O POMIARACH BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki
Wojskowa Akademia Techniczna, ul. S. Kaliskiego 2, 00–908 Warszawa
lider@ita.wat.edu.pl

Streszczenie

Artykuł dotyczy zagadnienia pomiarów „bezpieczeństwa". Główna teza artykułu głosi, że bezpieczeństwa nie można, w sensie technicznym, pomierzyć. Mierzalny jest natomiast stan ochrony obiektu lub systemu, który to wynik pomiaru może mieć wpływ na subiektywne poczucie bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo teleinformatyczne, pomiar.

ABOUT SECURITY MEASUREMENT

Summary

The paper presents security/safety measurement problem. Main paper thesis is that security, in technical meaning, is not measurable. Measurable is object or system security state, and measurement result may have impact on a subjective sense of security.

Keywords: safety, security, measurement.

1. WSTĘP

> *When you can measure what you are speaking about and express it in numbers, you know something about it. But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind.*
>
> Lord Kelvin, 1883

W modnym od początku XXI wieku podejściu „procesowym" dużą wagę w zarządzaniu (jakością, ryzykiem, bezpieczeństwem itp.) przykłada się do wsparcia tego procesu mierzalnymi wskaźnikami. Klasycznym przykładem jest *Capability Maturity Model* (CMM)[1] w którym już dla poziomu 3, tzw. zdefiniowanego, wymaga się aby: *„...Większość składowych procesu była monitorowana względem określonych miar"*, a dla poziomu 4 (zarządzanego): *„... Możliwe jest monitorowanie i pomiar zgodności z procedurami oraz podjęcie działań w sytuacji, gdy widoczne jest, że procesy nie działają efektywnie"*. W zakresie zarządzania bezpieczeństwem informacji przykładem może być planowana, w nowej serii norm ISO/IEC 27000 związanych z bezpieczeństwem, norma ISO/IEC 27004: *System Zarządzania Bezpieczeństwem Informacji. Wskaźniki i pomiar*.

Bezpośrednio o „pomiarze bezpieczeństwa" jest mowa w publikacji [8] zatytułowanej *„Security Measurement"*. W uznanym standardzie [12] wymaga się, aby miary bezpieczeństwa systemów teleinformatycznych bazowały na celach i zadaniach tych systemów w zakresie bezpieczeństwa, które to cele i zadania określają pożądane rezultaty implementacji programu zapewniania bezpieczeństwa. Wspomniane miary ([12], str. VII):

- muszą przedstawiać informacje ilościowe (procenty, średnie, liczby);
- dane stanowiące podstawę miar muszą być łatwe do uzyskania;
- tylko procesy powtarzalne mogą być brane pod uwagę do pomiarów (w oryginale: *considered for measurement*);
- miary muszą być przydatne do oceny wydajności i zarządzania zasobami.

Firma lub organizacja może opracować i gromadzić miary trzech typów [12]:

- miary „implementacyjne" do mierzenia (w oryginale: *measure*) implementacji polityki bezpieczeństwa;
- miary „efektywności/skuteczności" do mierzenia rezultatów dostarczonych usług z zakresu bezpieczeństwa (w oryginale: *security services*);
- miary „wpływu" do mierzenia wpływu zdarzeń z zakresu bezpieczeństwa na procesy biznesowe lub misję firmy (organizacji).

[1] Opracowany w Software Engineering Institute Carnegie Mellon University, określa wielopoziomowy model referencyjny profesjonalnej dojrzałości firmy/organizacji oraz kryteria jej kwalifikowania do poszczególnych poziomów dojrzałości. Rozwinięcie tego modelu na potrzeby bezpieczeństwa teleinformatycznego jest zawarte w normie [15].

Ożywiona w ostatnich latach działalność publikacyjna (por. np. [1, 8, 16]) i standaryzacyjna ([11, 12, 13, 18, 20]), ma na celu przede wszystkim doprowadzenie do zmniejszenia chaosu terminologicznego[2] i wypracowanie ogólnie uznawanych „miar bezpieczeństwa". Niestety, nadal wiele zagadnień związanych z pomiarami bezpieczeństwa pozostaje w sferze dyskusji. Na gruncie polskim dokładają się do tego trudności z jednoznacznym przetłumaczeniem i interpretacją terminów angielskich *„safety"* i *„security"*, zwykle tłumaczonych w obu przypadkach jako „bezpieczeństwo", co implikuje także trudności z precyzyjnym określeniem przedmiotu pomiaru.

Kolejnym zagadnieniem, mogącym budzić uzasadnione obiekcje u „tradycyjnego" inżyniera, jest używanie terminu „pomiar" nawet tam, gdzie niczego się nie mierzy w sensie fizycznym a jedynie zbiera dane obserwacyjne, oraz swobodne używanie terminów „metryka"[3] i „miara".

Niniejsza publikacja stanowi próbę rozważenia zagadnień określania, pozyskiwania (tutaj pojawia się właśnie dyskusyjny w rozważanym kontekście termin „pomiar") i zastosowania miar bezpieczeństwa na tle tradycyjnej, formalnej teorii pomiaru. W szczególności powinna zostać znaleziona odpowiedź na pytanie, czy jest uprawnione stosowanie terminu „pomiar", tak jak stosuje się ten termin w naukach technicznych, w odniesieniu do działań związanych z określaniem różnych miar i wskaźników „bezpieczeństwa".

2. POMIAR

Za [14] można podać następującą, niesformalizowaną definicję pomiaru (formalna definicja pomiaru jest podana w rozdziale 3):

Definicja 1

Pomiar *jest procesem empirycznym obiektywnego przyporządkowania liczb właściwościom obiektów i zdarzeń świata realnego w sposób umożliwiający jego opisanie.*

Gdy właściwość przedmiotu lub zdarzenia jest scharakteryzowana liczbą, to liczba ta „niesie" informację o tej właściwości. Liczbę taką, reprezentującą właściwości fizyczne, nazywa się **miarą**. Poza właściwościami fizycznymi istnieją także inne właściwości, dla których odpowiednie miary są problematyczne (trudno jest ustalić skale pomiarowe): „piękno" dzieła sztuki, „bezpieczeństwo" informacji, „smarowalność" masła itp.

Podana definicja pomiaru jako pewnego procesu, zawiera wymagania co do:

- określenia przedmiotu pomiaru;
- przyporządkowania liczb (miar);
- obiektywności;
- empiryczności.

Przez wymaganą w definicji pomiaru „obiektywność" rozumie się to, że liczby przyporządkowane właściwościom muszą być, w granicach błędu, niezależne od obserwatora. W definicji pomiaru nacisk jest położony także na empiryczny charakter procesu pomiarowego. Oznacza to, że:

1) pomiar musi być wynikiem **obserwacji** (a nie np. eksperymentu myślowego);
2) koncepcja właściwości mierzonej musi być oparta na relacji **empirycznej** (a nie na arbitralnej decyzji).

Pomiar musi być poprzedzony określeniem przedmiotu pomiaru. Mierzenie takiego pojęciowego tworu jak „sprawność zarządzania" czy „bezpieczeństwo teleinformatyczne" musi zawieść, o ile jego koncepcja nie jest wyraźnie sprecyzowana. Pojęciem podstawowym jest tutaj pojęcie „przejawu właściwości" obiektu, cechy abstrakcyjnej, pojedynczej wyczuwalnej cechy obiektu lub zdarzenia, np. twardość materiału, zapach substancji itp. Jeżeli nie istnieje obiektywna reguła klasyfikacji pewnych aspektów obserwowalnych obiektów, to nie ma sensu mówienie o pomiarze.

3. ELEMENTY FORMALNEJ TEORII POMIARU (za [14])

Reprezentacyjna teoria pomiaru [14] rozważa pomiar jako ustanowienie odpowiedniości pomiędzy zbiorem przejawów właściwości i relacji między nimi z jednej strony a zbiorem liczb i relacji między nimi z drugiej strony.

1. *Właściwość jako empiryczny system relacyjny*. Rozpatrzmy pewną właściwość (np. długość) i niech $q_1, q_2, \ldots, q_i, \ldots$ będą indywidualnymi przejawami tej właściwości. Zbiór wszystkich możliwych przejawów właściwości to:

$$Q = \{ q_1, q_2, \ldots, q_i, \ldots\}$$

Niech

$$\Omega = \{\omega_1, \omega_2, \ldots, \omega_i, \ldots\}$$

będzie klasą wszystkich obiektów przejawiających właściwości $q_1, q_2, \ldots, q_i, \ldots$ ze zbioru Q.

Załóżmy, że istnieje na Q zbiór $\mathcal{R}$ empirycznych relacji $R_1, R_2, \ldots, R_i, \ldots, R_n$, i oznaczmy:

$$\mathcal{R} = \{ R_1, R_2, \ldots, R_i, \ldots, R_n\}$$

Właściwość jest empirycznym systemem relacyjnym

$$\mathcal{I} = \langle Q, \mathcal{R} \rangle$$

2. *Liczbowy system relacyjny.*
Niech N będzie klasą liczb i niech

$$\mathcal{P} = \{P_1, P_2, \ldots, P_i, \ldots, P_n\}$$

[2] Dobre omówienie tego problemu znajduje się w [1].
[3] Zwykle jako dosłowne tłumaczenie angielskiego wyrazu *metrics*.

będzie zbiorem relacji określonych na N tak, że

$$\mathcal{N} = \langle N, \mathcal{P} \rangle$$

jest liczbowym systemem relacyjnym (zwykle $\mathcal{N}$ jest ciałem liczb rzeczywistych).

3. *Warunek reprezentatywności.*
Warunek ten wymaga, aby pomiar był ustalaniem odpowiedniości pomiędzy przejawami właściwości a liczbami w taki sposób, aby relacje pomiędzy przejawami właściwości implikowały relacje pomiędzy ich obrazami w zbiorze liczb i na odwrót.

Symbolicznie **pomiar** określamy jako obiektywną operację empiryczną:

$$M: Q \rightarrow N \qquad (1)$$

taką, że $\mathcal{I} = \langle Q, \mathcal{R} \rangle$ jest odwzorowane homomorficznie w $\mathcal{N} = \langle N, \mathcal{P} \rangle$ przez M i F. F jest jedno-jednoznacznym odwzorowaniem, z dziedziną $\mathcal{R}$ i przeciwdziedziną $\mathcal{P}$:

$$F: \mathcal{R} \rightarrow \mathcal{P}$$

tak, że można zapisać:

$$P_i = F(R_i); \qquad P_i \in \mathcal{P}; \qquad R_i \in \mathcal{R};$$

P jest n-członową relacją wtedy i tylko wtedy, jeżeli jest obrazem według F n-członowej relacji R. Homomorficzność odwzorowania oznacza, że dla każdego $R_i \in \mathcal{R}$ i każdego $P_i \in \mathcal{P}$ oraz $P_i = F(R_i)$ zachodzi związek:

$$R_i(q_1, ..., q_i, ..., q_n) \Leftrightarrow P_i[M(q_1), ..., M(q_i), ..., M(q_n)]$$

Pomiar jest homomorfizmem, ponieważ operacja M nie jest jedno-jednoznaczna, odwzorowuje ona mianowicie oddzielne, lecz nierozróżnialne przejawy w tę sama liczbę.

Uporządkowana czwórka

$$\mathcal{L} = \langle \mathcal{I}, \mathcal{N}, M, F \rangle \qquad (2)$$

nazywa się **skalą pomiarową** dla $n_i = M(q_i)$. Obraz q_i w N według M jest nazywany **miarą q_i według skali $\mathcal{L}$**.

W praktyce istnieje wiele sytuacji, w których obiekty realnego świata, ich cechy i charakterystyki są reprezentowane nie za pomocą liczb, lecz umownych symboli. Zdefiniujmy symbol jako przedmiot lub zdarzenie, które ma określony stosunek do pewnego bytu (przedmiotu lub zdarzenia innego rodzaju), umożliwiający ujawnienie o tym bycie informacji.

Niech Q będzie zbiorem bytów i niech $\mathcal{R}$ będzie pewnym zbiorem relacji na Q, tworzącym z nim system relacyjny:

$$\mathcal{I} = \langle Q, \mathcal{R} \rangle$$

Q może być zbiorem obiektów, zdarzeń, bytów abstrakcyjnych itp., a relacje zbioru R nie muszą mieć charakteru empirycznego. Niech Z będzie zbiorem przedmiotów lub zdarzeń, które będą użyte jako symbole, i niech $\mathcal{P}$ będzie zbiorem relacji określonych albo istniejących w Z i stanowiących wraz z nim system relacyjny:

$$\mathcal{Z} = \langle Z, \mathcal{P} \rangle$$

Wraz z F odwzorowującym $\mathcal{R}$ na $\mathcal{P}$, tak jak w przypadku pomiaru, można zdefiniować M jako odwzorowanie Q w (na) Z takie, że M i F odwzorowują $\mathcal{I}$ homomorficznie w (na) $\mathcal{Z}$.

Reprezentacja bytów Q symbolami Z ma postać:

$$\mathcal{K} = \langle \mathcal{I}, \mathcal{Z}, M, F \rangle \qquad (3)$$

Niech $Z_i = M(q_i)$ będzie obrazem q_i w Z według M. Wtedy Z_i jest nazywane symbolem q_i według $\mathcal{K}$ a q_i znaczeniem z_i według $\mathcal{K}$, natomiast $\mathcal{K}$ nazywa się **kodem** albo symbolizmem.

Przedstawiona w tym rozdziale teoria pomiaru może być stosowana zatem również w ogólniejszym przypadku reprezentacji za pomocą symboli. Takie reprezentacje **nie stanowią pomiarów**, ale mają z nimi zasadnicze cechy wspólne – najważniejszą cechą wyróżniającą pomiar jest to, że przyporządkowanie liczb w jego procesie jest obiektywne i reprezentuje fakty empiryczne.

4. DYSKUSJA WYMAGAŃ DEFINICJI POMIARU

Zagadnienia bezpieczeństwa teleinformatycznego należą do tych zagadnień, w których problemy pomiaru są trudne – istnieje wiele obiektywnych obserwacji eksperymentalnych i teorii jakościowych, przy czym nie ma możliwości przeprowadzenia pomiarów (podobnie jak w naukach społecznych i behawiorystycznych). Oprócz przedstawionych w kolejnych podrozdziałach wymagań definicji 1, należy mieć na uwadze, że z terminem „pomiar" związane są zwykle narzędzia pomiarowe. Oznacza to, że należałoby rozważyć nie tylko co i jak, ale także za pomocą czego (jakich narzędzi) będzie mierzone.

4.1. Określenie przedmiotu pomiaru

W zależności od przeznaczenia i konstrukcji systemu teleinformatycznego rozróżnia się zwykle tzw. *bezpieczeństwo na zewnątrz* oraz *bezpieczeństwo do wewnątrz*. Termin „bezpieczeństwo na zewnątrz" określa ochronę przed **zagrożeniami dla środowiska** (w tym dla człowieka) w którym pracuje system komputerowy, spowodowane nieprawidłowym działaniem tego systemu komputerowego. Dotyczy to głównie systemów sterowania (zwykle są to systemy czasu rzeczywistego), takich jak systemy monitorujące stan pacjenta w szpitalu, systemy kontroli działania elektrowni jądrowej, systemy nadzoru ruchu

kolejowego czy też systemy pokładowe np. samolotów. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie: niedopuszczania do katastrof [2]) określa się zwykle terminem *safety*.

Termin „bezpieczeństwo do wewnątrz" określa ochronę przed **zagrożeniami dla informacji** przechowywanej, przetwarzanej i przesyłanej w systemie teleinformatycznym. Dotyczy to głównie sieci teleinformatycznych banków, firm, organizacji naukowych itd. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie: niedopuszczania do utraty tajności, integralności, dostępności informacji) określa się zwykle terminem *security*.

Dalsze rozważania w niniejszej publikacji będą dotyczyły wyłącznie ostatniego typu bezpieczeństwa, nazywanego dalej bezpieczeństwem teleinformatycznym. Proponowana definicja tej nazwy [7] jest następująca:

Definicja 2

Termin **bezpieczeństwo teleinformatyczne** *oznacza poziom uzasadnionego*[4] *zaufania, że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych nie zostaną poniesione.*

Z definicji tej wynika, że bezpieczeństwo teleinformatyczne dotyczy **informacji** oraz pośrednio, jako środka przechowywania, przesyłania i przetwarzania informacji, **systemów teleinformatycznych**. Warto sobie uświadomić, że celem wszelkich działań z zakresu bezpieczeństwa teleinformatycznego jest ochrona informacji a nie komputerów.

Można zauważyć, że „bezpieczeństwo" nie jest ani obiektem, ani zdarzeniem (nie podpada więc pod podaną w rozdz. 2 definicję pomiaru) – to imponderabilia z dziedziny psychologii.

4.2. Przyporządkowanie liczb (miar)

Istnieje rozbieżność w poglądach co do tego, jakie przyporządkowanie liczbowe można uznać za pomiar. Uznawane, acz dyskutowane wciąż poglądy to [14]:

1) pomiarem jest każde empiryczne i obiektywne przyporządkowanie liczb, które opisuje przejawy właściwości (pogląd uznawany w naukach społecznych i behawiorystycznych);
2) pomiarem jest tylko takie przyporządkowanie liczb, które odwzorowują w pewien sposób stosunek przejawu właściwości do wielkości wzorcowej przyjętej za jednostkę miary (pogląd uznawany przez ogół techników i fizyków);
3) pomiarem może być tylko takie przyporządkowanie liczb, które implikuje przynajmniej empiryczny porządek przejawów właściwości, odpowiadający koncepcji uporządkowania według wielkości[5].

Warto zauważyć, że pogląd drugi wymaga ustalenia jednostki miary. Nasuwa się tutaj natychmiast pytanie, jaka jest jednostka miary „bezpieczeństwa"? Nie ma dotąd takiej jednostki, jaką np. dla napięcia jest *volt* [V] a dla natężenia prądu *amper* [A]. Zatem pogląd drugi, techniczny, w dziedzinie bezpieczeństwa teleinformatycznego nie ma racji bytu. Z przyczyn praktycznych należy odrzucić pogląd pierwszy na korzyść trzeciego, bo tylko on wymaga uporządkowania miar, niezbędnego np. w ocenie poziomu bezpieczeństwa.

Pomiary właściwości fizycznych, dla których można skonstruować empiryczne działanie dodawania, nazywa się pomiarami ekstensywnymi. W „bezpieczeństwie", podobnie jak w naukach społecznych, istnieje wiele właściwości, których nie można empirycznie dodawać, i których nie można wyprowadzić z wielkości addytywnych.

4.3. Obiektywność

Jak stwierdzono w rozdz.4.1, „bezpieczeństwo" nie jest ani obiektem, ani zdarzeniem (nie podpada więc pod podaną w rozdz. 2 definicję pomiaru). Ale obiektem może być system teleinformatyczny wraz ze środowiskiem eksploatacyjnym [4]. Wtedy „bezpieczeństwo" można uznać za jeden z „przejawów właściwości" takiego obiektu. Rzecz w tym, że co najmniej dyskusyjne jest mówienie o obiektywnej regule klasyfikacji bezpieczeństwa – zgodnie z definicją jest ono subiektywnym odczuciem, co najwyżej wspartym mało obiektywnymi przesłankami w postaci analizy ryzyka[6].

W technice przez obiektywność rozumie się, że **liczby** przyporządkowane właściwościom muszą być w granicach błędu, niezależnie od obserwatora. W dziedzinie bezpieczeństwa korzysta się zwykle nie z miar liczbowych a **symboli** (miar opisowych, np. określa się ryzyko jako wysokie, średnie lub niskie). Ze względu na rozmytość takich pojęć, wyniki uzyskiwane najczęściej na drodze ankietowania (tj. uzyskiwane od ludzi wypowiadających się na dany temat na podstawie swoich odczuć), nie spełniają kryterium obiektywności.

[4] Np. analizą ryzyka.

[5] Właściwość jest nazywana *wielkością*, jeżeli w jej empirycznym systemie relacyjnym znajduje się relacja porządkująca, która umożliwia uporządkowanie pojedynczych przejawów w sposób formalnie podobny do uporządkowania liczb przez relację równy, większy, mniejszy.

[6] Warto tutaj zauważyć, że warunek ten (obiektywność) nie jest spełniony np. przy podawaniu miar ryzyka (istotny element oceny „bezpieczeństwa"), gdy korzysta się z ocen ekspertów.

Zakładając, że wspomniane miary opisowe dotyczą one obiektów i zdarzeń, takich jak np. zasoby teleinformatyczne i incydenty naruszenia ustalonych zasad bezpieczeństwa, stosowane „mierzenie" dotyczy tej części formalizmu, który jest przedstawiony pod koniec rozdziału 3. Oznacza to, że nie używa się tutaj skal pomiarowych (w sensie wzoru 2) a jedynie oznaczania symbolicznego (w sensie wzoru 3).

4.4. Empiryczność

W rozdz. 4.2. uzasadniono wybór poglądu trzeciego jako odpowiedniego dla dziedziny bezpieczeństwa teleinformatycznego. Dyskusji wymaga używane w tym poglądzie stwierdzenie „ ... *empiryczny* porządek przejawów właściwości ...". Empiryzm oznacza tutaj, że:

- koncepcja właściwości mierzonej musi być oparta na relacji empirycznej. W zakresie bezpieczeństwa nie jest to spełnione, ponieważ definicja właściwości takiej jak „bezpieczeństwo" jest całkowicie arbitralna;
- „porządek przejawów właściwości" powinien wynikać z doświadczenia, a nie z arbitralnie przyjętych kryteriów klasyfikacyjnych. A zatem z tych samych powodów co w punkcie poprzednim, również „porządek przejawów właściwości" w dziedzinie bezpieczeństwa nie może być uznany za empiryczny (por. także różnorodne standardy z zakresu oceny bezpieczeństwa teleinformatycznego, takie jak Common Criteria, ITSEC, TCSEC)[7].

5. PODSUMOWANIE

Z przedstawionych w poprzednich rozdziałach rozważań wynika, że „bezpieczeństwo" jest niemierzalne w sensie pomiarów technicznych. W rozdziale 4 wypunktowano, że:

- bezpieczeństwo nie jest obiektem ani zdarzeniem, tylko kategorią psychologiczną. Mierzyć, w sensie technicznym, można tylko przejawy właściwości obiektów lub zdarzeń;
- w dziedzinie bezpieczeństwa operuje się miarami arbitralnymi a nie empirycznymi;
- miary są najczęściej symboliczne a nie liczbowe (z miar prostych wyprowadza się, por. np. [18], wskaźniki liczbowe, np. procentowe).

To, co faktycznie robi się w dziedzinie bezpieczeństwa teleinformatycznego, to **zbieranie danych stanowiące podstawę opracowania wskaźników na podstawie których będą wydawane sądy** o np. osiągnięciu (lub nie) założonych celów. Przykładem mogą być tutaj zapisy normy PN-I-02000: „Technika informatyczna. Zabezpieczenia w systemach informatycznych" gdzie jest podana jest definicja „oceny": *ocenianiem bezpieczeństwa informacji w systemach teleinformatycznych nazywa się proces określenia wartości miary gwarantowanej odporności systemu teleinformatycznego na czynniki mogące spowodować utratę tajności*[8]*, integralności i dostępności przetwarzanej w nim informacji.*

W tej samej normie wyjaśnia się, jak interpretowany jest termin **miara** (w kontekście *miary gwarantowanej odporności*; *assurance* w angielskojęzycznym oryginale). Otóż miara ta, to „pewność, że obiekt oceniany spełnia cele zabezpieczenia". Do tej definicji są dodane wyjaśnienia:

- że jest to *„właściwość obiektu ocenianego dająca podstawy, aby sądzić, że jego funkcje zabezpieczenia realizują politykę zabezpieczenia obiektu"*;
- że *„skuteczność i poprawność są głównymi aspektami pewności"*[9].

Zgodnie z ogólnie przyjętymi poglądami, **ocena** to sąd wartościujący, wszelka wypowiedź wyrażająca dodatnie lub ujemne ustosunkowanie się wypowiadającego do kogoś lub czegoś. Oceny są uwarunkowane psychicznie i społecznie, zmieniają się historycznie, zgodnie ze zmianami systemów wartości, do których należą.

Podaną za wspomnianą normą definicję można zatem rozpisać tak: osoba oceniająca ma się wypowiedzieć na temat skuteczności i poprawności spełniania funkcji zabezpieczenia przez obiekt oceniany. Ten proces wypracowywania oceny i samą ocenę zwykle nazywa się, jak wynika z dotychczasowych rozważań niepoprawnie, *pomiarem bezpieczeństwa*.

W kontekście diagnostyki technicznej warto zadać sobie pytanie czy, skoro bezpieczeństwo jest w sensie technicznym niemierzalne, można je diagnozować? Zdaniem autora tak, ale przechodząc z rozmytej kategorii „bezpieczeństwo" na bardziej precyzyjną „stan ochrony"[10] – można ustalić/zdefiniować stany ochrony i w procesie diagnozowania określić, jaki ze zdefiniowanych wcześniej stanów został osiągnięty.

Przykładem takiej diagnozy jest w dziedzinie bezpieczeństwa teleinformatycznego audyt informatyczny i audyt bezpieczeństwa teleinformatycznego [5], [6].

---

[7] ITSEC - Information Technology Security Evaluation Criteria.
TCSEC - Trusted Computer System Evaluation Criteria.

[8] Tajność opisuje stopień ochrony informacji jakiej ma ona podlegać. Stopień ten jest uzgadniany przez osoby lub organizacje dostarczające i otrzymujące informację (z tajnością jest ściśle związana *dotycząca ludzi* poufność, czyli prawo jednostki do decydowania o tym, jakimi informacjami chce się podzielić i jakie jest skłonna przyjąć).

[9] Warto skonfrontować te zapisy dotyczące miary z wymaganiami formalnej teorii pomiarów przedstawionej w rozdziale 3.

[10] Czyli przyjęcie manifestu Galileusza „uczynienia niemierzalnego mierzalnym".

LITERATURA

[1] Caseley P.: *Safety Process Measurement – a Review*. DSTL/CP06715 V1. UK. 2003.
[2] Jaźwiński J., Ważyńska-Fiok K.: *Bezpieczeństwo systemów*. PWN. Warszawa.1993.
[3] Liderman K.: *Miernictwo i diagnostyka systemów komputerowych*. WAT. Warszawa. 1994.
[4] Liderman K.: *System bezpieczeństwa teleinformatycznego*. Biuletyn IAiR. Nr 17.WAT. Warszawa. 2002.
[5] Liderman K., Patkowski A.:. *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*. Biuletyn IAiR. Nr 19. WAT. Warszawa. 2003.
[6] Liderman K.:. *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny" ?* Biuletyn IAiR. Nr 21. WAT. Warszawa. 2004.
[7] Liderman K.: *Podręcznik administratora bezpieczeństwa teleinformatycznego*. MIKOM. Warszawa. 2003. ISBN 83-7279-377-8
[8] Murdoch J.: *Security Measurement*. PSM White Paper, v.3.0. 13 Jan. 2006.
[9] Rozwadowski T.: *Diagnostyka techniczna obiektów złożonych*. WAT. Warszawa. 1983.
[10] Stokalski A.: *Elementy teoretycznych podstaw inżynierii procesów przetwarzania informacji*. Dodatek do biuletynu WAT. Warszawa. 1982.
[11] Stoneburner, G.,:NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001, NIST.
[12] Swanson, M., *et al.*: NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003, NIST.
[13] Swanson, M., *et al.*: NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*.
[14] Sydenham P.H. (red.): *Podręcznik metrologii*. WKŁ. Warszawa. 1988
[15] Szewczyk A.: *Diagnostyka systemów informacyjnych*. *Problemy podstawowe*. W: Informatyka 11/92.
[16] Wang Ch., Wulf W.: *Towards a framework for security measurement*. Dep. of Comp. Sc. University of Virginia.
[17] Żurakowski Z.: *Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem*. Str.20-28. W: Informatyka, nr 3. 1995.
[18] Corporative Information Security Working Group: *Report of a best practices and metrics team*. 10 January 2005.
[19] PN-I-02000: *Technika informatyczna. Zabezpieczenia w systemach informatycznych*. 1998.
[20] ISO/IEC 21827 (v.3.0): *System Security Engineering Capability Maturity Model (SSE-CMM).*

Krzysztof LIDERMAN, absolwent Wojskowej Akademii Technicznej, jest mianowanym adiunktem w Instytucie Teleinformatyki i Automatyki WAT. W swojej pracy naukowej i dydaktycznej zajmował się projektowaniem systemów komputerowych oraz teorią i praktyką systemów eksperckich. Od ponad 10 lat swoje zainteresowania ukierunkowuje na bezpieczeństwo teleinformatyczne.

Autor książek *„Projektowanie systemów komputerowych"* i *„Podręcznik administratora bezpieczeństwa teleinformatycznego"* oraz licznych publikacji naukowych oraz popularyzatorskich z bezpieczeństwa teleinformatycznego.