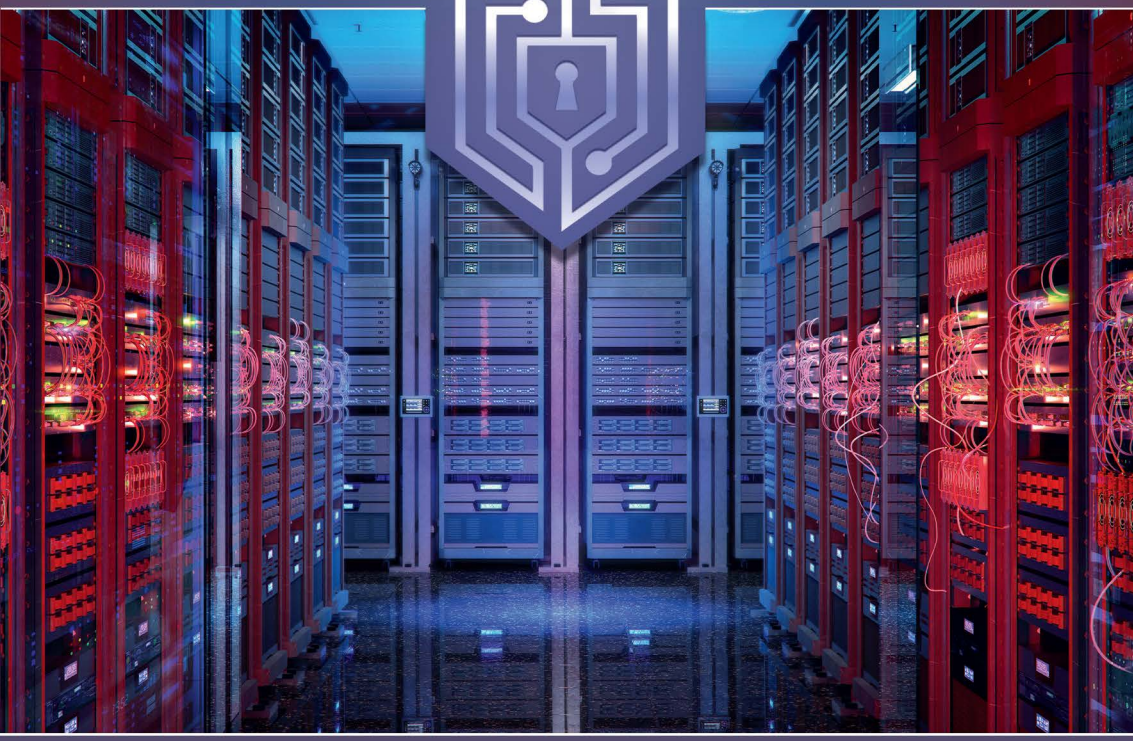
Przemysław Jatkiewicz

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH FIRM I INSTYTUCJI



Wydawnictwo Uniwersytetu Gdańskiego

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH FIRM I INSTYTUCJI

Przemysław Jatkiewicz

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH FIRM I INSTYTUCJI

Wydawnictwo Uniwersytetu Gdańskiego
Gdańsk 2020

Recenzent
prof. dr hab. Zdzisław Szyjewski

Redaktor Wydawnictwa
Jerzy Toczek

Projekt okładki i stron tytułowych
Filip Sendal

Ilustracja na okładce
Corona Borealis z zasobów Adobe Stock

Skład i łamanie
Mariusz Szewczyk

Publikacja sfinansowana ze środków Katedry Informatyki Ekonomicznej
Wydziału Zarządzania Uniwersytetu Gdańskiego

ISBN 978-83-8206-136-9

Wydawnictwo Uniwersytetu Gdańskiego
ul. Armii Krajowej 119/121, 81-824 Sopot
tel.: 58 523 11 37; 725 991 206
e-mail: wydawnictwo@ug.edu.pl
www.wyd.ug.edu.pl

Księgarnia internetowa: www.kiw.ug.edu.pl

Druk i oprawa
Zakład Poligrafii Uniwersytetu Gdańskiego
ul. Armii Krajowej 119/121, 81-824 Sopot
tel. 58 523 14 49

Spis treści

Wstęp

W dobie społeczeństwa informacyjnego zarządzanie bezpieczeństwem informacji jest kluczowym elementem pozwalającym funkcjonować instytucjom oraz przedsiębiorcom. Zapewnienie poufności, integralności oraz dostępności informacji wynika z przepisów prawa, a także warunkuje poprawne i efektywne realizowanie prowadzonych działań.

Zespół CERT Polska (ang. Computer Emergency Response Team) działający w strukturach NASK przyjął w 2018 r. zgłoszenie 19 439 incydentów związanych z bezpieczeństwem systemów informatycznych. W stosunku do poprzedniego roku odnotowano 17% wzrost[1]. Z kolei Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, odnotował w tym samym roku aż 31 865 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych w sieciach znajdujących się w obszarze swoich kompetencji[2]. Kompetencje te dotyczą zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa, systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w ustawie o zarządzaniu kryzysowym[3].

[1] *Raport roczny z działalności CERT Polska 2018*, CERT Polska, Warszawa 2019.

[2] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*, CSIRT GOV, Warszawa 2019.

[3] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2020 r., poz. 1856).

Badania przeprowadzone przez Vecto sp. z o.o w 2019 r. wśród polskich przedsiębiorców wykazały, że 46% respondentów zetknęło się z cyberatakiem[4]. Raport firmy PricewaterhouseCoopers wskazuje, iż incydenty zakłóciły działanie lub doprowadziły do przestojów 62% badanych firm, a 44% z nich poniosło z tego tytułu straty finansowe[5]. Równocześnie 85% konsumentów twierdziło, że nie zamierza współpracować z firmą, która nie będzie w stanie przekonać ich, że powierzone jej dane są odpowiednio zabezpieczone[6].

Temat zarządzania bezpieczeństwem informacji obejmuje szerokie spektrum zagadnień dotyczących aspektów technicznych i organizacyjnych. Publikacja skupia się na bezpieczeństwie serwerów jako głównego elementu systemu informatycznego. Jak wskazują badania przeprowadzone przez firmę One System, w lipcu 2019 r. jedynie 5% małych i średnich firm nie posiadało fizycznego serwera, a jednocześnie aż 67% miało ich więcej niż jedną sztukę[7]. Brak fizycznego serwera nie świadczy jednoznacznie o tym, iż firmy nie korzystają z rozwiązań serwerowych w postaci usług chmurowych, elektronicznej administracji czy też innych zasobów sieci Internet.

Znaczna część przykładów zawartych w tekście dotyczy serwerów opartych o system operacyjny z rodziny Linux. Wybór ten nie jest przypadkowy, gdyż Linux uważany jest za system znacznie bardziej bezpieczny niż Windows. Marynarka Wojenna USA i Amerykańskie Siły Powietrzne po serii ataków na swoje systemy informatyczne zdecydowały się na migrację z Windows na Linuxa.

Chociaż jedynie 2% użytkowników komputerów klasy PC korzysta z tego systemu, to już 100% komputerów superkomputerów (ang. *mainframe*) pracuje pod kontrolą systemu Linux[8]. Równocześnie zdecydowana większość serwerów WWW także oparta jest o Linuxa. W urządzeniach IoT (ang. Internet of Things), np. komputerach samochodowych czy telewizorach,

[4] *Cyberbezpieczeństwo w polskich firmach*, Vecto, Warszawa 2020.

[5] *Cyber-ruletka po polsku. 5. edycja Badania Stanu Bezpieczeństwa Informacji*, PWC, Warszawa 2018.

[6] *Consumer Intelligence Series: Protect.me*, PWC, London 2017.

[7] *Bezpieczeństwo przechowywania danych w MŚP*, One System, Warszawa 2019.

[8] https://www.top500.org/statistics/sublist/ [dostęp: 4.03.2020].

również stosowane są systemy oparte o jądro Linux. Na jądrze tym oparty jest Android, zainstalowany na 90% smartfonów[9], jak i MacOS.

W rozdziale 1 omówiono pojęcia i definicje związane z bezpieczeństwem informacji. Przytoczono szereg norm, do których odwołują się obowiązujące akty prawne. Przedstawiono klasyfikacje zagrożeń oraz metodyki analizy ryzyka. Rozdział 2 opisuje środowisko pracy serwerów w rozumieniu sprzętowym i programowym. Zaprezentowano w nim stosowane obecnie technologie i miary niezawodności. Omówiono zagadnienia związane z infrastrukturą wspomagającą pracę serwerowych urządzeń oraz wyszczególniono podstawowe serwery świadczące usługi sieciowe. Kolejny 3 rozdział obejmuje techniki uwierzytelniania w systemie operacyjnym. Zaprezentowano w nim metody ochrony haseł z uwzględnieniem algorytmów kryptograficznych, a także techniki biometryczne i behawioralne. Rozdział 4 zawiera zagadnienia ochrony zasobów sprzętowych serwera oraz zawartych w nim danych. Przedstawiono systemy plików i zawarte w nich mechanizmy kontroli dostępu. Podano także przykłady związane z ograniczeniem dostępu do zasobów oraz poddano analizie ich skuteczność. Całość rozdziału 5 poświęcono szkodliwemu oprogramowaniu. Zaprezentowano sposób działania i źródła infekcji. Przytoczono raporty i dane dotyczące obecnych zagrożeń związanych ze złośliwym oprogramowaniem. Uwagę poświęcono też zjawisku spamu i phishingu. Zanalizowano mechanizmy pozwalające na wykrycie zainfekowanych plików oraz ich skuteczność w odniesieniu do stosowanych przez przestępców metod przeciwdziałania wykryciu. W ostatnim rozdziale umieszczono informację o wykonywaniu kopii bezpieczeństwa, które stanowią końcową linię obrony przed cyberzagrożeniami. Wyszczególniono metody wykonywania kopii, stosowane nośniki i urządzenia oraz strategie rotacji nośników. Rozdział ten zawiera również omówienie metod bezpiecznego usuwania danych i ich skuteczność w odniesieniu do różnych nośników.

[9] https://mobirank.pl/2019/05/27/udzial-wersji-systemu-android-w-maju-2019-r/ [dostęp: 4.03.2020].

Rozdział 1
Pojęcia i definicje

Celem dogłębnego i poprawnego zrozumienia zagadnień bezpieczeństwa związanego z szeroko pojętą informatyką należy zapoznać się ze stosowaną w literaturze oraz praktyce terminologią. Już samo bezpieczeństwo jest pojęciem polisemantycznym i zależnym od dziedziny wiedzy. W naukach społecznych utożsamiane jest jako stan pewności, spokoju, zabezpieczenia oraz jego poczucia, jak również brak zagrożenia oraz ochrona przed niebezpieczeństwami[10]. W informatyce przyjęto definicję związaną z bezpieczeństwem informacji zawartą w normie ISO 17799, według której jest to zachowanie trzech najważniejszych jej atrybutów, tj.[11]:

- poufności (ang. *confidentiality*),
- integralności (ang. *integrity*),
- dostępności (ang. *availability*).

Dodatkowo mogą być brane pod uwagę dodatkowe własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Najnowsze wydania norm odwołują się jednak do definicji zawartej w ISO 20000, która zastępuje termin dostępność terminem osiągalność, przy czym niezmienne pozostaje jego znaczenie jako zapewnienie, że osoby upoważnione mają dostęp do informacji i aktywów zawsze wtedy, gdy są im one potrzebne[12]. Aktywa (ang. *assets*) to wszystko co ma wartość dla organizacji, a zwłaszcza sprzęt i oprogramowanie. Integralność oznacza

[10] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych Polskiej Akademii Nauk, Warszawa 1996.

[11] PN-ISO/IEC 17799, *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2003.

[12] PN-ISO/IEC 20000-1, *Technika informatyczna. Zarządzanie usługami,* część 1: *Wymagania dla systemu zarządzania usługami*, Polski Komitet Normalizacyjny, Warszawa 2014.

dokładność i kompletność aktywów, a poufność – własność polegającą na braku dostępu do nich dla nieupoważnionych podmiotów, osób lub procesów. Spośród wymienionych dodatkowych atrybutów informacji na uwagę zasługuje zwłaszcza rozliczalność (ang. *accountability*), która stanowi wymóg krajowych przepisów. Jest to właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie[13].

Terminem niezawodność (ang. *reliability*) oznacza się gwarancję oczekiwanego zachowania systemu oraz otrzymanych wyników. Autentyczność (ang. *authenticity*) natomiast to własność polegająca na tym, że pochodzenie lub zawartość obiektu informatycznego (program, dane) są takie jak deklarowane, a niezaprzeczalność to brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie[14].

Kolejne atrybuty związane z bezpieczeństwem informacji znaleźć można w standardzie COBIT (ang. Control Objectives for Information and Related Technology)[15]:

- efektywność (ang. *effectiveness*) – zapewnienie informacji istotnej, stosownej i użytecznej oraz dostarczenie jej na czas w poprawnej i spójnej formie,
- wydajność (ang. *efficiency*) – dostarczenie informacji z wykorzystaniem dostępnych zasobów w sposób optymalny (ekonomiczny),
- zgodność (ang. *compliance*) – uwzględnia wymagania narzucone na organizację przez podmioty zewnętrzne, prawo, rozporządzenia, umowy oraz określone wymagania i polityki wewnętrzne,

Następnym niejednoznacznym pojęciem jest informacja, którą często utożsamia się mylnie z danymi. Zestawienie najczęściej stosowanych definicji zostało zaprezentowane w tabeli 1.1.

[13] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz. U. Nr 93, poz. 545).

[14] PN-I 02000, *Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.* Polski Komitet Normalizacyjny, Warszawa 2002.

[15] *Control Objectives for Information and Related Technology (COBIT) 4.0*, IT Governance Institute, Rolling Meadows, IL 2005.

Tabela 1.1. Definicje danych i informacji

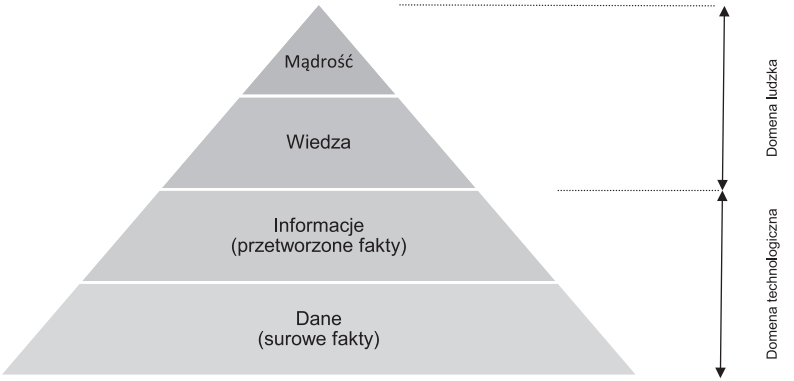
Autorzy	Definicje danych	Definicje informacji
Avison i Fitzgerald (1995)	Dane reprezentują nieustrukturyzowane fakty	Informacja ma znaczenie, pochodzi z wyselekcjonowania danych, ich podsumowania i prezentacji w taki sposób, by były użyteczne dla odbiorcy
Clare i Loucopoulos (1987)	Fakty zgromadzone z obserwacji lub zapisów dotyczących zjawisk, obiektów lub ludzi	Wymagania do podejmowania decyzji. Informacje są produktem istotnego przetwarzania danych
Galland (1982)	Fakty, koncepcje lub wyniki w postaci, która może być komunikowana i interpretowana	Informacje to to, co powstaje w wyniku pewnych działań myślowych człowieka (obserwacji, analiz) z sukcesem zastosowanych do danych, by odkryć ich istotę lub znaczenie
Hicks (1993)	Reprezentacja faktów, koncepcji lub instrukcji w sposób sformalizowany, umożliwiający komunikowanie, interpretację lub przetwarzanie przez ludzi lub urządzenia automatyczne	Dane przetworzone tak, by miały znaczenie dla decydenta w konkretnej sytuacji decyzyjnej
Knight i Silk (1990)	Numery reprezentujące obserwowalne obiekty lub zagadnienia (fakty)	Znaczenie dla człowieka związane z obserwowanymi obiektami i zjawiskami
Laudon i Laudon (1991)	Surowe fakty, które mogą być kształtowane i formowane, by stworzyć informacje	Dane, które zostały ukształtowane lub uformowane przez człowieka w istotną i użyteczną postać
Maddison (1989)	Język naturalny: podane fakty, z których inni mogą dedukować, wyciągać wnioski. Informatyka: znaki lub symbole, w szczególności w transmisji w systemach komunikacji i w przetwarzaniu w systemach komputerowych; zwykle choć nie zawsze reprezentujące informacje, ustalone fakty lub wynikającą z nich wiedzę; reprezentowane przez ustalone znaki, kody, zasady konstrukcji i strukturę	Zrozumiała, użyteczna, adekwatna komunikacja w odpowiednim czasie; jakikolwiek rodzaj wiedzy o rzeczach i koncepcjach w świecie dyskusji, która jest wymieniana pomiędzy użytkownikami; to treść, która ma znaczenie, a nie jej odwzorowanie

Tabela 1.1 cd.

Autorzy	Definicje danych	Definicje informacji
Martin i Powell (1992)	Surowce życia organizacji; składają się z rozłącznych numerów, słów, symboli i sylab odwołujących się do zjawisk i procesów biznesu	Informacje pochodzą z danych, które zostały przetworzone, tak by stały się użyteczne w podejmowaniu decyzji w zarządzaniu

Źródło: M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, z. 798, s. 99–116.

Z tabeli 1.1 jasno wynika różnica pomiędzy danymi i informacją. Informacja leży na wyższym poziomie abstrakcji powstałym na skutek przetworzenia danych. Część z definicji wiąże jednak uzyskanie informacji z działaniami natury ludzkiej. Współczesne systemy informatyczne nie służą jednak wyłącznie gromadzeniu danych, lecz pozwalają na ich segregowanie, łączenie, a nawet – w przypadku systemów z zaimplementowanymi mechanizmami sztucznej inteligencji – wyciąganiu wniosków. Dlatego też warstwę danych i informacji w modelu DIKW (ang. Data-Information-Konowledge-Wisdom) należy łączyć z domeną technologiczną, co zostało zaprezentowane na rysunku 1.1.



Rysunek 1.1. Piramida wiedzy

Źródło: W. Grudzewski, I. Hajduk, *Zarządzanie wiedzą w przedsiębiorstwach*, Difin, Warszawa 2004.

Kolejnymi pojęciami związanymi z bezpieczeństwem informacji, które należy rozróżnić, to zdarzenie oraz incydent. Zdarzeniem jest stan systemu, usługi lub sieci, który wskazuje na możliwość naruszenia norm, przepisów czy też wewnętrznych regulacji, błąd lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem. Pojedyncze zdarzenie lub seria niepożądanych lub nieoczekiwanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, określane jest mianem incydentu. Kluczem pozwalającym odróżnić zdarzenie od incydentu jest prawdopodobieństwo wywołania negatywnych skutków, które dla incydentu winno być wysokie, choć niekoniecznie musi przerodzić się w pewność. Mylne jest więc utożsamianie incydentu ze zrealizowanym zagrożeniem rozumianym jako przyczyna incydentu.

Przykładowymi zdarzeniami i incydentami związanymi z bezpieczeństwem są:

- utrata dostępu do aktywów,
- niepoprawne działanie systemu informatycznego,
- błędy ludzkie,
- niezgodność z zaleceniami czy regulacjami,
- naruszenie dostępu.

W 2018 r. rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL (obecnie CSIRT GOV) przyjął zgłoszenia 19 439 incydentów, spośród których 3739 zostało sklasyfikowanych i uznanych za poważne. Szczegółowe informacje zaprezentowano w tabeli 1.2.[16] Należy zauważyć, że rzeczywista liczba incydentów znacznie przekracza liczby wykazane przez CERT, gdyż zbiera on informacje głównie od instytucji.

W literaturze przedmiotu występuje wiele różnych klasyfikacji zagrożeń bezpieczeństwa informacji. Najbardziej ogólnym jest podział ze względu na lokalizację ich źródła[17]:

- wewnętrzne (powstające wewnątrz organizacji), obejmujące zagrożenie utratą, uszkodzeniem lub brakiem dostępu do danych, spowodowane błędem, przypadkiem albo celowym działaniem nieuczciwych użytkowników,

[16] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska 2018*, NASK/CERT Polska, Warszawa 2019.

[17] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Abrys, Poznań 2000.

- zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu,
- fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe.

Tabela 1.2. Incydenty obsłużone przez CERT Polska według typów

Typ incydentu	Liczba incydentów	%
Obraźliwe i nielegalne treści	431	11,53
Złośliwe oprogramowanie	862	23,05
Gromadzenie informacji	101	2,70
Próby włamań	153	4,09
Włamania	125	3,34
Dostępność zasobów	49	1,31
Atak na bezpieczeństwo informacji	46	1,23
Oszustwa komputerowe	1878	50,23
Podatne usługi	69	1,85
Inne	25	0,67

Źródło: Opracowanie własne na podstawie *Krajobraz bezpieczeństwa polskiego internetu…*

Przytoczona powyżej klasyfikacja jest obecnie coraz trudniejsza do zastosowania, gdyż współczesne systemy informacyjne, a w szczególności systemy instytucji publicznych, użytkowane są przez szeroką rzeszę użytkowników spoza organizacji będącej właścicielem systemu. Ze względu na publiczne przeznaczenie systemu nie można ich nazwać osobami trzecimi. Równie problematyczne jest wydzielenie zagrożenia fizycznego. Awarie czy wypadki mogą być skutkiem działania lub zaniechania działania zarówno użytkowników, jak i osób trzecich. Bezzasadny wydaje się również rozdział systemu informacyjnego oraz urządzeń sieciowych. Na system informacyjny składają

się sprzęt komputerowy, oprogramowanie, bazy danych, urządzenia i środki łączności, ludzie i procedury[18].

Bardziej szczegółowy katalog zagrożeń opracował Rządowy Zespół Reagowania na Incydenty Komputerowe, który został zaprezentowany na rysunku 1.2. Oprócz zagrożeń wymieniane są w nim również podatności (ang. *vulnerability*).

Z uwagi na fakt, że podatności zdefiniowane są jako słabości aktywów umożliwiające realizację zagrożeń, powyższa klasyfikacja jest błędna. Zawarte w niej podatności stanowią w większości uszczegółowienie zagrożeń. Przykładowo podatnością zagrożenia złośliwym oprogramowaniem jest brak systemu antywirusowego lub aktualnej bazy sygnatur, o czym więcej napisano w rozdziale 6.

Katalog zagrożeń CERT.GOV.PL						
ZAGROŻENIA		PODATNOŚCI				
1. DZIAŁANIA CELOWE	1.1 – OPROGRAMOWANIE ZŁOŚLIWE	1.1.1 – wirus	1.1.2 – robak sieciowy	1.1.3 – koń trojański	1.1.4 – dialer	1.1.5 – klient botntu
	1.2 – PRZEŁAMANIE ZABEZPIECZEŃ	1.2.1 – nieuprawnione logowania	1.2.2 – włamanie na konto/ ataki siłowe		1.2.3 – włamanie do aplikacji	
	1.3 – PUBLIKACJE W SIECI INTERNET	1.3.1 – treści obraźliwe	1.3.2 – pomawianie (zniesławienie)	1.3.3 – naruszenie praw autorskich		1.3.4 – dezinformacja
	1.4 – GROMADZENIE INFORMACJI	1.4.1 – skanowanie	1.4.2 – podsłuch	1.4.3 – inżynieria społeczna	1.4.4 – szpiegostwo	1.4.5 – SPAM
	1.5 – SABOTAŻ KOMPUTEROWY	1.5.1 – nieuprawniona zmiana informacji		1.5.2 – nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji		
	1.6 – CZYNNIK LUDZKI	1.6.1 – naruszenie procedur bezpieczeństwa		1.6.2 – naruszenie obowiązujących przepisów prawnych		
	1.7 – CYBERTERRORYZM	1.7.1 – przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni				
2. DZIAŁANIA NIECELOWE	2.1 – WYPADKI I ZDARZENIA LOSOWE	2.1.1 – awarie sprzętowe	2.1.2 – awaria łącza	2.1.3 – awarie (błędy) oprogramowania		
	2.2 – CZYNNIK LUDZKI	2.2.1 – naruszenie procedur	2.2.2 – zaniedbanie	2.2.3 – błędna konfiguracja urządzenia	2.2.4 – brak wiedzy	2.2.5 – naruszenie praw autorskich

Rysunek 1.2. Katalog zagrożeń CERT.GOV.pl

Źródło: http://www.cert.gov.pl [dostęp 5.05.2018].

[18] A. Januszewski, *Funkcjonalność informatycznych systemów zarządzania: zintegrowane systemy transakcyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Jednym z zagrożeń zawartych w katalogu CERT jest cyberterroryzm związany z pojęciami cyberprzestrzeni i cyberbezpieczeństwa. Według ustawy o krajowym systemie cyberbezpieczeństwa cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[19]. Geneza pojęcia cyberprzestrzeni sięga lat 80. XX wieku i wywodzi się z literatury science fiction. Nadal utożsamiane jest z rzeczywistością wirtualną[20]. Według przepisów prawa przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne („system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego"[21]), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[22].

Analizując różne definicje, Janusz Wasilewski dokonał trafnego uogólnienia, wskazując, że cyberbezpieczeństwo jest wydzielonym logicznie obszarem – cyfrową domeną przetwarzania oraz wymiany informacji. Przestrzeń ta, mająca charakter ponadnarodowy, jest tworzona przez systemy teleinformatyczne połączone za pośrednictwem sieci telekomunikacyjnych, w tym sieci, których elementy infrastrukturalne są zlokalizowane na terenie innych państw[23].

[19] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369 ze zm.).

[20] W. Gogołek, W. Cetera, *Leksykon tematyczny: zarządzanie IT*, Wydział Dziennikarstwa i Nauk Politycznych, Uniwersytet Warszawski, Warszawa 2014.

[21] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2020 r., poz. 346 ze zm.).

[22] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323).

[23] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*. „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 5(9), s. 225–234.

Najbardziej trafną klasyfikację zarówno zagrożeń, jak i podatności zawiera norma ISO 27005[24]. Przedstawione w niej podatności odnoszą się wprost do rodzajów aktywów i podatności. Szczegółowe informacje zostały zaprezentowane w tabelach 1.3 i 1.4.

Tabela 1.3. Typy zagrożeń według ISO 27005

Rodzaj	Zagrożenie
Zniszczenia fizyczne	• pożar, zalanie, zanieczyszczenie, pył, korozja, wychłodzenie • poważny wypadek, zniszczenie urządzeń lub nośników
Zjawiska naturalne	• zjawiska klimatyczne • zjawiska sejsmiczne • zjawiska wulkaniczne • zjawiska pogodowe, powódź
Utrata podstawowych usług	• awarie systemu klimatyzacji • utrata dostaw prądu • awaria urządzenia telekomunikacyjnego
Zakłócenia spowodowane promieniowaniem	• promieniowanie elektromagnetyczne • promieniowanie cieplne
Naruszenie bezpieczeństwa informacji	• przechwycenie sygnałów na skutek zjawiska interferencji • szpiegostwo zdalne, podsłuch • kradzież nośników, dokumentów, sprzętu • ujawnienie, odtwarzanie z powtórnie wykorzystanych lub wyrzuconych nośników • dane z niewiarygodnych źródeł • manipulowanie urządzeniem • sfałszowanie oprogramowania • detekcja umiejscowienia
Awarie techniczne	• awaria urządzenia lub niewłaściwe jego funkcjonowanie • przeciążenie systemu informacyjnego • niewłaściwe funkcjonowanie oprogramowania • naruszenie zdolności utrzymania systemu informacyjnego

[24] PN-ISO/IEC 17799, *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji,* Polski Komitet Normalizacyjny, Warszawa 2003.

Tabela 1.3. cd.

Rodzaj	Zagrożenie
Nieautoryzowane działania	• nieautoryzowane użycie urządzeń • nieuprawnione kopiowanie oprogramowania • nielegalne przekształcanie danych lub ich zniekształcanie
Naruszenie bezpieczeństwa funkcji	• błąd użytkownika • naruszenie lub fałszowanie praw • odmowa działania • naruszenie dostępności personelu

Źródło: Opracowanie własne na podstawie załącznika C normy ISO 27005.

Tabela 1.4. Przykłady podatności i zagrożeń w odniesieniu do aktywów

Rodzaj aktywów	Przykład podatności	Przykład zagrożeń
Sprzęt	• brak planów okresowej wymiany	• zniszczenie urządzeń lub nośników
	• niewystarczające utrzymanie/ błędna instalacja	• naruszenie zdolności utrzymania systemu informacyjnego
	• wrażliwość na zmiany napięcia	• utrata zasilania
Oprogramowanie	• skomplikowany interfejs użytkownika	• błąd użytkowania
	• brak wylogowania po zaprzestaniu używania stacji roboczej	• nadużycie praw
	• brak skutecznej kontroli zmian	• niewłaściwe funkcjonowanie oprogramowania
Sieć	• przesyłanie haseł jawnym tekstem	• szpiegostwo zdalne
	• niezabezpieczone połączenie z siecią publiczną	• nieautoryzowane użycie urządzeń
	• brak identyfikacji i uwierzytelnienia nadawcy i odbiorcy	• fałszowanie praw
Personel	• niewystarczające szkolenie	• błąd użytkowania
	• brak mechanizmów monitorowania	• nielegalne przetwarzanie danych
	• praca personelu zewnętrznego bez nadzoru	• kradzież nośników i dokumentów

ISBN 978-83-8206-136-9