacyjnego i rzetelności urządzeń i systemów pomiarowych pełnią standardy i normy bezpieczeństwa, które w metrologii koncentrują się na bezpieczeństwie oprogramowania i przechowywania danych oraz na zabezpieczeniach transmisji wyników pomiarów. W tej dziedzinie szczególnie użyteczne wydają się wytyczne organizacji metrologicznych, jak OIML i WELMEC oraz szczegółowe normy branżowe, tworzone w oparciu o dostępne standardy.

Wykorzystanie nowoczesnej informatyki w metrologii daje wiele korzyści, pomimo konieczności uwzględniania licznych zagadnień, związanych z zapewnieniem bezpieczeństwa cyfrowego przyrządów pomiarowych. Są to korzyści, które bez informatyki byłyby niedostępne, dające nowe możliwości i posiadające wiele zalet, takich jak: możliwość gromadzenia dużych ilości danych, ich bieżącą i przyszłą analizę oraz użycie sprzętu i oprogramowania w rozproszonych systemach komputerowych.

Literatura

[1] Jaworski J. M., Morawski R. Z. [et al.], Wstęp do metrologii i techniki eksperymentu, Wydawnictwa Naukowo-Techniczne, Warszawa 1992, s. 3-5, 153-190.

[2] Lisowski M., Podstawy metrologii, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011, s. 7, 68, 70, 72.

[3] Winiecki W., Organizacja komputerowych systemów pomiarowych, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2006, s. 256.

[4] Więcaszek-Kuczyńska L., Zagrożenia bezpieczeństwa informacyjnego, „Obronność. Zeszyty Naukowe" 2014, nr 2(10), s. 210-233.

[5] Liderman K., Bezpieczeństwo informacyjne: nowe wyzwania, PWN, Warszawa 2017, s. 10, 17-18, 84-137, 318-353.

[6] PN-ISO/IEC, 27005:2014-01. Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN, Warszawa 2014, s. 10, 20-28.

[7] ISTQB, Słownik wyrażeń związanych z testowaniem. Wersja 2.3 (2014), Stowarzyszenie Jakości Systemów Informatycznych 2014, s. 69, 71.

[8] Esche M., Thiel F., Software Risk Assessment for Measuring Instruments in Legal Metrology, Łódź 2015, t. 5, s. 1114.

[9] Stokłosa J., Bilski T., Pankowski T., Bezpieczeństwo danych w systemach informatycznych, Wyd. Naukowe PWN, Warszawa, Poznań 2001.

[10] Wojsław D., Pojęcie bezpieczeństwa. CIA, http://websecurity.pl/pojecie-bezpieczenstwa-cia/ [6 listopad 2018 r.].

[11] Cherdantseva Y., Hilton J., Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals [w:] Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.), IGI Global Publishing 2013.

[12] Wikipedia, Information security, https://en.wikipedia.org/wiki/Information_security [16 listopad 2018 r.].

[13] Białas i in. A., Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria, Katowice 2011.

[14] ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security.

[15] Department of Defense Standard, Trusted Computer System Evaluation Criteria (TCSEC, Orange Book), 15.08.1983 r., https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf [7 grudzień 2018 r.].

[16] ITSEC, Information Technology Security Evaluation Criteria (ITSEC). Provisional Harmonised Criteria, https://web.archive.org/web/20060523094527/http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf [7 grudzień 2018 r.].

[17] British Standard Institute, BSI, Code of practice for Information Security Management (BS 7799-1:1995), 1995.
[18] British Standard Institute, BSI, Specification for Information Security Management Systems (BS 7799-2:1998), 1998.
[19] National Institute of Standards and Technology, NIST Special Publications, https://csrc.nist.gov/publications/sp [7 grudzień 2018 r.].
[20] Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense, https://web.archive.org/web/20160919021105/https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf [7 grudzień 2018 r.].
[21] Information Systems Audit and Control Association (ISACA), Control Objectives for Information and related Technology (COBIT), https://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx [7 grudzień 2018 r.].
[22] AXELOS, ITIL – IT Service Management, https://www.axelos.com/best-practice-solutions/itil [7 grudzień 2018 r.].
[23] SSE-CMM, The Systems Security Engineering Capability Maturity Model, http://www.sse-cmm.org/model.htm [7 grudzień 2018 r.].
[24] OIML, General requirements for software controlled measuring instruments, D 31, https://www.oiml.org/en/files/pdf_d/d031-e08.pdf [7 grudzień 2018 r.].
[25] MID, Dyrektywa Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych, http://www.ce-polska.pl/upload/pictures/2014-32-ue.pdf [17 grudzień 2018 r.].
[26] WELMEC, Software Guide, https://www.welmec.org/fileadmin/user_files/publications/WG_07/WELMEC_Guide_7.2_Software_Guide_2018.pdf [7 grudzień 2018 r.].
[27] Rozporządzenie Ministra Gospodarki z dnia 17 lutego 2014 r. 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.
[28] Kowalak T., Wybrane wymagania dla liczników odbiorców końcowych oraz liczników bilansujących w kontekście współpracy Infrastruktury AMI z Infrastrukturą Sieci Domowej (d. HAN) oraz potrzeb rozliczeniowych odbiorców końcowych, http://old.ure.gov.pl/download/1/5634/Wybranewymaganiadlalicznikowodbiorcowkoncowychorazlicznikowbilansujacychwkonteks.pdf [17 październik 2018 r.].
[29] Billewicz K., Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach, Jurata 2011.
[30] Tabakow M., Korczak J., Franczyk B., Big Data – definicje, wyzwania i technologie informatyczne, „Informatyka Ekonomiczna Business Informatics" 2014, nr 1(31), s. 141, 147.