Maciej Szmit

Systemy Zarządzania Bezpieczeństwem Informacji

Wybrane zagadnienia zarządzania cyfrową gotowością śledczą

Systemy Zarządzania Bezpieczeństwem Informacji

Wybrane zagadnienia zarządzania cyfrową gotowością śledczą

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Maciej Szmit

Systemy Zarządzania Bezpieczeństwem Informacji

Wybrane zagadnienia zarządzania cyfrową gotowością śledczą

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Łódź 2025

Maciej Szmit (ORCID: 0000-0002-6115-9213)
Uniwersytet Łódzki, Wydział Zarządzania, Katedra Informatyki
90-237 Łódź, ul. Matejki 22/26

RECENZENCI
Piotr Niedzielski, Anna Sołtysik-Piorunkiewicz

REDAKTOR INICJUJĄCA
Monika Borowczyk

REDAKCJA
Monika Baranowska

SKŁAD I ŁAMANIE
PAJ-Press

KOREKTA TECHNICZNA
Wojciech Grzegorczyk

PROJEKT OKŁADKI
Polkadot Studio Graficzne
Aleksandra Woźniak, Hanna Niemierowicz
Zdjęcie wykorzystane na okładce: Freepik.com/macrovector

https://doi.org/10.18778/8331-902-5

Wydane przez Wydawnictwo Uniwersytetu Łódzkiego
Wydanie I. W.11675.25.0.M
Ark. wyd. 7,0; ark. druk. 7,875

ISBN 978-83-8331-901-8
e-ISBN 978-83-8331-902-5

Wydawnictwo Uniwersytetu Łódzkiego
90-237 Łódź, ul. Jana Matejki 34A
www.wydawnictwo.uni.lodz.pl
e-mail: ksiegarnia@uni.lodz.pl
tel. 42 635 55 77

Spis treści

Wstęp

Problematyka związana z zarządzaniem bezpieczeństwem informacji ma charakter multidyscyplinarny i interdyscyplinarny[1]. Dla podejmującego się badania dotyczących jej zagadnień jednym z pierwszych zadań jest wybór przedmiotu formalnego, który implikował będzie umiejscowienie prowadzonych badań w obrębie odpowiedniej dyscypliny naukowej lub na pograniczu takich dyscyplin. Oczywiście z metodologicznego punktu widzenia istotne jest nie samo formalne przyporządkowanie, ale określenie interesującego aspektu badanego zjawiska, który w konsekwencji decyduje m.in. o wyborze właściwych dla danej dyscypliny metod, narzędzi i technik badawczych.

Będące przedmiotem materialnym poniższych rozważań zagadnienia cyfrowej gotowości śledczej (*digital forensic readiness*, DFR), można – jak się wydaje – rozpatrywać z punktu widzenia co najmniej pięciu dyscyplin należących do dwóch dziedzin nauki[2]: inżynierii bezpieczeństwa oraz informatyki technicznej i telekomunikacji (dziedzina nauk inżynieryjno-technicznych); nauk prawnych, nauk o bezpieczeństwie, nauk o zarządzaniu i jakości (dziedzina nauk społecznych). W niniejszej monografii[3] zagadnienia te rozpatrywane są z punktu widzenia

---

1 Zob. np.: L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, EAS, Kraków 2008, s. 47; M. Szmit, *Cyberbezpieczeństwo jako zagadnienie interdyscyplinarne*, [w:] M. Chrabkowski, C. Tatarczuk, J. Tomaszewski, W. Wosek (red.), *Bezpieczeństwo w administracji i biznesie jako czynnik europejskiej integracji i rozwoju*, WSAiB, Gdynia 2015, s. 391–413; S. Sudoł, *Zarządzanie jako dyscyplina naukowa*, „Przegląd Organizacji" 2016, nr 4(915), s. 4; W. Czakon, M. Komańda (red.), *Interdyscyplinarność w naukach o zarządzaniu*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2011 (passim).

2 Zob. Rozporządzenie Ministra Edukacji i Nauki z dnia 11 października 2022 r. (Dz. U. z 2022 r. poz. 2202).

3 Uwarunkowania i problemy natury kryminalistycznej i informatycznej zostały poruszone we wcześniejszych publikacjach autora, w szczególności: M. Szmit, *O stanowczości opinii biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2022, s. 149–155; idem, *Jeszcze o statusie i odpowiedzialności biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2022, s. 211–223; idem, *O owocach zatrutego drzewa i kategoryczności opinii biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2019, s. 27–38; idem, *Zjawisko plagiatu programu komputerowego z punktu widzenia biegłego informatyka*, [w:] I. Staniec (red.), *Natura i uwarunkowania ryzyka*, Wydawnictwo Politechniki Łódzkiej, Łódź 2014, s. 338–348; idem, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, wyd. II rozszerzone i uzupełnione, Polskie Towarzystwo

zarządzania (a więc formalnie dyscypliny „nauki o zarządzaniu i jakości"): zarządzania organizacją, której dotyczy zdarzenie, zwłaszcza zdarzenie związane z bezpieczeństwem informacji i zarządzania wybranymi elementami procesu obsługi tego zdarzenia, przy czym nie zajmowano się tutaj szczegółowo procesami reakcji na incydent w ogólności, ale przygotowaniem organizacji na sytuacje, w których na skutek wystąpienia incydentu bezpieczeństwa informacji lub z innych powodów konieczne jest przeprowadzenie śledztwa z badaniem cyfrowych śladów dowodowych oraz nadzorem zarządczym nad ryzykiem związanym z koniecznością wykorzystania przez organizację specyficznych metod informatyki śledczej.

Organizacja może odgrywać w tym zdarzeniu różne role: może być (czy to ona sama jako podmiot, czy też jej pracownicy) ofiarą incydentu bezpieczeństwa, może być miejscem jego wystąpienia, zarówno *sensu stricto*, np. gdy ma miejsce na terenie siedziby organizacji, jak i – gdy mowa o zasobach informatycznych – np. gdy mowa o nieuprawnionym dostępie do danych informatycznych stanowiących własność organizacji, ale znajdujących się „w chmurze", poza jej siedzibą, może wreszcie sama taki incydent spowodować, czy to przez złą wolę, czy lekkomyślność, czy też przez niedbalstwo swoich pracowników. Poza tematyką rozważaną w pracy pozostaje sytuacja, w której sama organizacja w sposób celowy i świadomy generuje incydenty bezpieczeństwa, co obejmować może działalność zorganizowanych grup przestępczych, ewentualnie służb specjalnych lub wojsk prowadzących „wojnę w cyberprzestrzeni". Konieczność wykorzystania metod śledczych dla posłużenia się danymi bądź metadanymi zebranymi w systemie informatycznym organizacji może wyniknąć również w związku z innymi niż incydent bezpieczeństwa okolicznościami (np. trzeba ustalić czas logowania i aktywności użytkownika w systemie dla potrzeb postępowania z zakresu prawa pracy, dla ustalenia czy pracownik pracował w nadgodzinach).

Cel niniejszej monografii ma charakter eksploracyjny: jest nim rozpoznanie współczesnego rozumienia pojęcia cyfrowej gotowości śledczej i praktycznego podejścia do zarządzania nią przez różne organizacje.

Rozważanie zagadnień dotyczących naruszania bezpieczeństwa jest – z metodologicznego punktu widzenia – problematyczne z kilku powodów: po pierwsze, gdy mowa o celowych atakach, sami sprawcy są zainteresowani ukryciem sposobu swojego działania (choćby po to, aby móc go ponownie wykorzystać), zaś

Informatyczne, Warszawa 2014; idem, *Biegły informatyk w postępowaniu cywilnym*, „Zeszyty Naukowe Politechniki Łódzkiej" 2011, seria Elektryka, z. 121, nr 1078, s. 487–501; M. Szmit (red.), A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec, *Elementy Informatyki Sądowej*, Polskie Towarzystwo Informatyczne, Warszawa 2011; M. Szmit, I. Politowska, *O artykule 267 Kodeksu Karnego oczami biegłego*, „Prawo Mediów Elektronicznych", nr 8, dodatek do „Monitora Prawniczego" 2008, nr 16, s. 34–40; M. Szmit, *Informatyka śledcza*, [w:] S. Wrycza, J. Maślankowski (red.), *Informatyka ekonomiczna. Teoria i zastosowania*, Wydawnictwo Naukowe PWN, Warszawa 2019, s. 779–791; idem, *O standardach informatyki śledczej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 355, s. 81–91.

jeśli dojdzie do ich zdemaskowania i ujęcia – niejednokrotnie takim przedstawieniem przebiegu zdarzeń, które skutkowało będzie wymierzeniem jak najmniejszej kary, po wtóre – w czasie trwania czynności dowodowych informacje objęte są tajemnicą postępowania przygotowawczego, nie można więc uzyskać szczegółów ze śledztwa czy dochodzenia. Po trzecie – również pokrzywdzeni niejednokrotnie nie są zainteresowani udzielaniem jakichkolwiek wyjaśnień, obawiając się strat związanych z faktem, że niewłaściwie zabezpieczyli swoje zasoby. Po czwarte – ocena stanu zabezpieczeń może być i bywa dokonana również *ex ante* przez specjalistów (np. audytorów), ale raporty z ich pracy – wyjąwszy ewentualne certyfikaty zgodności z normami – nie są udostępniane publicznie[4]. Wszystko to – w połączeniu z brakiem głębszych statystyk przestępczości w Polsce – powoduje, że w praktyce nie da się prowadzić szerokich i pogłębionych systematycznych badań obejmujących zagadnienia gotowości śledczej, które mogłyby dać miarodajne wyniki. Z tego też powodu dla osiągniecia zamierzonego celu w niniejszej monografii posłużono się głównie badaniami literaturowymi obejmującymi analizę pojęcia cyfrowej gotowości śledczej w literaturze przedmiotu oraz badaniem wybranych przypadków praktycznych, przy czym – ponieważ część z tych przypadków znajduje się obecnie na etapie postępowań przygotowawczych bądź sądowych – z konieczności głównym źródłem informacji odnośnie do nich były powszechnie dostępne informacje prasowe i internetowe.

Książka składa się z czterech rozdziałów.

Rozdział pierwszy zawiera uwagi terminologiczne, w tym definicje i dyskusje najważniejszych – z punktu widzenia poruszanej tematyki – pojęć dotyczących działań postincydentalnych i wybranych aspektów zarządzania nimi. Może on być bez szkody dla dalszej lektury pominięty przez Czytelnika znającego fachowe słownictwo.

Rozdział drugi poświęcony jest wybranym aspektom zarządzania bezpieczeństwem informacji, rozumianym jako istotna część obszaru *Governance*, *Risk Management and Compliance*, w szczególności próbie określenia najważniejszych cech samej problematyki, uzasadniających potrzebę i konieczność formalizacji działań związanych z zapewnianiem bezpieczeństwa informacji, w tym na poziomie poszczególnych organizacji – zbudowania i doskonalenia odpowiednich procesów zarządzania, zwłaszcza obejmujących m.in. zapewnienie i nadzór nad DFR oraz podstawowemu przeglądowi sytuacji odnośnie do najpopularniejszych obecnie standardów, metodyk, ram postępowania, modeli dojrzałości czy narzędzi komputerowego wspomagania zarządzania zagadnieniami związanymi z zarządzaniem bezpieczeństwem informacji.

Rozdział trzeci zawiera krótki przegląd wybranych źródeł odnoszących do zagadnień związanych z DFR. Obejmuje normy ISO z uwagi na ich szczególne

4 Zob. np. M. Molski, M. Łacheta, *Podręcznik audytora systemów informatycznych*, Helion, Gliwice 2006, s. 121 i nast.; M. Forsytek, *Audyt informatyczny*, Infoaudit, Warszawa 2005, s. 24 i nast.; T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006, s. 15 i nast.

miejsce w praktyce informatycznej, publikacje NIST z uwagi na rolę, jaką odgrywają Stany Zjednoczone Ameryki Północnej zarówno w IT, jak i praktyce podejścia do zarządzania organizacjami oraz anglojęzyczną literaturę naukową.

Rozdział czwarty zawiera przegląd literatury krajowej oraz uwagi odnośnie do pewnych aspektów DFR, które – jak się wydaje – powinny być uwzględniane przy zarządzaniu gotowością śledczą w warunkach krajowych, wsparte przykładami aktualnych zdarzeń dotyczących tej tematyki.

1. Pojęcia podstawowe

1.1. Systemy Zarządzania Bezpieczeństwem Informacji

Międzynarodowa Organizacja Standaryzacyjna ISO rozwija wiele rodzin standardów dotyczących tzw. systemów zarządzania, czyli wyodrębnionych konceptualnie części systemu zarządzania organizacją, takich jak np.: System Zarządzania Ciągłością Działania (*Business Continuity Management System*, BCMS) czy system zarządzania jakością *Quality Management System* (QMS). Wspólną ich podstawą są: podejście zorientowane na zarządzanie ryzykiem, podejście systemowe, podejście procesowe oraz wymóg ciągłego doskonalenia. Z punktu widzenia nauk o zarządzaniu i jakości podejście Międzynarodowej Organizacji Standaryzacyjnej wpisuje się w paradygmat neopozytywistyczno-funkcjonalistyczno-systemowy[1].

Pojęcie „System Zarządzania Bezpieczeństwem Informacji" (SZBI, *Information Security Management System*, ISIM) związane jest z rodziną norm przygotowaną wspólnie z Międzynarodową Komisją Elektrotechniczną (*International Electrotechnical Commission*, IEC). ISO oraz IEC utworzyły wspólny komitet techniczny – ISO/IEC JTC 1, który zajmuje się m.in. opracowywaniem i wprowadzaniem międzynarodowych standardów dla systemów zarządzania bezpieczeństwem informacji (grupa robocza ISO/IEC JTC 1/SC 27/WG 1). Numery norm rozpoczynają się od cyfr 2 i 7. Wszystkie normy z tej rodziny mają numery, poczynając od dwadzieścia siedem tysięcy (numer 27000 ma norma słownikowa o tytule „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia"), na oznaczenie całej rodziny norm stosuje się więc zapis 27x lub 27k.

ISMS jest tą częścią całościowego systemu zarządzania organizacją, która pozostaje odpowiedzialna za ustanowienie, wdrożenie, funkcjonowanie,

1 Przyjmując typologię paradygmatów za: Ł. Sułkowski, *Funkcjonalistyczna wizja kultury organizacyjnej w zarządzaniu – dominujący paradygmat i jego krytyka*, „Problemy Zarządzania" 2013, t. 11, nr 4 (44), s. 21.

monitorowanie, przeglądy, utrzymanie i doskonalenie bezpieczeństwa informacji, przy czym sam system zarządzania jest rozumiany jako zbiór wytycznych, polityk, procedur, procesów i związanych z nimi zasobów (zarówno materialnych, takich jak komputery czy maszyny, ludzkich – jak pracownicy, czy raczej role organizacyjne, wraz z przypisanymi do nich umiejętnościami, jak i niematerialno-prawnych – jak programy komputerowe czy know-how) mających na celu zapewnienie organizacji spełnienia swoich zadań[2]. Zarządzanie bezpieczeństwem informacji w podejściu opisanym normami ISO/IEC 27k oparte jest na koncepcji zarządzania ryzykiem biznesowym[3]. Dwoma głównymi normami w rodzinie norm 27k są normy ISO/IEC 27001 (w chwili pisania niniejszej książki jej aktualną polską wersją jest norma PN-EN ISO/IEC 27001:2023-08 – wersja polska Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności –Systemy zarządzania bezpieczeństwem informacji – Wymagania) – zawierająca wymagania, na zgodność z którymi przeprowadzane są audyty ISMS oraz ISO/IEC 27002 (w chwili pisania niniejszej książki jej aktualną polską wersją jest – przyjęta w wersji „okładkowej" norma PN-EN ISO/IEC 27002:2023-01 – wersja angielska Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji) zawierająca zalecenia odnośnie do działania ISMS i używanych w nim zabezpieczeń. Sama koncepcja ISMS wywodzi się z trzyczęściowego brytyjskiego standardu BS 7799 opracowanego przez British Standard Institution (pierwsza część została opublikowana w 1995 roku. Obecnie rodzina norm ISO/IEX 27x obejmuje niemal 60 standardów (w tym kilka wieloczęściowych) dotyczących zarówno samych Systemów Zarządzania Bezpieczeństwem Informacji, jak i różnych – często bardzo specyficznych – aspektów związanych z różnymi kwestiami cyberbezpieceństwa, począwszy od specyficznych zaleceń dla organizacji działających w różnych branżach i sektorach (np. w telekomunikacji[4] czy ochronie zdrowia[5]), poprzez zagadnienia związane z prywatnością i ochroną danych osobowych, Internetem rzeczy aż do zarządzania incydentami i informatyką śledczą.

2 Zob. A. Gillies, *Improving the quality of information security management systems with ISO27000*, „TQM Journal" 2011, Vol. 23, Issue 4, s. 367–376; E. Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Norwood 2007, s. 11–44.

3 Zgodnie z ogólnym podejściem prezentowanym przez ISO odnośnie do poszczególnych systemów zarządzania np. w normie PN-ISO/IEC 31000:2012 – Zarządzanie ryzykiem – Zasady i wytyczne.

4 Przygotowana również jako rekomendacja Międzynarodowego Związku Telekomunikacyjnego ITU norma ISO/IEC 27011:2024 / ITU-T X.1051 – Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations (third edition).

5 ISO 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002 (second edition).

1.2. Znaczenie terminologii znormalizowanej[6]

Biorąc pod uwagę szczególną rolę i znaczenie standardów międzynarodowych, w tym norm z rodziny ISO/IEC 27k, w książce przyjęto jako punkt wyjścia definicje i rozumienie poszczególnych pojęć prezentowane w normach ISO. Odwoływanie się do prac normalizacyjnych w obrębie monografii naukowej może być oczywiście kontrowersyjne o tyle, że normy nie są pracami naukowymi, ich znaczenie zarówno w systemie prawnym[7], jak i ekonomicznym (w szczególności rola w odniesieniu do nadzoru rynku[8]) jest dość specyficzne, wreszcie dlatego również, że istnieją negatywne aspekty normalizacji (wśród których można wymienić nadmierną biurokratyzację, czaso- i kosztochłonność związaną z przygotowaniem odpowiednich dokumentów, zagrożenie popadnięciem w schematyzm, wzrost oporu przed zmianami, spadek elastyczności pracowników[9] i wiele innych), niemniej biorąc pod uwagę wspomnianą rolę standardów międzynarodowych w zagadnieniach dotyczących bezpieczeństwa informacji, wydaje się, że wykorzystanie ich jako punkt odniesienia zarówno w kwestiach leksykalnych, jak i odnośnie do przyjętych praktyk działania nie będzie niewłaściwe. Wprawdzie również do języka norm można mieć pewne zastrzeżenia, w szczególności można mieć wątpliwość, czy w ogóle niektóre definicje są z formalnego punktu widzenia poprawnie skonstruowane, niemniej w porównaniu z terminologią tworzoną *ad hoc*, a nawet czasami z terminologią prawniczą jest on zdecydowanie bardziej precyzyjny[10]. Warto też podkreślić rosnące znaczenie rynkowe normy ISO/IEC 27001. W roku 2023 według raportu The ISO Survey[11] w Polsce wydanych było 846 ważnych certyfikatów na zgodność ISMS z wymaganiami ISO/IEC 27001:2013 oraz ISO/IEC 27001:2022, na świecie – 47291.

---

6 Czasami w literaturze używa się pojęcia „normatywne", co może być powodem nieporozumień: „normatywny" w języku prawniczym odnosi się do dokumentu zawierającego normy prawne (np. ustawy), natomiast w odniesieniu do zarządzania i nauk technicznych – do norm (standardów) np. zakładowych, krajowych czy międzynarodowych.

7 Zob. Ustawa z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483).

8 Zob. Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854, z 2024 r. poz. 1089).

9 Zob. np. U. Bukowska, *Normalizacja w kształtowaniu jakości zasobów ludzkich*, [w:] B. Urbaniak (red.), *Efektywność zarządzania zasobami ludzkimi*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2011, s. 515–527.

10 W książce B. Szafrański *et al*., *Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej* (PTI, Katowice 2006, s. 38) autorzy piszą: „Podstawy metodologiczne analizowanych aktów normatywnych są poprawniejsze niż aktów prawnych poddanych analizie […] dlatego też postulujemy wykorzystanie norm zarządzania bezpieczeństwem [systemu] informacyjnego jako platformy integracji regulacji zawartych w ustawach z zakresu bezpieczeństwa teleinformatycznego". Zob. też np.: M. Szmit, I. Politowska, *O artykule 267 Kodeksu Karnego oczami biegłego*, „Prawo Mediów Elektronicznych", nr 8, dodatek do „Monitora Prawniczego" 2008, nr 16, s. 34–40.

11 The ISO Survey, 2023, International Organization for Standardization, https://www.iso.org/the-iso-survey.html

Rodzina norm 27k rozwinęła się z brytyjskich standardów BS-7799, opublikowanych pierwszy raz w 1995 roku, obejmując początkowo dwie normy (oznaczone później jako 27001 i 27002) zawierające odpowiednio: wymagania odnośnie do ISMS (na zgodność z którymi możliwe jest przeprowadzanie audytów) oraz praktyczne zasady zabezpieczania informacji, do – współcześnie – ponad sześćdziesięciu norm poświęconych różnym aspektom bezpieczeństwa informacji. Jednocześnie intensywny rozwój nowych technik, takich jak choćby różnego rodzaju przetwarzanie w chmurach obliczeniowych, Internet rzeczy, przemysł 4.0, a ostatnio również sztuczna inteligencja, wraz z uwarunkowaniami takimi jak choćby transgraniczność globalnej sieci, doprowadził do wielu zmian cywilizacyjnych, stawiających nowe wyzwania zarówno w skali makro (a więc np. odnośnie do stanowienia prawa czy ochrony infrastruktury krytycznej państwa) jak i – w skali mikro – do zarządzania takimi aspektami przetwarzania informacji, które do niedawna miały znaczenie marginalne bądź były zupełnie nieznane[12]. W takiej sytuacji konieczny jest „poziomy" rozwój standardów i rozwiązań wspierających kolejne zagadnienia związane z różnymi aspektami zarządzania bezpieczeństwem, np. wyodrębnienie całej rodziny norm 291x związanej z ochroną prywatności czy 223x poświęconych Systemom Zarządzania Ciągłością Działania, które obejmują zresztą nie tylko kwestie bezpieczeństwa informacji, ale całości organizacji, a także ich rozwój „pionowy", w sensie standaryzacji coraz bardziej szczegółowych zagadnień dotyczących wąskich fragmentów zarządzania bezpieczeństwem informacji. Konieczne są również stosunkowo częste nowelizacje standardów. Dla przykładu norma słownikowa ISO/IEC 27000 (obecnie podlegająca przeglądom co pięć lat) w latach 2009–2018 miała aż pięć kolejnych wersji.

Najważniejszymi z punktu widzenia poruszanej tematyki normami międzynarodowymi ISO są: norma słownikowa PN-EN ISO/IEC 27000:2020-07 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia stanowiąca tzw. implementację okładkową anglojęzycznej normy Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018) oraz norma terminologiczna ISO/IEC 2382:2015 Information technology – Vocabulary. Ponieważ w chwili pisania monografii obie obowiązujące wersje norm są anglojęzyczne (i w wersjach międzynarodowych anglojęzycznych są udostępnione przez ISO nieodpłatnie do celów niekomercyjnych), poniżej podano tłumaczenia nieoficjalne tam, gdzie to możliwe, cytując lub opierając się na wycofanych – polskojęzycznych – wersjach norm, a więc PN-ISO/IEC 27000:2014 oraz PN-ISO/IEC 2382-8:2001, pomijając również uwagi zawarte w definicjach tam, gdzie nie miały one charakteru merytorycznego i poprawiając błędy językowe (np. niepoprawne użycie liczby pojedynczej od słowa „aktywa" itp.).

12 Zob. np. A. Pamuła, B. Gontar, P. Czerwonka, *Korzyści i problemy implementacji systemów w środowisku chmury obliczeniowej studia przypadków polskich przedsiębiorstw*. „Annales Universitatis Mariae Curie-Skłodowska, Sectio H Oeconomia" 2018, t. 52, s. 127–140.

1.3. Cyberbezpieczeństwo i bezpieczeństwo informacji

Zagadnienia cyfrowej gotowości śledczej należą niewątpliwie do zagadnień związanych z bezpieczeństwem informacji czy cyberbezpieczeństwem. Polskie słowo „bezpieczny" (w języku staro- i średniopolskim „przezpieczny") jest dosłownym tłumaczeniem łacińskiego zrostu *secura*[13] (od *se*, *sine* – osobno, *cura* – troska), przy czym słowo to używane było w znaczeniu bliskim współczesnemu słowu „beztroski"[14] – od czasownika piec się 'palić, martwić się' i od prasłowiańskiego czasownika pekti i rdzenia *pek-, obecnego w opisach stanów pierwotnie związanych z uczuciem gorąca („pieczenia"), a wtórnie – w opisach stanów związanych z emocjami psychicznymi („zapiekły", „pieklić się"), a także staropolskie „pieczliwy" – zaniepokojony, zatroskany (z tego samego rdzenia wywodzi się wyraz „piekło"). Zakres tego przymiotnika stopniowo się rozszerzał aż do znaczenia współczesnego. Pojęcie „bezpieczeństwo" współcześnie odnosi się przede wszystkim do bezpieczeństwa człowieka, jego życia, potrzeb, praw, wartości. Wtórnie przymiotnikiem „bezpieczny" określa się taki stan rzeczy, który nie stwarza niebezpieczeństwa bądź przed niebezpieczeństwem chroni. Słownik Języka Polskiego[15] podaje dwa znaczenia słowa „bezpieczny":

1. „taki, któremu nic nie grozi";
2. „niczym niezagrażający, chroniący przed niebezpieczeństwem".

L. Korzeniowski[16] określa zakres znaczeniowy pojęcia „bezpieczeństwo", odwołując się do trzech atrybutów: podmiotu, obiektywnego stanu (to jest sytuacji występowania bądź niewystępowania zagrożeń, niezależnie od świadomości podmiotu bądź obserwatora) oraz subiektywnego odczucia (poczucia bezpieczeństwa). **Bezpieczeństwo** to zatem stan braku zagrożenia, poczucia braku zagrożenia bądź cecha obiektu, który ma taki stan zapewnić (np. w wyrażeniach takich jak „pasy bezpieczeństwa", „hamulec bezpieczeństwa" itd.).

W języku angielskim istnieją dwa słowa określające bezpieczeństwo: *safety* i *security*. Pierwsze używane jest często w odniesieniu do bezpieczeństwa osób i zabezpieczenia ich podstawowych potrzeb życiowych, drugie – bezpieczeństwu zasobów, w tym informatycznych, zwłaszcza w aspekcie potencjalnych zagrożeń

13 Podobnie np. słowackie *bezpečný*, angielskie *secure*, czeskie *bezpečný*, portugalskie *seguro*, baskijskie *segurua* itd.

14 Zob. np. H. Popowska-Taborska, *Dlaczego pol. bezpieczny nie znaczy 'niebezpieczny'?*, „Acta Universitatis Wratislaviensis" 2014, nr 3578, Slavica Wratislaviensis CLIX; Z. Krótki, *Polskie leksemy o rdzeniu piecz-/piek- pochodne od piec się*, „Poznańskie Studia Polonistyczne" 2015, Seria Językoznawcza, t. 22 (42), nr 2, s. 69–88; L. F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 92 i nast.

15 https://sjp.pwn.pl/sjp/bezpieczny;2443955.html (dostęp: 5 stycznia 2025).

16 *Ibidem*, s. 112 i nast.

spowodowanych celową działalnością człowieka. *Safety* interpretuje się również czasami jako bezpieczeństwo od zagrożeń losowych i naturalnych, a *security* – od działań intencjonalnych, np. włamań.

Oczywiście bezpieczeństwo (rozumiane przedmiotowo) będzie dotyczyło innych własności w przypadku, gdy mowa o obiektach materialnych (rzeczach), a innych wypadku, gdy mowa o przedmiotach niematerialnych, jakimi są np. dane czy informacje.

Bezpieczeństwo informacji definiowane jest w normie PN-ISO/IEC 27000:2018 jako zachowanie poufności, integralności i dostępności informacji, dodatkowo można brać pod uwagę inne własności, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[17].

Podstawowe własności bezpieczeństwa informacji zdefiniowane są, jak następuje:

Poufność to własność polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom ani procesom[18].

Integralność to własność polegająca na zapewnieniu dokładności i kompletności aktywów[19].

Dostępność to własność bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu[20].

Trzy powyższe własności (zwane CIA – *Confidentiality*, *Integrity*, *Availability*) są najważniejszymi – z punktu widzenia omawianych norm – własnościami bezpieczeństwa informacji. Oprócz nich wyróżnia się m.in. własności:

Autentyczność to własność zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana[21].

Niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i następstwa[22].

Rozliczalność zdefiniowana jest w normie ISO/IEC 2382:2015 jako właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi[23].

Niezaprzeczalność – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot[24].

---

17 **Information security** – preservation of confidentiality, integrity and availability of information. Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability) can also be involved. ISO/IEC 27000:2018-3.28.

18 **Confidentiality** – property that information is not made available or disclosed to unauthorized individuals, entities, or processes. ISO/IEC 27000:2018-3.10.

19 **Integrity** – property of accuracy and completeness. ISO/IEC 27000:2018-3.36.

20 **Availability** – property of being accessible and usable on demand by an authorized entity. ISO/IEC 27000:2018-3.7.

21 **Authenticity** – property that an entity is what it claims to be. ISO/IEC 27000:2018-3.6.

22 **Reliability** – property of consistent intended behaviour and results. ISO/IEC 27000:2018-3.55.

23 **Accountability** – property that ensures that the actions of an entity may be traced uniquely to that entity. ISO/IEC 2382:2015-2126250.

24 **Non-repudiation** – ability to prove the occurrence of a claimed event (3.21) or action and its originating entities. ISO/IEC 27000:2018-3.48.

Oprócz triady CIA warto wspomnieć jeszcze o tzw. heksadzie Parkera, w której do CIA dodano atrybuty posiadania lub kontroli w odniesieniu do nośnika informacji, autentyczności oraz użyteczności[25]. W zależności od kontekstu niezaprzeczalność może dotyczyć różnych akcji (np. można mówić o niezaprzeczalności wysłania wiadomości, niezaprzeczalności jej otrzymania itd.)[26].

Oczywiście powyższa lista nie ma charakteru zamkniętego. W zależności od rodzaju i kontekstu przetwarzanej informacji istotne mogą być również inne własności bezpieczeństwa informacji nie ujęte *explicite* powyżej, takie jak np. prywatność – wolność od ingerencji w życie prywatne lub sprawy osoby fizycznej, jeżeli ingerencja ta związana byłaby z niewłaściwym lub nielegalnym zbieraniem i wykorzystywaniem danych na temat tej osoby[27] czy anonimowość – cecha informacji, która nie pozwala na bezpośrednią lub pośrednią identyfikację osoby fizycznej[28]. Oczywiście definicje te odnoszą się do przetwarzania danych osobowych i osób fizycznych, w szerszym rozumieniu anonimowość może dotyczyć takiej własności bezpieczeństwa informacji, która będzie zapewniała brak rozliczalności poszczególnych transakcji, nawet jeśli prowadził je proces, a nie osoba, prywatność zaś dotyczy również innych, niż związane z przetwarzaniem danych, ingerencji w sfery życia, które powinny pozostawać poza sferą publiczną.

Pojęciem przeżywającym dość szybką ewolucję, za to niezwykle popularnym jest cyberbezpieczeństwo. Użycie prefiksu „cyber-" (z gr. *κυβερνητικός* – „sternik") wielokrotnie było krytykowane w literaturze przedmiotu, jednak obecnie przyjęło się w uzusie językowym, stąd różne próby zaadaptowania słownictwa fachowego. Słowo „cyberprzestrzeń", które jak się wydaje było pierwotną przyczyną popularności tego prefiksu, zostało użyte po raz pierwszy w opowiadaniu *Burning Chrome* autorstwa W. Gibsona[29], przy czym desygnat tego słowa był pierwotnie nieokreślony. W obowiązującej w chwili pisania tej książki wersji normy międzynarodowej ISO/IEC 27032:2023 (za normą ISO/IEC 27102) zdefiniowano **cyberbezpieczeństwo** jako ochronę osób, społeczeństwa organizacji i narodów przed cyberryzykiem z uwagą, że ochrona jest rozumiana jako utrzymywanie cyberryzyka na znośnym poziomie[30]. Konsekwentnie przez **cyberryzyko** normy rozumieją ryzy-

25 Zob. D.B. Parker, *Fighting Computer Crime*, John Wiley & Sons, New York 1988

26 Zob. np. ISO/IEC 13888-1:2020 Information security – Non-repudiation – Part 1: General.

27 **Privacy** – freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. ISO/IEC 2382:2015-2126263.

28 **Anonymity** – characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly ISO/IEC 29100:2011-2.1.

29 Część źródeł podaje, że miało to miejsce w powieści *Neuromancer* – zob. np.: S. Dziwisz, *Odpowiedzialność karna za przestępstwa popełnione w cyberprzestrzeni*, [w:] A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013.

30 **Cybersecurity** – safeguarding of people, society, organizations and nations from cyber risks. ISO/IEC TS 27032:2023-3.6.
Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level.

ko spowodowane przez cyberzagrożenie[31], przez **cyberzagrożenie** – zagrożenie wykorzystujące cyberprzestrzeń[32], a przez **cyberprzestrzeń** – środowisko połączonych sieci, usług, systemów i procesów[33]. Zatem *sensu stricto* cyberbezpieczeństwo jest częścią bezpieczeństwa informacji (to bowiem obejmuje również bezpieczeństwo systemów izolowanych od cyberprzestrzeni).

Warto zauważyć, że są to definicje zupełnie różne od definicji przyjmowanych choćby w poprzedniej wersji normy ISO/IEC 27032 i trudno przewidywać, na ile są ostateczne.

1.4. Nadzór, zgodność i zarządzanie ryzykiem w bezpieczeństwie informacji

Różne narzędzia i stojące za nimi podejścia czy metodyki prezentują niejednokrotnie daleko różne punkty widzenia na zagadnienia związane z zarządzaniem bezpieczeństwem informacji, poczynając od elementarnych definicji[34], a kończąc na systematyzacji procesów zarządzania, czy nawet określaniu roli poszczególnych elementów obszaru *Governance, Risk Management, Compliance*[35].

Pojęcie **GRC** zdefiniowano jako „zintegrowany zbiór zdolności, które umożliwiają organizacji rzetelne osiąganie celów, radzenie sobie z niepewnością i uczciwe działanie”[36]. Sam skrót GRC został pierwszy raz użyty na początku XXI wieku, jego pierwsze użycie jest przypisywane Michaelowi Rasmussenowi pracującemu podówczas dla Forrester Research Inc. Niektórzy rozróżniają generacje (oznaczane kolejnymi numerami od GRC1 do GRC4)[37].

Słowo ***governance*** tłumaczy się najczęściej jako „**ład korporacyjny**” lub „**nadzór korporacyjny**”, **„ład organizacyjny”** itp., rozumiejąc pod tym drugim

31 **Cyber-risk** – risk caused by a cyber-threat. ISO/IEC 27102:2019-3.4.

32 **Cyber-threat** – threat that exploits a cyberspace. ISO/IEC 27102:2019-3.5.

33 **Cyberspace** – interconnected digital environment of networks, services, systems, and processes. ISO/IEC 27102:2019-3.6.

34 Dyskusje różnych niespójnych terminologii można znaleźć np. w publikacjach: M. Szmit, A. Szmit, *O normatywnych definicjach cyberbezpieczeństwa*, [w:] K. Załęski, P. Polko (red.), *Bezpieczeństwo Polski w drugiej dekadzie XXI wieku*, Akademia WSB, Dąbrowa Górnicza 2019, s. 113; A. Szmit, M. Szmit, *Bezpieczeństwo, cyberbezpieczeństwo, ryzyko w bezpieczeństwie informacji – próba uporządkowania pojęć*, [w:] I. Staniec (red.), *Natura i uwarunkowania ryzyka*, Wydawnictwo Politechniki Łódzkiej, Łódź 2014, s. 275; D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, European Association for Security, Kraków 2016 s. 15 i nast.

35 Czasami również rozwijane jako Governance, Risk, Compliance.

36 S. Mitchell, *GRC360: A framework to help organisations drive principled performance*, „International Journal of Disclosure and Governance” 2007, Vol. 4, https://doi.org/10.1057/palgrave.jdg.2050066

37 Zob. np. *Risk Optics: IRM, ERM, and GRC: Is There a Difference?*, 22.08.2002, https://reciprocity.com/irm-erm-and-grc-is-there-a-difference (dostęp: 5 stycznia 2025).

określeniem nadzór nad organizacją sprawowany przez właścicieli (akcjonariuszy) bądź szerzej – interesariuszy, ochronę właścicieli, a pod tym pierwszym – ustrój organizacji (zbiór zasad i norm) czy nawet metodykę podejmowania decyzji[38].

W obrębie norm ISO zagadnienia dotyczące zgodności oraz nadzoru normalizowane są przez normy z serii ISO 37x opisujące systemy zarządzania zgodnością (*Compliance Management Systems*, CMS). W szczególności norma ISO 37000:2021 *Governance of organizations – Guidance* (w chwili pisania niniejszej książki w ogóle nie wprowadzona do systemu Polskich Norm) definiuje ład organizacyjny jako system tworzony i realizowany przez ludzi, za pomocą którego organizacja jest kierowana, nadzorowana i rozliczana z realizacji swojego zdefinowanego celu[39].

W rodzinie norm ISO/IEC 27k odpowiednie definicje brzmią:

Ciało/Organ nadzorczy – osoba lub grupa osób, które są odpowiedzialne za wyniki i zgodności organizacji[40].

- **Najwyższe kierownictwo** – osoba lub grupa osób, która kieruje i kontroluje organizację na najwyższym poziomie.
  - Uwaga 1: Kierownictwo ma prawo do delegowania władzy i zapewnienia zasobów w ramach organizacji.
  - Uwaga 2: Jeśli zakres systemu zarządzania (2.46) obejmuje tylko część organizacji, wtedy pojęcie „najwyższe kierownictwo" odnosi się do tych osób, które kierują i kontrolują tę część organizacji.
  - Uwaga 3 do wpisu: Najwyższe kierownictwo jest czasami nazywane kierownictwem wykonawczym i może obejmować dyrektorów generalnych, dyrektorów finansowych, dyrektorów ds. informatyki i osoby na podobnych stanowiskach[41].
- **Ład korporacyjny bezpieczeństwa informacji** – System, za pomocą którego działania organizacji w zakresie bezpieczeństwa informacji są kierowane i kontrolowane[42].

---

38 Obszerną analizę użycia pojęcia *governance* zawiera artykuł: M. Szulc, *Pojęcie governance w piśmiennictwie na temat nauk o zarządzaniu*, „Studia i Prace Kolegium Zarządzania i Finansów" 2019, z. 176, s. 85–110.

39 **Governance of organizations** – human-based system by which an organization is directed, overseen and held accountable for achieving its defined purpose. ISO/IEC 37000:2021-3.1.1.

40 **Governing body** – person or group of people who are accountable for the performance (3.52) and conformity of the organization. PN-ISO/IEC 27000:2018-3.24.

41 **Top management** – person or group of people who directs and controls an organization (3.50) at the highest level.
Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.
Note 2 to entry: If the scope of the management system (3.41) covers only part of an organization, then top management refers to those who direct and control that part of the organization.
Note 3 to entry: Top management is sometimes called executive management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles. PN-ISO/IEC 27000:2018-3.75.

42 **Governance of information security** – system by which an organization's information security activities are directed and controlled. PN-ISO/IEC 27000:2018-3.23.

Compliance oznacza dosłownie **zgodność**, w omawianym kontekście zgodność w szczególności z wymagania prawa, regulacjami (tam, gdzie mowa o rynkach regulowanych) czy z przyjętymi przez organizację zobowiązaniami. W kontekście rozumienia i rozwoju pojęcia *compliance* szczególnie należy zwrócić uwagę na rolę ustawy Sarbanesa-Oxleya[43]. Wywarła ona wpływ na liczne firmy na całym świecie, z jednej strony nakładając zobowiązania na firmy z udziałem kapitału amerykańskiego, z drugiej – regulując działanie dużych firm zajmujących się audytem, również często podlegających wymogom prawa USA, z trzeciej – stając się wzorem i punktem odniesienia rozwiązań w innych krajach, np. w Chinach (tzw. China-SOX w 2009 roku) czy Kanadzie (w 2003 roku). Istnieje również wiele przepisów prawa regulujących kwestie związane z bezpieczeństwem informacji (np. amerykańska ustawa *Health Insurance Portability and Accountability Act*, HIPAA[44], w Unii Europejskiej RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE), regulacji obowiązujących na poszczególnych rynkach (np. standard PCI DSS – *Payment Card Industry Data Security Standard* wydany przez Payment Card Industry Security Standards Council, który muszą stosować przedsiębiorcy akceptujący płatności kartami i centra autoryzacyjne w ramach współpracy z organizacjami płatniczymi takimi jak Visa czy MasterCard) czy rekomendacji[45]. Norma ISO 37000:2021 definiuje zgodność jako spełnienie wszystkich wymogów zgodności obowiązujących organizację[46], przy czym przez **wymogi zgodności** rozumie się zarówno te wymagania, które organizacja musi spełnić w sposób obligatoryjny, jak i te, które zobowiązała się spełnić w sposób dobrowolny[47]. W rodzinie ISO 37x za zarządzanie zgodnością odpowiada norma ISO 37301:2021 – *Compliance Management Systems – Requirements with Guidance*, która zawiera wymagania dla systemów zarządzania zgodnością, na zgodność z którymi można certyfikować CMS.

Centralnym pojęciem w zarządzaniu bezpieczeństwem informacji jest ryzyko (w literaturze, szczególnie profesjonalnej, używa się coraz częściej liczby mnogiej „ryzyka", choć formalnie jest to rzeczownik nieposiadający liczby mnogiej; wśród

43 SOX lub SarOX z 2002 roku, https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf (dostęp: 5 stycznia 2025).

44 https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (dostęp: 5 stycznia 2025).

45 Taką rolę odgrywała np. Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach Komisji Nadzoru Finansowego, obecnie zastąpiona przez rozporządzanie DORA – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011) i szereg aktów wykonawczych do niego.

46 **Compliance** – meeting all the organization's compliance obligations. ISO 37000:2021-3.2.5.

47 **Compliance obligations** – requirements that an organization mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with. ISO 37000:2021-3.2.6.

językoznawców dominuje jednak pogląd, że należy raczej stosowanie form pluralnych dopuścić[48]). Jest to pojęcie wielowymiarowe, a próby jego zdefiniowania napotykają na kilka przeszkód natury zarówno teoretycznej, jak i praktycznej. Już sama etymologia słowa „ryzyko" jest niepewna. Wywodzi się je od starowłoskiego *riscare* –„odważyć się", hiszpańskiego *riesgo* i łacińskiego *resecum* (oznaczającego *rozcięcie, rzecz, która kaleczy* lub *pułapkę*) bądź greckiego ριζική oznaczającego szansę[49]. Już na tym poziomie można zauważyć, że ryzyko może być używane tylko w odniesieniu do potencjalnych zagrożeń (np. w pedagogice, gdy mowa o zachowaniach ryzykownych) bądź też – gdy mowa o (pozytywnych) szansach. Po wtóre, można przez ryzyko rozumieć samo prawdopodobieństwo materializacji owego zagrożenia (bądź szansy) bądź też kombinację tego prawdopodobieństwa i skutków tej materializacji.

Standardem poświęconym zarządzaniu ryzykiem jest norma ISO/IEC 31000, zaś w rodzinie norm ISO 27k – norma ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*.

Ryzyko to wpływ niepewności na cele z sześcioma uwagami:

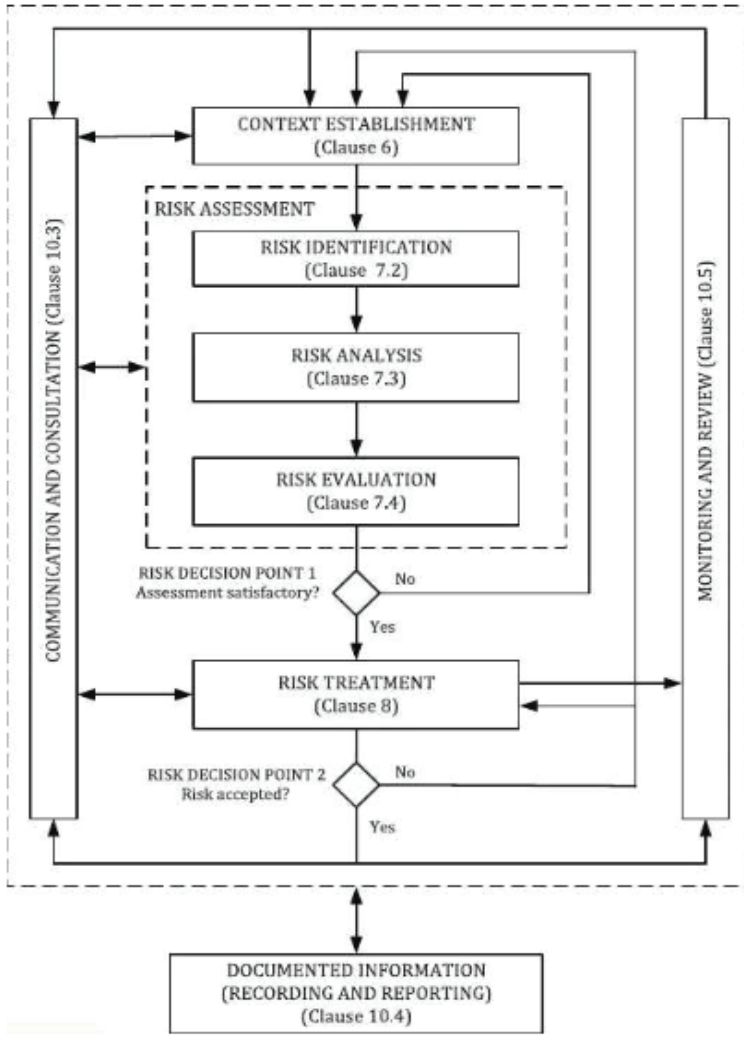
- Uwaga 1: Następstwem jest odchylenie od oczekiwań – pozytywne lub negatywne.
- Uwaga 2: Niepewność to stan, niedoboru informacji (również częściowego) związanej ze zrozumieniem lub wiedzą dotyczącą zdarzenia, jego następstw lub prawdopodobieństwa.
- Uwaga 3: Ryzyko jest często opisywane w odniesieniu do potencjalnych zdarzeń i następstw lub ich kombinacji.
- Uwaga 4: Ryzyko jest często wyrażane w połączeniu z następstwami zdarzenia (w tym zmianami okoliczności) oraz związanego z nimi prawdopodobieństwa wystąpienia.
- Uwaga 5: W kontekście systemów zarządzania bezpieczeństwem informacji, ryzyko związane z bezpieczeństwem informacji może być wyrażone jako wpływ niepewności na cele bezpieczeństwa informacji.
- Uwaga 6: Ryzyko związane z bezpieczeństwem informacji jest związane z możliwością, że zagrożenia będą wykorzystywały podatności aktywów informacyjnych lub grupy aktywów informacyjnych, a tym samym powodowały szkodę dla organizacji[50].

---

48 Por. np. https://sjp.pwn.pl/poradnia/haslo/kilka-ryzyk;743.html; https://gazetawroclawska.pl/prof-jan-miodek-ryzyka/ar/3357449 (dostęp: 5 stycznia 2025).

49 Zob. np. R. Lemonnier, *Model ubezpieczeń na francuskim rynku finansowym* (rozprawa doktorska, promotor: dr hab. Michał Mariański, prof. UWM), Uniwersytet Warmińsko-Mazurski w Olsztynie, maszynopis, https://wpia.uwm.edu.pl/sites/default/files/u12/model_ubezpieczen_na_francuskim_rynku_finansowym_watermarked.pdf (dostęp: 5 stycznia 2025), s. 110.

50 **Risk** – effect of uncertainty on objectives.
Note 1 to entry: An effect is a deviation from the expected – positive or negative.
Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.



Rysunek 1. Zarządzanie ryzykiem w normie ISO/IEC 27005:2022
Źródło: ISO/IEC 27005:2022 Figure 1.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

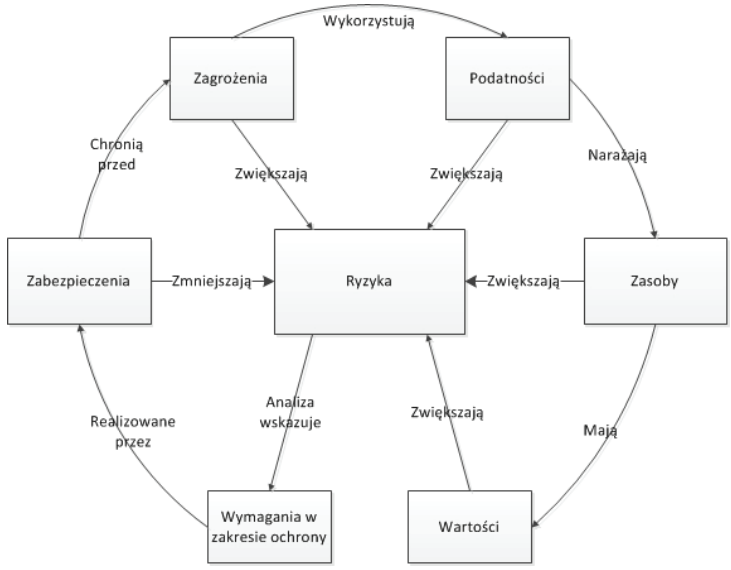
Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization. ISO/IEC 27000:2018-3.6.

W odniesieniu do poruszanej tematyki ryzyko będzie więc rozumiane jako kombinacja prawdopodobieństwa zajścia zdarzenia i jego (negatywnych) skutków. W normach używa się pojęcia „kombinacji", aby wskazać, że nie zawsze najlepszym sposobem oceny ryzyka jest prosty iloczyn (a więc formalnie wartość oczekiwana straty). Prawdopodobieństwo określa się raczej anglojęzycznym *likelyhood*, nie zaś *probability*, aby wskazać, że mowa jest nie o dokładnie wyliczonym statystycznym prawdopodobieństwie zajścia zdarzenia, ale o wielkości szacowanej, często wyrażanej na skali porządkowej (np. wysoce średnio bądź mało prawdopodobne).

Zarządzanie ryzykiem zostało zdefiniowane w normie ISO/IEC 27000 jako skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka[51]. Jest zorganizowane jako iteracyjny proces składający się z siedmiu elementów (działań): informowania i konsultowania, określania kontekstu, identyfikowania ryzyka, analizy ryzyka, oceny ryzyka, postępowania z ryzykiem oraz jego przeglądania i monitorowania[52] (zob. rysunek 1).



Rysunek 2. Związki pomiędzy podstawowymi pojęciami z zakresu bezpieczeństwa
Źródło: PN-I-13335-1:1999[53].

51 **Risk management** – Coordinated activities to direct and control an organization with regard to risk. ISO/IEC 27000:2018-3.69.

52 **Risk management process** – systematic application of management policies (3.53), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk. ISO/IEC 27005:2022-3.70. Note 1 to entry: ISO/IEC 27005 uses the term "process" to describe risk management overall. The elements within the risk management process are referred to as "activities".

53 W wersji normy z 1999 roku nie ma zapisu, że zasoby zwiększają ryzyka (brak strzałki między „zasoby" a „ryzyka"), co było oczywistą pomyłką, która miała zostać usunięta w kolejnej wersji, ale ostatecznie w kolejnej edycji normy z 2004 roku rysunek ten został już usunięty.

Zgodnie z wymogami normy ISO/IEC 27001 niektóre działania zarządzania ryzykiem muszą być dokumentowane, stąd dodatkowa czynność dokumentowania i raportowania udokumentowanej informacji.

Związek pomiędzy ryzykiem a pojęciami: zagrożenia, podatności, zabezpieczeń, zasobów czy wymagań w zakresie ochrony pokazano w (wycofanej) normie PN-ISO/IEC 13335-1:1999 (por. rysunek 2).

Użyte pojęcia norma ISO/IEC 27000:2018 definiuje jak poniżej:

- **Podatność** – słabość zasobu lub zabezpieczenia, która może być wykorzystana przez jedno lub więcej zagrożeń[54].
- **Zagrożenie** – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji[55].
- **Wymaganie** – potrzeba lub oczekiwanie, które jest wyrażone, ogólnie rozumiane lub obowiązkowe.
  - Uwaga 1: „ogólnie rozumiane" oznacza, że jest zwyczajem lub powszechną praktyką w zakresie organizacji i zainteresowanych stron, że bierze się pod uwagę taką potrzebę lub oczekiwanie.
  - Uwaga 2: określonym jest wymaganie, które zostało ustanowione, np. dokumentowanie informacji[56].
- **Zabezpieczenie** – środek, który modyfikuje ryzyko.
  - Uwaga 1: Zabezpieczenia obejmują procesy, polityki, urządzenia, praktyki lub inne działania modyfikujące ryzyko.
  - Uwaga 2: Zabezpieczenia nie zawsze wywierają zamierzony lub zakładany skutek modyfikujący.

Zabezpieczenia dzieli się zazwyczaj na zapobiegające (*preventive*), wykrywcze (*detective*) oraz naprawcze (*corrective*), w zależności od tego, czy służą zapobieganiu wystąpienia incydentu, czy jego wykryciu czy też naprawie sytuacji po jego zaistnieniu. Niektóre metodyki rozróżniają jeszcze zabezpieczenia kompensacyjne (*compensative*), czyli uzupełniające działanie innych zabezpieczeń oraz odstraszające (*deterrent*).

Zasoby (czasem zwany też **aktywami**[57] – *asset*) zdefiniowane zostały w normie ISO 27002:2022 jako wszystko, co ma wartość dla organizacji z uwagą: w kontekście bezpieczeństwa informacji można wyróżnić dwa rodzaje aktywów:

---

54 **Vulnerability** – weakness of an asset or control that can be exploited by one or more threats. ISO/IEC 27000:2018-3.77.

55 **Threat** – potential cause of an unwanted incident, which can result in harm to a system or organization. ISO/IEC 27000:2018-3.74.

56 **Requirement** – need or expectation that is stated, generally implied or obligatory.
Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.
Note 2 to entry: A specified requirement is one that is stated, for example in documented information. ISO/IEC 27000:2018-3.56.

57 W języku polskim słowo „aktywa" nie ma liczby pojedynczej, choć czasami można spotkać się z nowotworem językowym „aktywo". Biorąc pod uwagę źródłosłów łaciński, lepszym (choć równie źle brzmiącym) wyrazem byłby zapewne „aktywus" (łac. *activus* – czynny) lub

aktywa podstawowe:
– informacje;
– procesy biznesowe (3.1.27) i działania;
aktywa pomocnicze (od których zależą aktywa podstawowe) wszelkiego typu, np.:
– sprzęt;
– oprogramowanie;
– sieć;
– personel (3.1.20);
– siedziba;
– struktura organizacji[58].

Norma ISO/IEC 27000:2018 zawiera następujące definicje pojęć związanych z nadzorem i zgodnością:

- **Zgodność** – spełnienie wymagania[59].
- **Niezgodność** – niespełnienie wymagania[60].

1.5. Naruszenia bezpieczeństwa informacji i reakcja na nie

Z naruszeniami bezpieczeństwa informacji wiążą się następujące definicje zawarte w normach:

- **Zdarzenie związane z bezpieczeństwem informacji** jest wystąpieniem określonego stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczeń lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem[61].

„aktywum" (łac. *activum* – strona czynna). Liczba pojedyncza (*activo*) na określenie składnika majątku funkcjonuje w języku hiszpańskim.

58 **Asset** – anything that has value to the organization.
Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:
– the primary assets:
  – information;
  – business processes (3.1.27) and activities;
  – the supporting assets (on which the primary assets rely) of all types, for example:
    – hardware;
    – software;
    – network;
    – personnel (3.1.20);
    – site;
    – organization's structure.
ISO/IEC 27002:2022-3.1.2.

59 **Conformity** – fulfilment of a requirement PN-ISO/IEC 27000:2018-3.11.

60 **Nonconformity** – non-fulfilment of a requirement PN-ISO/IEC 27000:2018-3.47.

61 **Information security event** – identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously

- **Incydent związany z bezpieczeństwem informacji** pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji[62].
- **Zarządzanie incydentami związanymi z bezpieczeństwem informacji** – zbiór procesów wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji[63].
- **Atak** – udana lub nieudana próba zniszczenia, zmiany, uniemożliwienia dostępu, lub uzyskania dostępu do zasobu albo jakakolwiek próba ujawnienia, kradzieży lub nieautoryzowanego użycia zasobu[64].
- **Poważne naruszenie**[65] – naruszenie bezpieczeństwa systemu informatycznego, po którym dane lub programy mogą być modyfikowane, niszczone lub mogą stać się dostępne dla nieuprawnionych podmiotów[66].
- **Włamanie**, **przełamanie** – takie obejście lub zneutralizowanie jakiegoś elementu bezpieczeństwa systemu informatycznego, wykryte lub nie, którego skutkiem może być penetracja systemu przetwarzania danych[67].

---

unknown situation that can be security relevant. ISO/IEC 27000:2018-3.30. Podobna definicja zamieszczona jest w normie ISO/IEC 27002: **information security event** occurrence indicating a possible information security breach or failure of controls. ISO/IEC 27002:2022-3.1.14.

62 **Information security incident** – single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. PN-ISO/IEC 27000:2018-3.31. Podobna definicja w normie ISO/IEC 27002:2022 **Information security incident** – one or multiple related and identified information security events that can harm an organization's assets or compromise its operations. ISO/IEC 27002:2022-3.1.15.

63 **Information security incident management** – set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. PN-ISO/IEC 27000:2018-3.32. Inaczej w ISO/IEC 27002:2022 **Information security incident management** – exercise of a consistent and effective approach to the handling of information security incidents. ISO/IEC 27002:2022-3.1.16.

64 **Attack** – successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset. PN-ISO/IEC 27002:2022-3.1.3.

65 W definicji anglojęzycznej użyto słów *violation* oraz *compromise*. Jak można się spodziewać, z powodu tego, że oba z nich tłumaczy się na polski jako „naruszenie", w definicji PN-ISO/IEC 2382-8:2001-08.05.11 użyto dodatkowo przymiotnika „poważne", aby nie używać explicite definiendum w definiensie (błąd *idem per idem*). Czasami mówi się w źródłach polskojęzycznych o „skompromitowaniu" systemu, co odwołuje się do rzadko używanego znaczenia słowa „compromise".

66 **Compromise** – violation of computer security whereby programs or data may have been modified, destroyed, or made available to unauthorized entities. ISO/IEC 2382:2015-2126328.

67 **Breach** – circumvention or disablement of some element of computer security, with or without detection, which could result in a penetration of the data processing system. ISO/IEC 2382:2015-2126334. Nieco inaczej w ISO/IEC 27002:2022, gdzie mowa o przełamaniu zabezpieczeń informacji. **Information security breach** – compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed. ISO/IEC 27002:2022-3.1.13.

- **Reakcja na incydent** – działania podjęte w celu ochrony i przywrócenia normalnych warunków działania systemów informatycznych oraz przechowywanych w nich informacji w przypadku ataku lub naruszenia bezpieczeństwa[68].

Elementem reakcji na incydent jest m.in. analiza mająca na celu ustalenie jego przyczyn i mechanizmu. W języku polskim (a w zasadzie w profesjolekcie informatycznym) używa się najczęściej pojęcia „analizy powłamaniowej", które jest o tyle nieszczęśliwe, że nie każdy incydent bezpieczeństwa informacji musi być włamaniem, a działania, które należy podjąć po wystąpieniu incydentu, nie ograniczają się do jego analizy. Neologizm „postincydentalny" (lub nieprawidłowo „post-incydentalny", co jest kalką pisowni amerykańskiej) używany jest sporadycznie w materiałach reklamowych i dokumentach urzędowych[69].

W języku prawniczym funkcjonują pojęcia „dowodu" i „śladu dowodowego" – oba nieposiadające definicji legalnych. Dalej przyjęto, że przez „**dowód**" rozumie się dopuszczony przez organ prowadzący postępowanie (sąd, prokuraturę itd.), środek służący ustaleniu okoliczności mających znaczenie dla rozstrzygnięcia sprawy, przez „**ślad dowodowy**" – dowolne zmiany będące spostrzegalnymi znamionami po zdarzeniach będących przedmiotem postepowania, przez „**źródło dowodowe**" – nośnik informacji, a więc osobę lub rzecz, która dostarcza lub może dostarczyć informacji (np. dokument, biegły sądowy, świadek), przez „**środek dowodowy**" – samą informację, która została uzyskana ze źródła dowodowego (np. treść e-maila) lub metodę, dzięki której można uzyskać wiadomości ze źródła dowodowego (np. przesłuchanie świadka, opinię biegłego sądowego), przez „**materiał dowodowy**" – formę przekazywania informacji (np. wypowiedzi świadka). Ślad dowodowy może więc stać się dowodem, po jego dopuszczeniu przez organ prowadzący do wykorzystania w postępowaniu. W literaturze anglojęzycznej występują pojęcia *evidence* i *potential evidence*, przyjęto dalej, że drugiemu z nich odpowiada pojęcie śladu dowodowego.

Pojęcie „**cyfrowy**", jakkolwiek utrwalone w uzusie językowym, nie jest do końca prawidłowe, oznacza bowiem zapis składający się z cyfr bądź też procesy i jednostki funkcjonalne operujące na takich danych[70]. Współczesne urządzenia korzystające z techniki informatycznej operują wprawdzie (na jakimś poziomie abstrakcji) danymi dającymi się przedstawić w postaci cyfrowej, ale po pierwsze, taka sama sytuacja dotyczy też urządzeń zupełnie „niekomputerowych" (np. w postaci cyfr reprezentuje wyniki swojej pracy mechaniczny zegarek), a po wtóre, jest to tylko

68 **Incident response** – action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs. ISO/IEC 27039:2015-2.24.

69 Zob. np.: Załącznik C do Raportu z wykonywania wyroków Europejskiego Trybunału Praw Człowieka przez Polskę za 2020 r., VII Sprawozdanie Okresowe Rzeczypospolitej Polskiej z realizacji postanowień Konwencji w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania obejmujące okres od 15 października 2011 r. do 15 września 2017 r. (ze szczególnym uwzględnieniem okresu od 22 listopada 2014 r. do 15 września 2017 r.); A. Chojnowski, *Informatyka sądowa w praktyce*, Helion, Gliwice 2020, s. 75.

70 **Digital** – pertaining to data that consist of digits as well as to processes and functional units that use those data. ISO/IEC 2382:2015-2121328.

jeden z poziomów abstrakcji, poniżej którego występują często dyskretne sygnały elektryczne bądź optyczne, a powyżej – dane w postaci alfanumerycznej (litery i inne znaki pisma), dźwięki czy obrazy. Ściślej byłoby zapewne mówić nie o „śladach cyfrowych", ale o „śladach informatycznych", tj. powstałych w wyniku działania procesów składowania bądź przetwarzania informacji w urządzeniach techniki komputerowej, szczególnie że współcześnie nie wykorzystuje się komputerów niecyfrowych (zwanych analogowymi, również nie do końca ściśle).

Pojęcie „śledztwo" w polskim języku prawnym oznacza jeden z rodzajów postępowania przygotowawczego (obok dochodzenia). **Śledztwo** jest bardziej sformalizowanym rodzajem postępowania przygotowawczego – może być prowadzone tylko przez prokuratora lub na jego zlecenie przez organy ścigania (np. policję). **Dochodzenie** jest prostszą formą, używaną przy mniej poważnych sprawach, może być prowadzone przez odpowiednie organy pod nadzorem prokuratora. W języku standardów używa się jednego określenia – *investigation*[71], tłumaczonego zazwyczaj jako „śledztwo", gdzie oznacza zastosowanie odpowiednich badań, analiz i interpretacji w celu ułatwienia zrozumienia zdarzenia. Ponieważ kwestie formalnoprawne dotyczące postępowań przygotowawczych nie są z punktu widzenia tematyki książki istotne (a ponadto można mówić również o „śledztwach wewnętrznych" – prowadzonych przez organizację dla potrzeb np. postępowania dyscyplinarnego czy po prostu ustalenia przyczyn i mechanizmów zaistnienia niepożądanych zjawisk czy zdarzeń), dalej w książce pojęcia „śledztwo" i „dochodzenie" używane są zamiennie, z całą świadomością, że w odniesieniu do przepisów postępowania karnego nie jest to do końca prawidłowe.

Śledztwo wymaga oczywiście prowadzenia całego szeregu czynności, w tym takich, które mogą zostać usprawnione poprzez zastosowanie technik informatycznych (np. prowadzenie akt, korespondencji itd.), stąd – jak się wydaje – powinno się unikać mówienia o „cyfrowym śledztwie", zamiast tego mówiąc o „śledztwie z wykorzystaniem cyfrowych śladów dowodowych", jednak w krajowej literaturze przedmiotu taki – nie do końca precyzyjny – skrót myślowy funkcjonuje.

Pojęcie gotowości śledczej (*Forensic Readiness*, FR) wprowadził J. Tan[72], który określił ją przez dwa cele (*objectives*):

1. maksymalizację zdolności środowiska do pozyskiwania wiarygodnych dowodów cyfrowych oraz
2. minimalizację kosztów analizy śledczej w ramach reakcji na incydent.

Współcześnie w literaturze przedmiotu pisze się bądź o gotowości śledczej, bądź o cyfrowej gotowości śledczej (*Digital Forensic Readiness*, DFR). Pierwotnie pojęcie *Forensic Readiness* dotyczyło zatem gotowości rozumianej jako zdolność pewnego środowiska (oprogramowania czy szerzej – systemu informatycznego) do pozyskiwania cyfrowych śladów dowodowych połączonej z minimalizacją kosztów ich

71 **Investigation** – application of examinations, analyses, and interpretation to aid understanding of an incident, ISO/IEC 27041:2015-3.7.

72 J. Tan, *Forensic Readiness*, 2001, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f7e0e2ef046f7755d2f7e6d (dostęp: 5 stycznia 2025).

analizy, odnosiło się więc do aspektów technicznych. Sam artykuł[73] omawiał zresztą takie aspekty, jak: pliki historii (logi) w różnych systemach operacyjnych, znaczniki czasu, systemy wykrywania włamań (IDS – *Intruder Detecion Systems*) itd. Podobnie jak miało to miejsce niejednokrotnie w przypadku innych pojęć pierwotnie dotyczących informatyki – np. podejścia zwinnego (*agile*) czy interoperacyjności – również pojęcie cyfrowej gotowości śledczej (*Digital Forensic Readiness*, DFR) rozszerzyło swój zakres pojęciowy i we współczesnym rozumieniu obejmuje nie tylko poszczególne programy czy systemy, nie tylko system informatyczny (*Information Processing System*[74]), a więc skomputeryzowaną część systemu informacyjnego organizacji, czy nawet nie tylko całość jej systemu informacyjnego (*Information System*[75]), ale całość organizacji. **Cyfrowa gotowość śledcza** to zdolność organizacji do wyprzedzającego maksymalizowania wykorzystania dowodów cyfrowych przy jednoczesnym minimalizowaniu kosztów dochodzenia[76].

Sensu largo gotowość śledcza dotyczy zatem nie tylko możliwości i ekonomicznej efektywności technicznego procesu zbierania śladów dowodowych, ale i wielu innych zagadnień, np. zarządzania ciągłością działania (*Continuity Management*), która może być zakłócona nie tylko przez sam incydent, ale i przez działania dochodzeniowe, odpowiedzialności społecznej (w tym konieczności ochrony osób poszkodowanych na skutek wystąpienia incydentu bezpieczeństwa informacji tak, aby nie dopuścić np. do zjawiska wtórnej wiktymizacji przy ujawnianiu danych związanych z przestępstwem), która uwzględniona musi być również w trakcie prowadzonego postępowania, a nawet w ramach podjęcia decyzji o jego rozpoczęciu bądź zaniechaniu, zgodności z wymogami prawnymi i regulacjami branżowymi (zasady wykorzystania danych telekomunikacyjnych[77], ochrona danych osobowych, tajemnic zawodowych itd.) i innych.

73 *Ibidem*.

74 **Information processing system** – one or more data processing systems and devices, such as office and communication equipment, that perform information processing. ISO/IEC 2382:2015-2121292.

75 **Information system** – information processing system, together with associated organizational resources such as human, technical, and financial resources, that provides and distributes information. ISO/IEC 2382:2015-2121292.

76 J. Sachowski, *Implementing Digital Forensic Readiness*, Elsevier Inc. 2016, s. 45.

77 Zob. np. D. Wilk, *Telefony komórkowe i sieci telekomunikacyjne jako źródło informacji dla organów ścigania*, [w:] V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz, *Kryminalistyka a nowoczesne technologie*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2019, s. 333–356.

2. Współczesne uwarunkowania zarządzania bezpieczeństwem informacji

2.1. Złożoność, dynamika, niepewność

Pierwszą cechą charakterystyczną dla problematyki bezpieczeństwa informacji (ewentualnie cyberbezpieczeństwa) jest jej złożoność. Stąd popularność rozmaitych „map drogowych", które próbują schematycznie usystematyzować, czy to całość problematyki[1], czy tylko jej poszczególne aspekty, np. certyfikaty i szkolenia[2] czy nawet poszczególne rynki[3], jak również innych narzędzi, które mają wspomagać zainteresowanych w zorientowaniu się w bieżącej sytuacji w interesującym ich aspekcie bezpieczeństwa informacji. Wykorzystanie pozawerbalnych metod przekazu poprawia oczywiście komunikatywność takich publikacji, natomiast częste aktualizacje dają możliwość zachowania ich merytorycznej wartości pomimo zachodzących zmian. Czasami wizualizacje publikowane są w formie interaktywnej i uaktualnianej na bieżąco (czy to w sposób automatyczny, czy manualny). Jako przykłady mogą posłużyć: interaktywna mapa narodowych strategii cyberbezpieczeństwa[4] opracowana przez ENISA (European Union Agency for Cybersecuruity) odzwierciedlająca sytuację prawną w poszczególnych krajach UE, czy mapy zagrożeń i ataków (w dużej mierze służące wizualizacji działalności botnetów) publikowane przez producentów oprogramowania i urządzeń zabezpieczających,

1 Zob. np. Henry Jiang, https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/ (dostęp: 5 stycznia 2025).

2 Zob. np. Paul Jerimy, https://pauljerimy.com/security-certification-roadmap/ (dostęp: 5 stycznia 2025).

3 Zob. np. The Periodic Table Of Cybersecurity, https://www.cbinsights.com/research/periodic-table-cybersecurity; Canadian Cybersecurity Startup Ecosystem, https://www.serene-risc.ca/en/canadian-cybersecurity-startup-ecosystem (dostęp: 5 stycznia 2025).

4 Zob. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (dostęp: 5 stycznia 2025).

w oparciu o raporty zbierane z sensorów systemów detekcji, np. https://threatmap.checkpoint.com czy http://threatmap.fortiguard.com (listę takich map różnych producentów można znaleźć np. na stronie College of Art and Scieces Indiana State University, https://www.indstate.edu/cas/cybersecurity/cybersecurity-resources/cybersecurity-real-time-live-threat-maps).

Drugą – obok złożoności problematyki – cechą charakterystyczną poruszanych zagadnień jest wysoka dynamika zdarzeń związanych z bezpieczeństwem informacji (w tym zarówno znalezionych podatności jak i przeprowadzonych ataków). Współczesna informatyka rozwija się w sposób i wymuszający częste zmiany, zarówno oprogramowania (w tym systemów operacyjnych), jak i sprzętu. W szczególności duża dynamika związana jest z podejściem zwinnym (*agile*) do tworzenia oprogramowania. Zużycie moralne sprzętu następuje o wiele szybciej niż jego zużycie techniczne, a czas życia poszczególnych wersji produktów (w tym czas świadczenia wsparcia, polegającego również na udostępnianiu poprawek bezpieczeństwa) jest relatywnie krótki. W konsekwencji wymuszana jest wymiana oprogramowania (korzystanie z niewspieranej wersji jest niebezpieczne) i sprzętu (nowsza wersja oprogramowania może nie być zgodna ze starszym sprzętem). W szczególności dotyczy to oprogramowania systemowego; dla przykładu system Windows od swojej premiery w 1985 roku do Windows 11 w 2021 roku miał tylko w głównych liniach rozwojowych (a więc bez Windows CE czy Xbox OS) 37 istotnych wersji, co oznacza średnio rokrocznie nową wersję. Również dynamika procesu wykrywania podatności w oprogramowaniu (zob. tabela 1) jest wysoka: obecnie średnio codziennie raportowane jest ponad pół setki[5] informacji o podatnościach (tylko w najpopularniejszych programach i systemach informatycznych), którymi specjaliści od bezpieczeństwa informacji w poszczególnych organizacjach muszą odpowiednio zarządzać na bieżąco, bo publikacja informacji o podatności w praktyce oznacza, że w ciągu kilku godzin pojawi się, lub – jeśli mowa o atakach dnia zerowego (*Zero-day*) – już się pojawił, atak z niej korzystający. Oczywiście zarządzanie takie musi być realizowane przy daleko idącym wsparciu odpowiednich narzędzi informatycznych[6].

Tabela 1. Liczba podatności w bazie CVE w kolejnych latach

Rok	Liczba	Dynamika rok do roku (w %)
1999	894	–
2000	1020	14
2001	1677	64
2002	2156	29
2003	1527	-29

5 Z niewiadomych przyczyn dane na stronie CVE ulegają czasami nieznacznym zmianom, co można prześledzić korzystając z Internet Wayback Machine.

6 Zob. np.: M. Szmit, A. Szmit, *Kilka uwag o zarządzaniu podatnościami*, [w:] L. Kiełtyka (red.), *Wykorzystanie technik informacyjnych w zarządzaniu*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023, s. 114.

Rok	Liczba	Dynamika rok do roku (w %)
2004	2451	61
2005	4935	101
2006	6610	34
2007	6520	-1
2008	5632	-14
2009	5736	2
2010	4653	-19
2011	4155	-11
2012	5297	27
2013	5191	-2
2014	7939	53
2015	6504	-18
2016	6454	-1
2017	14 714	128
2018	16 510	12
2019	17 305	5
2020	18 323	6
2021	20 153	10
2022	25 084	24
2023	29 066	16

Źródło: MITRE Common Vulnerabilities and Exposures, Browse Vulnerabilities By Date MITRE CVE (dane za lata 1999–2017 według wersji strony z 14 kwietnia 2020, https://web.archive.org/web/20200414041337/, https://www.cvedetails.com/browse-by-date.php, dane za lata 2018–2023 według wersji strony z 28 grudnia 2024, https://www.cvedetails.com/browse-by-date.php) (dostęp: 5 stycznia 2025).

Wysoka jest także dynamika kulturowych czy cywilizacyjnych implikacji upowszechniania narzędzi informatycznych i związanych z nimi naruszeń bezpieczeństwa. Dla przykładu w tabelach 2 i 3 zebrano statystyki sądowe (prawomocnie skazanych dorosłych z oskarżenia publicznego) i policyjne i dotyczące przestępstw z rozdziału XXXIII Kodeksu Karnego (przestępstwa przeciwko ochronie informacji). Statystyki policyjne odwołują się do pojęć wszczętych postępowań i stwierdzonych przestępstw; podawanie tych dwóch wielkości jest uzasadnione m.in. przez przyjęte zasady wszczynania i prowadzenia postępowań – np. w przypadku samobójstwa zawsze wszczynane jest postępowanie z artykułu dotyczącego doprowadzenia do samobójstwa (art. 151 KK), choć w znacznej części przypadków nie stwierdza się ostatecznie popełnienia przestępstwa. Z kolei stosunkowo często

w sprawach gospodarczych, choć wszczynane jest jedno postepowanie, to w konsekwencji dochodzi do ujawnienia wielu przestępstw. W związku z tym ze stosunku tych dwóch wielkości (wszczętych postępowań i stwierdzonych przestępstw) nie można wysnuwać prostych wniosków, czy to odnośnie do wykrywalności przestępstw, czy efektywności prowadzenia postępowań.

Należy w tym miejscu wyjaśnić kilka szczegółów odnośnie do sposobu opracowywania statystyk przestępczości informatycznej w Polsce:

- Statystyki publikowane i zbierane przez Ministerstwo Sprawiedliwości do 2020 roku dotyczą wyłącznie prawomocnie skazanych dorosłych (a więc nie zawierają informacji o przestępczości nieletnich), przy czym analiza jest prowadzona w okresach rocznych według czynu głównego. Ponieważ statystyka jest prowadzona w układzie chronologicznym, a nie według identyfikatorów spraw (sygnatury akt), nie można porównywać ze sobą liczby stwierdzonych przestępstw ze statystyk policyjnych z liczbą skazań ze statystyk Ministerstwa Sprawiedliwości (popełnienie przestępstwa, wszczęcie postępowania i ewentualne skazanie nie musiały mieć miejsca w tym samym roku, ponadto sprawcami jednego przestępstwa mogło być kilka osób). Dodatkowo istnieje możliwość zmiany kwalifikacji czynu przez sąd w trakcie postępowania sądowego (bądź w czasie postępowania przygotowawczego przez organ je prowadzący, np. przez prokuraturę). Ponadto jeszcze, jeżeli sprawca popełnił dwa lub więcej przestępstw, zanim zapadł pierwszy wyrok, chociażby nieprawomocny, co do któregokolwiek z tych przestępstw i wymierzono za nie kary tego samego rodzaju albo inne podlegające łączeniu, sąd orzeka karę łączną (art. 85 KK, tzw. ciąg przestępstw), a więc w statystyce osób skazanych będzie figurowała jedna osoba raz skazana, choć stwierdzonych czynów przestępnych mogło być bardzo wiele (zwłaszcza gdy mowa o przestępstwach komputerowych, a więc możliwych do popełnienia w sposób „zautomatyzowany" przez uruchomienie odpowiednich programów masowo rozsyłających czy to złośliwe kody czy sfałszowane informacje pod zadany, czy wręcz losowy zestaw adresów). Wszystko to powoduje, że głębsze analizy z wykorzystaniem takich danych są niemożliwe.
- Statystyki prawomocnie skazanych dorosłych nie obejmują skazań nieletnich (osób poniżej 18. roku życia) oraz skazań z oskarżenia prywatnego.
- Zgodnie z informacjami na stronach statystyk policji: „Do końca 2012 roku prezentowane dane zawierały zarówno informacje o postępowaniach przygotowawczych prowadzonych przez Policję, jak również o postępowaniach prowadzonych we własnym zakresie przez prokuraturę (bez udziału Policji). Od początku 2013 roku gromadzone są tylko informacje w oparciu o postępowania przygotowawcze prowadzone wyłącznie przez Policję. Zmienił się także sposób zbierania danych dotyczących nieletnich. Poprzednio czyny karalne nieletnich wykazywane były w momencie skierowania wniosku o wszczęcie postępowania do Sądu Rodzinnego i Nieletnich. Od początku 2013 roku dane prezentowane są po uzyskaniu informacji o wszczęciu i zakończeniu postępowania przez sędziego rodzinnego. Dane dotyczące 2014 roku wynikają z Rozporządzenia

Rady Ministrów z dnia 9 sierpnia 2013 r. w sprawie programu badań statystyki publicznej na rok 2014 (Dz. U. z 2013 r. poz. 1159), zgodnie z którym Ministerstwo Sprawiedliwości zostało zobowiązane do gromadzenia i przekazywania danych o osobach nieletnich i ich czynach karalnych jako organ mający informację o całości zagadnienia. Oznacza to, iż publikowane dane za 2014 rok nie zawierają informacji na temat czynów karalnych nieletnich".

- Kodeks Karny jest ustawą stosunkowo często nowelizowaną. Od chwili uchwalenia w 1997 roku do września 2024 roku uchwalono 116 aktów prawnych zmieniających jego brzmienie, co daje średnio ponad cztery ustawy zmieniające Kodeks Karny w ciągu roku. Oczywiście nie wszystkie z tych zmian dotyczą przestępstw przeciwko ochronie informacji, niemniej część z nich ma na nie wpływ (dla przykładu art. 269a oraz 269b mają statystyki prowadzone dopiero od roku 2005, wcześniej bowiem czyny opisane w ich dyspozycjach nie były penalizowane; w roku 2017 wprowadzono zmiany w Kodeksie Karnym, które dodały ustawowe kontratypy czynów zabronionych określonych w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a i art. 269b KK). Nawet artykuły takie jak art. 306a KK (penalizujący zmianę wskazań drogomierza lub ingerencję w prawidłowość jego pomiaru, a wprowadzony w roku 2019) mogą stać się *lex specialis* do artykułów dotyczących naruszania integralności informacji, jeśli mowa o drogomierzach cyfrowych.
- Statystyki skazań prowadzone są na poziomie paragrafów KK, nie ma możliwości ustalenia, jaka liczba czynów przestępnych przeciwko bezpieczeństwu informacji dotyczy przestępstw „komputerowych", a jaka „papierowych". Na przykład w odniesieniu do artykułu 267 KK stypizowane w nim przestępstwa dotyczyć mogą zarówno informacji przesyłanej i przetwarzanej w systemach komputerowych, jak i – przy użyciu tradycyjnych („papierowych") metod.

W przedstawionych danych da się zauważyć rosnący poziom przestępczości (a przynajmniej tej jej części, która staje się przedmiotem zainteresowania sądów i organów ścigania): od nieco ponad półtorej setki stwierdzonych przestępstw przeciwko ochronie informacji w 1999 roku do prawie sześciu i pół tysiąca w roku 2020; od 71 skazań w roku 2006 do 138 w roku 2020. Trudno tu jednak o jakieś głębsze wnioski statystyczne (formalnie dyscypliną – w zasadzie postulowaną, trudno bowiem mówić, żeby – przynajmniej w polskich warunkach istniała ona rzeczywiście – zajmującą się pomiarami i modelowaniem statystycznym zjawisk związanych ze stosowaniem prawa jest prawometria[7]), bowiem nawet tak – wydawałoby się – elementarne dane, jak widać, są niekompletne i trudne do interpretacji i to nie tylko z powodów immanentnie związanych z samą naturą pomiarów przestępczości, ale i z powodu dość wybiórczego zbierania danych przez organy państwa. Dla przykładu w ogóle nie są zbierane statystyki dotyczące pozakodeksowych przestępstw

7 Zob. np. M. Szmit (red.), A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec, *Elementy Informatyki Sądowej*, Polskie Towarzystwo Informatyczne, Warszawa 2011, s. 21. O problemach metodologicznych związanych z pomiarami przestępczości zob. np. J. Błachut, *Problemy związane z pomiarem przestępczości*, Wolters Kluwer Polska, Kraków 2007, passim.

komputerowych, a więc np. czynów stypizowanych w art. 12 Ustawy z dnia 27 lipca 2001 roku o ochronie baz danych (t.j. Dz. U. z 2021 r. poz. 386, z 2024 r. poz. 1254) czy art. 6 oraz art. 7 Ustawy z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (t.j. Dz. U. z 2015 r. poz. 1341, z 2024 r. poz. 1222). Od 2021 roku zmianie uległ sposób zbierania i prezentowania danych statystycznych dotyczących przestępczości. Zgodnie z zarządzeniem Ministra Sprawiedliwości z dnia 19 stycznia 2021 roku w sprawie wzorów formularzy statystycznych w sądach powszechnych i wojskowych (Dz. U. M. S. poz. 4) wszystkie sądy powszechne i wojskowe mają obowiązek przygotować odpowiednie zestawienia statystyczne dotyczące między innymi przestępstw i przekazać je do Ministerstwa Sprawiedliwości. Poszczególne sądy publikują zazwyczaj również odpowiednie zestawienia na swoich stronach www, natomiast kompletne zestawienie zbiorcze zostało – do chwili pisania książki – opublikowane przez Ministerstwo Sprawiedliwości tylko dla roku 2023. O ile do roku 2020 publikowane były informacje o liczbie prawomocnie skazanych dorosłych, o tyle w nowym zestawieniu publikowane są dane o liczbie skazanych (niezależnie od wieku, a więc i dorosłych i nieletnich), w pierwszej instancji, a więc również i tych, którzy – po zastosowaniu zwyczajnych środków odwoławczych – uzyskają zmianę wyroku w drugiej instancji na uniewinnienie lub umorzenie, choć więc dane z 2023 roku (zob. tabela 4) są bardziej szczegółowe, nie da się z nich wyliczyć wartości poprzednio badanej cechy statystycznej, a zatem nie da się scharakteryzować dynamiki jej zmian.

Dodatkowo również zmiany w innych ustawach (niebędących nowelizacjami Kodeksu karnego) mogą mieć wpływ na statystyki dotyczące przestępczości komputerowej. Dla przykładu, Ustawa z dnia 19 czerwca 2020 roku o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz. U. z 2020 r. poz. 1086 ze zm., tzw. Tarcza 4.0), wprowadziła m.in. w artykule 26 ust. 1 nowy rodzaj wykroczenia (art. 107a Kodeksu Wykroczeń), penalizującego tzw. zoombombing (zakłócanie spotkań internetowych, w szczególności zdalnych lekcji, poprzez udostępnianie ekranu zawierającego nieprzyzwoite treści). Jak sygnalizowano w literaturze przedmiotu[8], podobieństwo ustawowych znamion czynów zabronionych określonych w dyspozycji tego artykułu oraz w artykułach 268 i 268a KK może powodować w niektórych przypadkach istotne trudności z subsumpcją konkretnych czynów, a nawet prowadzić do wniosku, że art. 107a Kodeksu Wykroczeń stanowi w istocie *lex specialis* w stosunku do artykułów 268 bądź 268a KK. Rzeczywiście z art. 268 KK nie było żadnego skazania w 2023 roku. Być może

8 Zob. np. M. Sewastianowicz, *Grzywną w nieproszonego gościa na Zoom party*, Prawo.pl 30.05.2020, https://www.prawo.pl/oswiata/grzywna-za-przerywanie-zdalnych-lekcji-wykroczenie,500657.html (dostęp: 5 stycznia 2025); K. Wala, *Ratio legis oraz analiza ustawowych znamion wykroczenia z art. 107a k.w.*, „Prokuratura i Prawo" 2021, nr 3, s 68–90; M. Szmit, *O pewnym nowym przepisie i jednym precedensowym wyroku*, „Rocznik Bezpieczeństwa Morskiego" 2021, s. 195–208.

więc rzeczywiście wykroczenie zoombombingu „skonsumowało" przestępstwo utrudniania zapoznania się z informacją[9] (zob. tabela 5).

Tabela 2. Statystyki policyjne wybranych przestępstw przeciwko ochronie informacji: liczba postępowań wszczętych i przestępstw stwierdzonych przez policję

Rok	Naruszenie tajemnicy korespondencji (art. 267)		Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)		Niszczenie danych informatycznych (art. 269)		Sabotaż komputerowy (art. 269a)		Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)	
	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
1999	182	113	59	49	10	1	–	–	–	–
2000	249	240	66	48	7	5	–	–	–	–
2001	259	175	60	118	9	5	–	–	–	–
2002	294	215	89	167	6	12	–	–	–	–
2003	362	232	114	138	2	2	–	–	–	–
2004	378	248	105	89	12	0	–	–	–	–
2005	430	260	152	98	2	3	1	1	6	6
2006	538	370	201	136	3	4	19	19	9	9
2007	616	384	244	168	6	0	11	11	4	4
2008	694	505	366	249	6	2	13	13	12	12
2009	982	645	555	1115	6	2	34	243	23	18
2010	1194	1102	690	479	7	0	22	18	35	71
2011	1583	948	885	629	3	5	38	30	38	29
2012	1657	1513	796	884	9	5	35	30	21	27
2013	2203	1655	765	589	14	9	37	34	42	28
2014	2868	1901	743	572	10	6	27	48	47	43
2015	3515	2452	759	579	4	4	52	38	58	44
2016	3401	2718	712	789	11	6	44	38	36	39
2017	3419	2503	654	703	13	3	39	34	28	24
2018	3676	2597	530	2432	9	6	51	41	29	34
2019	6718	5196	868	642	17	9	37	34	55	39
2020	7017	5663	911	761	9	7	33	20	49	41

Źródło: https://statystyka.policja.pl (dostęp: 5 stycznia 2025).

9 Zob. M. Szmit, *Przestępczość teleinformatyczna – garść statystyk*, referat wygłoszony na 6. Konferencji Przestępczość Teleinformatyczna XXI w., Gdynia 23 maja 2024 r.

Tabela 3. Statystyki skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba prawomocnych skazań osób dorosłych za przestępstwa komputerowe – czyn główny sądzony z oskarżenia publicznego

Rok	Naruszenie tajemnicy korespondencji (art. 267)								Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)						Niszczenie danych informatycznych (art. 269)		Sabotaż komputerowy (art. 269a)	Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)			
	Art. 267 §1 kk	Art. 267 §2 kk	Art. 267 §3 kk	Art. 267 §3 kk w zw. z §1	Art. 267 §4 kk	Art. 267 §4 kk w zw. z §1	Art. 267 §4 kk w zw. z §2	Art. 267 §4 kk w zw. z §3	Art. 268 §1 kk	Art. 268 §2 kk	Art. 268 §3 kk	Art. 268 §3 kk w zw. z §1	Art. 268a §1 kk	Art. 268a §2 kk	Art. 269 §1 kk	Art. 269 §2 kk	Art. 269a kk	Art. 269b §1 kk	Art. 269b §1 kk w zw. z Art. 165 §1 pkt 4 kk	Art. 269b §1 kk w zw. z Art. 268a §1 kk	Art. 269b §1 kk w zw. z Art. 269a kk
2006	22	8	–	13	–	–	–	–	14	7	–	1	3	–	–	1	1	–	–	–	1
2007	23	16	1	3	–	–	–	–	11	7	–	–	9	–	3	–	2	–	–	–	–
2008	29	6	1	–	–	–	–	–	19	13	–	–	17	–	1	2	1	–	–	1	–
2009	42	3	1	3	1	–	–	–	13	5	–	–	25	–	–	1	2	3	–	–	–
2010	52	–	11	4	1	–	–	–	12	11	1	–	33	1	1	1	3	1	–	–	–
2011	37	1	7	–	–	–	–	–	12	5	2	–	40	–	–	–	6	4	–	–	–
2012	49	3	14	–	1	5	–	–	8	2	–	–	28	–	–	–	3	2	–	–	1
2013	47	2	6	–	–	1	–	–	4	5	–	–	22	–	–	–	4	1	–	–	–
2014	44	–	11	–	–	–	–	–	5	6	1	–	18	–	–	–	1	1	–	–	–
2015	35	1	21	–	–	–	–	–	7	3	1	–	24	–	–	–	4	1	–	–	–
2016	52	5	25	–	2	1	–	–	15	5	1	–	16	–	–	–	2	2	–	–	–
2017	50	2	39	–	2	–	–	–	11	3	1	–	15	–	1	–	–	3	1	–	–

Rok	Naruszenie tajemnicy korespondencji (art. 267)								Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)						Niszczenie danych informatycznych (art. 269)		Sabotaż komputerowy (art. 269a)	Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)			
	Art. 267 §1 kk	Art. 267 §2 kk	Art. 267 §3 kk	Art. 267 §3 kk w zw. z §1	Art. 267 §4 kk	Art. 267 §4 kk w zw. z §1	Art. 267 §4 kk w zw. z §2	Art. 267 §4 kk w zw. z §3	Art. 268 §1 kk	Art. 268 §2 kk	Art. 268 §3 kk	Art. 268 §3 kk w zw. z §1	Art. 268a §1 kk	Art. 268a §2 kk	Art. 269 §1 kk	Art. 269 §2 kk	Art. 269a kk	Art. 269b §1 kk	Art. 269b §1 kk w zw. z Art. 165 §1 pkt 4 kk	Art. 269b §1 kk w zw. z Art. 268a §1 kk	Art. 269b §1 kk w zw. z Art. 269a kk
2018	59	9	41	–	3	3	–	2	4	7	–	–	20	–	–	–	1	3	–	–	–
2019	65	4	51	–	–	1	1	–	8	1	–	–	17	–	1	–	4	2	–	–	–
2020	45	6	50	–	1	2		2	9	3	–	–	15	1	1	–	–	3	–	–	–

Źródło: dane za lata 2006–2007 za: M. Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, wyd. II rozszerzone i uzupełnione, Polskie Towarzystwo Informatyczne, Warszawa 2014, s. 131 i nast.[10] Skazania w latach 2008–2020 wg: Informator Statystyczny Wymiaru Sprawiedliwości (arkusz „Skazania prawomocne z oskarżenia publicznego – dorośli – wg rodzajów przestępstw i wymiaru kary w l. 2008-2020"), https://isws.ms.gov.pl (dostęp: 5 stycznia 2025).

10 Opublikowane tamże były dane ówcześnie udostępnione przez Ministerstwo Sprawiedliwości oraz dane zawarte w odpowiedzi sekretarza stanu w Ministerstwie Sprawiedliwości na interpelację nr 15805 w sprawie internetowych przestępstw komputerowych (http://orka2.sejm.gov.pl/IZ6.nsf/main/7B767D38 [dostęp: 5 stycznia 2025]), gdzie ujawniono część danych ukrytych w statystykach Ministerstwa z uwagi na tajemnicę statystyczną (w tym konkretnym przypadku ukrywano niskie liczby skazań, bowiem uznano, że przy toczących się w skali kraju pojedynczych sprawach publikacja informacji o samym fakcie skazania mogła naruszać dobra osobiste skazańców).

Tabela 4. Statystyki skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba osób osądzonych oraz skazanych za przestępstwa komputerowe

Rok	Art. 267 §1 kk		Art. 268a kk		Art. 269 kk		Art. 269a KK		Art. 269b KK	
	Osądzonych	Skazanych	Osądzonych	Skazanych	Osądzonych	Skazanych	Osądzonych	Skazanych	Osądzonych	Skazanych
2023	159	98	45	32	3	3	4	2	21	5

Źródło: Informator Statystyczny Wymiaru Sprawiedliwości, https://isws.ms.gov.pl (dostęp: 5 stycznia 2025).

Tabela 5. Statystyki dotyczące wykroczenia zoomboombingu (art. 107a KW) skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba osób osądzonych oraz skazanych za przestępstwa komputerowe

Rok	Art. 107a KW				
	Wszczętych	Osądzonych	Skazanych	Umorzono postępowań	Uniewinniono
2023	65	70	54	4	2

Źródło: Informator Statystyczny Wymiaru Sprawiedliwości, https://isws.ms.gov.pl (dostęp: 5 stycznia 2025).

Jeśli – przy wszystkich zastrzeżeniach, o których wspomniano wcześniej – zestawienie rzędów wielkości liczby stwierdzonych w ostatnich latach przestępstw do liczby skazań (tysiące przestępstw versus nieco ponad setka skazań) może stwarzać wrażenie dużego kontrastu, do jeszcze bardziej niepokojących wniosków prowadzi zestawienie tych wielkości z liczbami alertów raportowanych przez zespoły CERT (*Computer Emergency Readiness Teams* – wcześniej w literaturze anglojęzycznej stosowano rozwinięcie *Computer Emergency Response Teams*, zmianę tłumaczenia można uznać za symptomatyczną o tyle, że zespoły CERT nie powinny zajmować się wyłącznie reakcją na już zaistniałe zdarzenia, w literaturze krajowej jednak nadal mówi się głównie o reakcji na incydenty i – osobno niejako – o zespołach CSIRT, tj. *Computer Security Incident Response Team*). W szczególności w tabeli 6 podano statystyki incydentów CERT.PL stanowiącego od 2018 roku część Krajowego Systemu Cyberbezpieczeństwa. CERT PL jest zespołem Naukowej Akademickiej Sieci Komputerowa Państwowego Instytutu Badawczego, NASK realizującym część zadań CSIRT NASK opisanych w art. 26 Ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Naukowa Akademicka Sieć Komputerowa podlegała wielu zmianom, technicznym, organizacyjnym i prawnym, których omawianie wykracza poza zakres poruszanej tematyki, a które powodują, że trudno jest ze sobą porównywać statystyki z kolejnych lat; warto tylko wspomnieć o wprowadzonym w roku 2005 systemie wczesnego ostrzegania o zagrożeniach (ARAKIS) wykorzystującym umieszczone w różnych miejscach sieci sensory, co – jak zresztą ujęli sami autorzy raportów CERT.PL spowodowało, że statystyki z roku 2005 są „jakościowo inne od statystyk z lat poprzednich"; system ARAKIS,

oczywiście już w zupełnie innej postaci jest rozwijany do dziś jako Arakis 2.0, m.in. w wersji Enterprise[11]. Zgodnie z ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa wybrane podmioty mają obowiązek zgłaszania incydentów odpowiednio, w zależności od rodzaju tych podmiotów, do CSIRT MON, CSIRT NASK (którego funkcję pełni CERT.PL) bądź CSIRT GOV. CERT.PL stosuje obecnie VI wersję klasyfikacji przyjętej przez European CSIRT Network[12], klasyfikacja ta nie jest tożsama z ustawowymi znamionami czynów stypizowanych w Kodeksie karnym, o których mowa we wcześniejszych tabelach.

Tabela 6. Wybrane statystyki incydentów CERT.PL

Rok	Atak blokujący serwis (DoS)	Rozproszony atak blokujący serwis (DDoS)	Sabotaż komputerowy	Złośliwe oprogramowanie	Ogólna liczba incydentów	Dynamika rok do roku (w %)
1996	–	–	–	–	50	–
1997	–	–	–	–	75	50
1998	–	–	–	–	100	33
1999	–	–	–	–	105	5
2000	–	–	–	–	126	20
2001	–	–	–	–	741	488
2002	–	–	–	–	1013	37
2003	10	10	0	80	1196	18
2004	15	62	0	165	1222	2
2005	13	14	1	594	2516	106
2006	20	19	1	340	2427	-4
2007	8	32	0	295	2108	-13
2008	4	22	0	276	1796	-15
2009	5	11	0	193	1292	-28
2010	1	10	0	91	674	-48
2011	3	11	0	46	605	-10
2012	8	17	0	226	1082	79
2013	0	43	0	746	1219	13
2014	6	63	0	98	1282	5
2015	2	33	0	142	1456	14
2016	3	30	2	211	1926	32
2017	11	41	0	854	3182	65

11 Zob. https://www.arakis.pl (dostęp: 5 stycznia 2025).

12 Zob. Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (dostęp: 5 stycznia 2025).

Tab. 6 (cd.)

Rok	Atak blokujący serwis (DoS)	Rozproszony atak blokujący serwis (DDoS)	Sabotaż komputerowy	Złośliwe oprogramowanie	Ogólna liczba incydentów	Dynamika rok do roku (w %)
2018	7	35	0	862	3739	18
2019	4	33	1	969	6484	73
2020	0	43	0	746	10 420	61
2021	6	74	1	2847	29 483	183
2022	6	97	0	3409	39 683	35
2023[a]	–	–	–	1650[b]	80 267	102

[a] W raporcie z 2023 roku podano statystyki na wyższym poziomie agregacji tej samej klasyfikacji, stąd brak części danych. Warto odnotować, że w roku 2023 niemal 95% incydentów (75 917 szt.) zaliczono do kategorii „oszustwa komputerowe".
[b] Opisane jako „szkodliwe oprogramowanie".

Źródło: Raport roczny z działalności CERT Polska 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf; Raport roczny z działalności CERT Polska 2022. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2022.pdf; Raport roczny z działalności CERT Polska 2021. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2021.pdf; Raport roczny z działalności CERT Polska 2020. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2020.pdf; Raport roczny z działalności CERT Polska 2019. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2019.pdf; Raport roczny z działalności CERT Polska 2018. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2018.pdf; Raport roczny z działalności CERT Polska 2017. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2017.pdf; Raport roczny z działalności CERT Polska 2016. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2016.pdf; Raport roczny z działalności CERT Polska 2015. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2015.pdf; CERT Polska Raport 2014, https://cert.pl/uploads/docs/Raport_CP_2014.pdf; CERT Polska Raport 2013, https://cert.pl/uploads/docs/Raport_CP_2013.pdf; Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, https://cert.pl/uploads/docs/Raport_CP_2012.pdf; Raport 2011 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011, https://cert.pl/uploads/docs/Raport_CP_2011.pdf; Raport 2010 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, https://cert.pl/uploads/docs/Raport_CP_2010.pdf; Raport 2009 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2009, https://cert.pl/uploads/docs/Raport_CP_2009.pdf; Raport 2008 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2008, https://cert.pl/uploads/docs/Raport_CP_2008.pdf; Raport 2007 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2007, https://cert.pl/uploads/docs/Raport_CP_2007.pdf; Raport 2006 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2006, https://cert.pl/uploads/docs/Raport_CP_2006.pdf; Raport 2005 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2005, https://cert.pl/uploads/docs/Raport_CP_2005.pdf; Raport 2004 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2004, https://cert.pl/uploads/docs/Raport_CP_2004.pdf; Raport 2003 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2003, https://cert.pl/uploads/docs/Raport_CP_2003.pdf (dostęp: 5 stycznia 2025).

W kolejnej tabeli (tabela 7) zebrano statystyki zespołu cert.gov.pl. CERT.GOV.PL (Rządowy Zespół Reagowania na Incydenty Komputerowe) został powołany w dniu 1 lutego 2008 roku na mocy porozumienia Ministra Spraw Wewnętrznych i Administracji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego. Od wejścia w życie ustawy z dnia 5 lipca 2018 roku o Krajowym Systemie Cyberbezpieczeństwa funkcjonuje jako CSIRT GOV[13]. W ostatniej kolumnie tabeli pokazano iloraz liczby incydentów przez liczbę zgłoszeń, jest to spowodowane tym, że występuje istotna różnica pomiędzy liczbą zgłoszeń a liczbą stwierdzonych incydentów spowodowana zarówno przez sytuacje wystąpienia błędów pierwszego rodzaju (*false positive*), tj. zgłoszenia sytuacji, w której nie było rzeczywistego incydentu, jak i z kilku zgłoszeń dla jednego incydentu (np. kilka podmiotów dotkniętych pojedynczym incydentem zgłasza niezależnie fakt jego wystąpienia). Niezależnie od tego głównym źródłem zgłoszeń raportowanych przez CERT.PL jest, wspomniany wcześniej, system wczesnego ostrzegania o zagrożeniach ARAKIS GOV. Według raportu CERT PL za rok 2022 z tego systemu pochodziło 1 207 287 zgłoszeń (a więc 97,87% zgłoszeń) i 16 604 incydentów (77,00%). Z jednej strony jest to niewątpliwie bardzo duży odsetek wykrytych incydentów, ale z drugiej – nieduża precyzja (formalnie można by ją obliczyć stosunek liczby wyników prawdziwie pozytywnych do sumy wyników prawdziwie pozytywnych i fałszywie pozytywnych, zatem jako iloraz liczby incydentów do liczby zgłoszeń, co daje wynik 1,38%; dla wszystkich pozostałych zgłoszeń i incydentów iloraz ten wynosi 18,54%).

Tabela 7. Wybrane statystyki incydentów CERT.GOV.PL

Rok	Atak blokujący serwis (DoS)	Rozproszony atak blokujący serwis (DDoS)	Złośliwe oprogramowanie	Ogólna liczba incydentów	Liczba zgłoszeń	Iloraz liczby incydentów przez liczbę zgłoszeń (w %)
2010	1	1	27[a]	155 (146)[b]	621	24,96
2011	4	3	32[c]	249	854	29,16
2012	8	23[d]	85[e]	457	1168	39,13
2013	2	8	4318[f]	5670	8817	64,31
2014	20[g]		5763	7498	12 017	–
2015	–	–	4368[h]	8914	16 123	55,29
2016	–	76	3376[i]	9288	19 954	46,55
2017	–	98	3715[j]	5819	28 281	20,58
2018	275[k]		2936[l]	6236	31 865	–
2019	–[m]	9	7256[n]	12 405	226 914	5,47
2020	–[o]	–	16 813[p]	23 309	246 107	9,47
2021	–[r]	–	24 187[s]	26 899	762 175	3,53

13 Zob. https://csirt.gov.pl (dostęp: 5 stycznia 2025).

Tab. 7 (cd.)

Rok	Atak blokujący serwis (DoS)	Rozproszony atak blokujący serwis (DDoS)	Złośliwe oprogramowanie	Ogólna liczba incydentów	Liczba zgłoszeń	Iloraz liczby incydentów przez liczbę zgłoszeń (w %)
2022	–[t]	–	61[u]	21 563	1 234 040	1,75
2023	–	–	37	43 785	322 656	13,6

[a] Suma wymienionych w oryginalnym raporcie kategorii: „Wirusy", „Robak sieciowy", „Botnety", „Koń trojański", „Oprogramowanie szpiegowskie".
[b] W oryginalnym raporcie uwzględniono dodatkowo zgłoszenia dziewięciu incydentów ćwiczebnych związanych z uczestnictwem zespołu CERT.GOV.PL w ćwiczeniach NATO „Cyber Coalition 2010".
[c] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Robak sieciowy", „Botnets", „Koń Trojański", „Oprogramowanie szpiegowskie".
[d] Rok 2011 był rokiem protestów przeciwko umowie ACTA, w których wykorzystywane było m.in. oprogramowanie LOIC (Low Orbit Ion Cannon) umożliwiające prowadzenie takich ataków praktycznie bez jakiejkolwiek wiedzy technicznej.
[e] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Botnety", „Koń Trojański".
[f] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Robak sieciowy", „Botnety", Koń Trojański, Oprogramowanie szpiegowskie.
[g] W raporcie podano sumaryczną liczbę ataków DoS i DDoS.
[h] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Klient botnetu".
[i] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Klient botnet".
[j] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Klient botnet".
[k] W oryginalnym raporcie opisane jako „niedostępność". Jest to nie do końca zrozumiała kategoria, ponieważ sama niedostępność usługi (ang. *unavailability*) usługi jest stanem, który może mieć różne przyczyny, np. błąd ludzki, awaria urządzenia, brak zasilania, skuteczny atak DoS (czy jego odmiany DDoS czy DRDoS) itd., a raport nie zawiera szczegółowego opisu tej kategorii.
[l] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Botnet".
[m] Odnotowano 290 incydentów opisanych jako „niedostępność".
[n] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Botnet".
[o] Odnotowano 254 incydentów opisanych jako „niedostępność".
[p] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Botnet".
[r] Odnotowano 310 incydentów opisanych jako „niedostępność".
[s] Suma wymienionych w oryginalnym raporcie kategorii: „Wirus", „Botnet".
[t] Odnotowano 826 incydentów opisanych jako „niedostępność" z komentarzem „o kategorii NIEDOSTĘPNOŚĆ zakwalifikowano incydenty polegające na niedostępności witryn internetowych, wynikających zarówno z ataków DDoS, jak również awarii czy wykonywanych prac technicznych".
[u] Raport z 2022 roku zawiera tylko jedną kategorię złośliwego oprogramowania („Wirus').

Źródło: Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku, https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku, https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku, https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku, https://csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.

pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku, https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku, https://csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2016roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku, https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku, https://csirt.gov.pl/download/3/191/RaportostaniebezpieczenstwacyberprzestrzeniRPw2018roku.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, https://csirt.gov.pl/download/3/199/raportostaniebezpieczenstwacyberprzestrzenirp2019.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku, https://csirt.gov.pl/download/3/201/RaportostaniebezpieczenstwacyberprzestrzeniRPw2020.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku, https://csirt.gov.pl/download/3/204/RaportostaniebezpieczenstwacyberprzestrzeniRPw2021compressed.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku, https://csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf; Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf (dostęp: 5 stycznia 2025).

Zwraca uwagę duża zmienność (w przeciwieństwie do CERT.PL) sposobu opisywania zdarzeń związanych z bezpieczeństwem informacji oraz incydentów bezpieczeństwa informacji. Co więcej, użyta typologia wydaje się wątpliwa z uwagi na nierozłączność poszczególnych klas (a co do zasady klasyfikacja jednopoziomowa powinna spełniać formalny warunek jednoznaczności). Dla przykładu: w poszczególnych latach występują obok siebie takie kategorie, jak „atak" i „niedostępność" (choć oczywiście niedostępność usługi może być skutkiem ataku), „niedostępność" i „DDoS" (choć rozproszony atak odmowy usług jest właśnie atakiem przeciw dostępności), pojęcia takie jak „podatność" (choć podatność sama w sobie nie jest incydentem bezpieczeństwa informacji, może nim być wykorzystanie podatności) itd. Oczywiście w praktyce w momencie zgłoszenia zdarzenia związanego z bezpieczeństwem informacji, a nawet w momencie uznania go za incydent, zespół CERT może nie mieć wiedzy wystarczającej do zrozumienia i wytłumaczenia mechanizmu zdarzenia. Zauważone jest zdarzenie (fenomen), np. wybitnie zwiększony ruch sieciowy, natomiast ustalenie jego przyczyn (np. awaria sprzętowa, atak DoS, DDoS, DRDoS itd.) wymaga już często głębszej analizy, która nie zawsze jest prowadzona lub o wynikach której CERT.PL nie musi być informowany, niemniej można albo prowadzić statystyki na podstawie pierwotnej wstępnej klasyfikacji, albo bazując na ustaleniach po zakończeniu postępowania postincydentalnego, bowiem niejednoznaczność klasyfikacji jest błędem.

Trzeci z wymienionych w ustawie zespołów – CERT MIL – nie publikuje informacji statystycznych o incydentach.

Do ciekawych wniosków prowadzi zestawienie liczby incydentów z raportów zespołów CSIRT prowadzonych przez administrację państwową z danymi zbieranymi przez największych operatorów internetowych. Dla przykładu CERT firmy

Orange Polska – największego polskiego operatora telekomunikacyjnego i jednego z największych krajowych dostawców Internetu (który jednak nie publikuje szczegółowych danych bezwzględnych, dla większości cech statystycznych podawane są informacje względne, tj. o procentowej zmianie np. liczby incydentów rok do roku, więc po raz kolejny nie ma możliwości bezpośredniego porównania danych z różnych źródeł) – w 2021 zablokował około 150 tysięcy domen phishingowych i ponad 300 milionów prób wejść na takie, wygenerowanych przez ponad 4,5 miliona unikatowych użytkowników (w roku 2023 było to już 350 tysięcy zablokowanych domen i 5,5 miliona użytkowników), w roku 2020 system ochrony przed atakami DDoS interweniował ponad 65 tysięcy razy w sieci stacjonarnej i 12,5 tysiąca razy w sieci mobilnej, w roku 2020 wykryto 3 083 720 sytuacji Malware callback (połączenie od złośliwego kodu zainstalowanego na komputerze ofiary ze zdalnym serwerem zarządzającym złośliwym oprogramowaniem)[14].

Z przytoczonych statystyk wyłania się więc obraz, w którym – w skali kraju – rokrocznie (w latach 20. XXI wieku) dochodzi do dziesiątek i setek milionów zdarzeń związanych z bezpieczeństwem informacji, z czego miliony okazują się rzeczywistymi incydentami bezpieczeństwa informacji, w krajowym systemie cyberbezpieczeństwa identyfikowanych jest dziesiątki tysięcy incydentów, do organów ścigania trafiają informacje jedynie o tysiącach popełnionych przestępstw, a w końcu zapada nieco ponad setka wyroków skazujących rocznie. Oczywiście, taki obraz musi być opatrzony wieloma zastrzeżeniami: jedna osoba może łatwo – posługując się złośliwym oprogramowaniem – wygenerować dziesiątki i setki tysięcy zdarzeń związanych z naruszaniem bezpieczeństwa informacji, spora część ataków internetowych jest prowadzonych spoza granic Polski, co rodzi poważne trudności w ustaleniu i ściganiu sprawców, nie każdy incydent bezpieczeństwa musi być skutkiem działań przestępczych itd., niemniej nie sposób nie dojść do wniosku, że skuteczność karno-prawnych mechanizmów ochrony bezpieczeństwa informacji jest nieszczególnie wysoka. Być może jest pewną przesadą anglojęzyczna gra słów określająca stan cyberbezpieczeństwa globalnej sieci jako *Worldwide Wild West*, ale z pewnością można obecny stan rzeczy określić jako sytuację działania w warunkach wysokiego ryzyka, w tym ryzyka prawnego. Warto przy tym zauważyć, że w literaturze istnieją różne definicje ryzyka prawnego. Większość z nich koncentruje się w szczególności na skutkach niestosowalności w praktyce unormowań prawnych, trudności w egzekwowaniu prawa czy wręcz na skutkach prowadzenia przez przedsiębiorstwo działalności wykraczającej poza ramy odpowiednich przepisów prawa lub regulacji. *Sensu largo* ryzyko prawne obejmuje również skutki niespodziewanych zmian prawa, nieskuteczności prawa

14 Według: Raport CERT Orange Polska 2020, https://cert.orange.pl/pobierz-raport/19/1 (dostęp: 5 stycznia 2025); Raport CERT Orange Polska 2021, https://cert.orange.pl/pobierz-raport/21/1 (dostęp: 5 stycznia 2025); Raport CERT Orange Polska 2022, https://cert.orange.pl/pobierz-raport/22/1 (dostęp: 5 stycznia 2025); Raport CERT Orange Polska 2023, https://cert.orange.pl/wp-content/uploads/2024/04/Raport_CERT_Orange_Polska_2023.pdf (dostęp: 5 stycznia 2025).

bądź złego stanowienia prawa. Choć takie aspekty rozważa tylko część autorów[15], to w kontekście omawianej tematyki należy, jak się wydaje, zdecydowanie brać je pod uwagę.

Kolejną immanentną cechą problematyki bezpieczeństwa informacji jest wreszcie działanie w warunkach niepewności, spowodowanej – oprócz samej złożoności i dynamiki zdarzeń – również celową dezinformacją. Z oczywistych względów taka dezinformacja jest prowadzona przez organizacje przestępcze (np. w ramach ataków socjotechnicznych), ale również przez służby państwowe, choć w obrębie prowadzonych działań wojennych czy operacji służb specjalnych. Można tu wspomnieć np. o prowokacji FBI z lat 2018–2021 – pod kryptonimem Trojan Shield bądź Operation Ironside, w ramach której dystrybuowano w środowisku przestępczym smartfony, które miały być odporne na podsłuch, a w rzeczywistości służyły inwigilowaniu przestępców przez służby specjalne wielu państw. W wyniku tej operacji zatrzymano ponad 800 osób[16]. Utrudnianie dostępu do informacji mają na celu również takie sposoby działania jak zaciemnianie kodu (*obfuscation*) czy podejście „bezpieczeństwo przez niejawność" (*security by obscurity*). Tego rodzaju niepewność jest źródłem kolejnych rodzajów ryzyka związanego z bezpieczeństwem informacji.

Wymienione w tytule tego podrozdziału charakterystyczne cechy problematyki bezpieczeństwa informacji: wybitnie duża złożoność techniczna i organizacyjna, wysoka dynamika zdarzeń i zjawisk, działanie w warunkach niepewności skutkującej ryzykiem różnego rodzaju i wreszcie niedoskonałość funkcjonowania zabezpieczeń natury prawnej, implikują konieczność podjęcia kwestii bezpieczeństwa informacji na poziomie zarządczym, przez osoby i podmioty zajmujące się jej przetwarzaniem, przesyłaniem czy magazynowaniem, a nie przez ustawodawcę, administrację państwową czy wymiar sprawiedliwości, nawet bowiem jeśli incydent bezpieczeństwa będzie spowodowany przez przestępcę, to nie sposób mieć nadzieję, że zostanie on szybko i skutecznie ustalony, schwytany i osądzony ani tym bardziej że uda się wyegzekwować odeń środki na pokrycie poniesionych strat. Drugą konsekwencją takiego stanu rzeczy jest oczywiście racjonalność położenia większego nacisku na działania zapobiegające[17] wystąpieniom incydentów, co czasami w praktyce wiąże się z niedocenianiem czy lekceważeniem roli działań postincydentalnych, szczególnie gdy mowa

15 Zob. np. K. Kuziak, *Zarządzanie ryzykiem prawnym w przedsiębiorstwie*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2008, nr 1196, Finanse, Bankowość, Rachunkowość, z. 6, s. 91; A. Korczowski, *Zarządzanie ryzykiem w projektach informatycznych teoria i praktyka*, Helion, Gliwice 2010, s. 21; S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki –organizacji – państwa*, CeDeWu, Warszawa 2019.

16 Zob. np. FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown, https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive (dostęp: 5 stycznia 2025).

17 Ang. *preventive controls*.

nie o bieżącym odparciu ataku czy usunięciu bezpośrednich szkód, ale o działaniach w dłuższej i głębszej perspektywie. Tymczasem, choć nie można odmówić słuszności zasadzie *morbum evitare quam curare facilius est*, to praktyka pokazuje, że nie istnieją idealne metody zapobiegania incydentom, należy więc być przygotowanym na ich wystąpienie, co obejmuje również odpowiednie zastosowanie zabezpieczeń o charakterze naprawczymi[18]. Zresztą działania postincydentalne powinny również obejmować aktualizację poszczególnych polityk czy procedur, tak aby zapobiec powtórzeniu się podobnych incydentów w przyszłości (zgodnie z koncepcją *lessons learned*[19]). Gotowość śledcza, nawet tylko na poziomie właściwego zebrania i przechowania wiarygodnych śladów dowodowych, może w pewnej mierze zmniejszać ryzyko związane z niedoskonałościami działania organów ścigania oraz sądów.

2.2. GRC, IRM, IRMS. Platformy, metodyki, ramy postępowania, modele dojrzałości

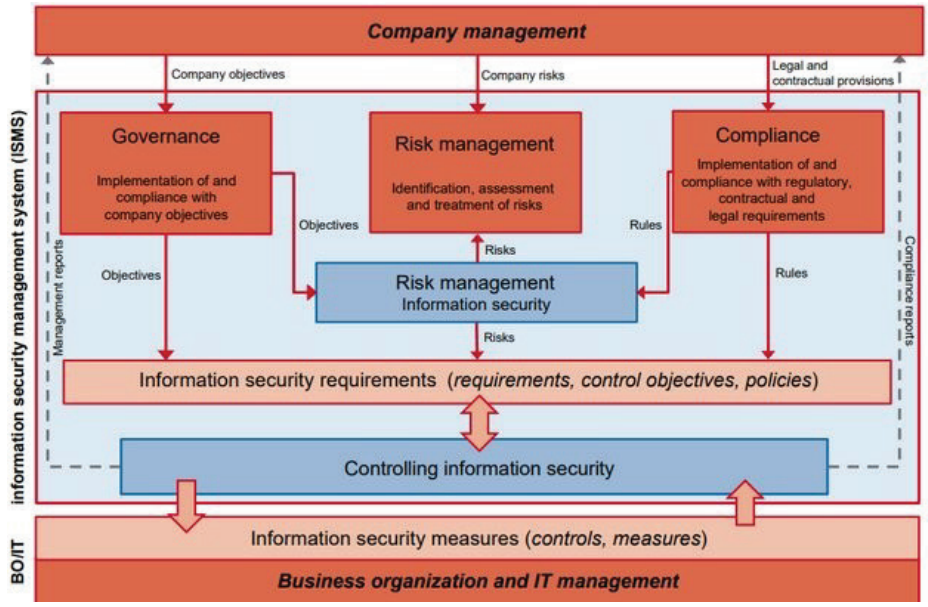
Zagadnienia zarządzania bezpieczeństwem informacji, z punktu widzenia zarządzania, są – jak już wspomniano – jednym z elementów obszaru GRC. W centrum GRC znajduje się zarządzanie ryzykiem (zob. rysunek 3), a w kontekście systemów zarządzania bezpieczeństwem informacji ryzykiem bezpieczeństwa informacji.

Warto poczynić zastrzeżenie, że mówiąc o zarządzaniu bezpieczeństwem informacji – trzeba rozróżnić sytuację organizacji gospodarczych, czy organizacji pozarządowych, a nawet części administracji państwowej niemającej bezpośredniego związku z obszarami krytycznymi dla istnienia i bezpieczeństwa państwa, od organów państwa odpowiedzialnych za jego bezpieczeństwo a także ludzkie życie i zdrowie. Z oczywistych przyczyn w przypadku takich organizacji (np. służb specjalnych czy wymiaru sprawiedliwości) większe znaczenie ma ścisłe zachowanie zgodności z wymaganiami i regulacjami, mniejsze natomiast – probabilistyczne metody

18 Ang. *corrective controls*.

19 Pojęcie *lessons learned* wzięte jest z zarządzania projektami i dotyczy procesu gromadzenia, uogólniania i formalizacji wiedzy zdobytej przez doświadczenie i ewaluacje projektów czy programów obejmującej takie elementy jak mocne i słabe strony przygotowań, projektowania i wdrażania, które wpływają na wydajność, wynik i wpływ. Por. np.: A. Grzenkowicz, *Lessons Learned odczarowane. Jak zebrać wiedzę po zakończonym projekcie i dobrze ją wykorzystać?*, „Strefa PMI" 2016, nr 12, marzec, s. 6, https://strefapmi.pl/pobierz/strefa-pmi-12-2016.pdf (dostęp: 5 stycznia 2025); K. Jugdev, *Learning from Lessons Learned: Project Management Research Program*, „American Journal of Economics and Business Administration" 2022, Vol. 4(1), s. 13, https://www.researchgate.net/profile/Kam-Jugdev/publication/258933493_Learning_from_Lessons_Learned_Project_Management_Research_Program/links/56322dd308ae0530378fbd7b/Learning-from-Lessons-Learned-Project-Management-Research-Program.pdf (dostęp: 5 stycznia 2025).

szacowania ryzyka. W zarządzaniu bezpieczeństwem *stricto sensu* wyróżnia się warunki deterministyczne (te, które są pewne) oraz indeterministyczne – odnośnie do których (momentu, a nawet faktu ich wystąpienia, natężenia itd.) występuje niepewność i ryzyko rozumiane jako jej skutek w odniesieniu do planowanych celów[20]. Takimi uwarunkowaniami deterministycznymi powinny być przepisy prawa: ich przestrzegane jest bezwzględnie konieczne (choć oczywiście praktyka pokazuje, że często przyczyną naruszeń bezpieczeństwa jest nie tyle źle przeprowadzone postępowanie z ryzykiem, co właśnie lekceważenie obligatoryjnych przepisów dotyczących bezpieczeństwa).



Rysunek 3. Miejsce SZBI w GRC

Źródła: O.G. Agboola, *Impact of cyber security implementation in an economy driven by Cyber Physical System (CPS)*, [w:] *Cyber Secure Nigeria 2019 Conference April 9–11, 2019, Governance, Risk Management, and Compliance*, s. 1, https://spara.ir/assets/en_css/files/GRC.pdf (dostęp: 5 stycznia 2025).

Pojęcie „System zarządzania bezpieczeństwem informacji" jest na powyższym rysunku rozumiane jak normach ISO/IEC z serii 27k.

Kolejnym – zyskującym ostatnio popularność – pojęciem mającym odwzorowywać podejście organizacji do zarządzania ryzykiem jest IRM (*Integrated Risk Management*) – pojęcie wprowadzone w 2018 roku przez firmę Gartner, zdaniem której GRC odnosi się do podejścia reaktywnego, stawiającego w centrum

20 Zob. np. M. Piśniak, *Ryzyko w teorii podejmowania decyzji*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 19, s. 116–126.

problematyki zagadnienia zgodności, w szczególności z wymaganiami prawnymi, zaś IRM ma być podejściem proaktywnym, stawiającym w centrum zarządzanie ryzykiem i obejmującym sześć elementów:

- strategię,
- szacowanie,
- odpowiadanie (postępowanie z ryzykiem),
- komunikowanie i raportowanie,
- monitorowanie oraz
- technikę (zaprojektowanie i wdrożenie rozwiązania wspomagającego IRM)[21].

Należy jednak zastrzec, że z każdym podejściem, metodyką czy ramami postępowania, w realiach rynkowych, związane są konkretne narzędzia (zwłaszcza oprogramowanie), czy usługi (np. consultingowe), stąd też należy zachować pewną ostrożność, szczególnie gdy mowa o promowaniu czy krytyce jakiegoś podejścia, metody czy narzędzia przez poszczególnych uczestników gry rynkowej[22]. Następnym krokiem rozwoju na wyższy poziom zarządzania według

---

21 Według słownika Gartnera (z 2024 roku): „Integrated risk management (IRM) is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

Under the Gartner definition, IRM has certain attributes:

1. Strategy: Enablement and implementation of a framework, including performance improvement through effective governance and risk ownership
2. Assessment: Identification, evaluation and prioritization of risks
3. Response: Identification and implementation of mechanisms to mitigate risk
4. Communication and reporting: Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response
5. Monitoring: Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives and the effectiveness of risk mitigation and controls
6. Technology: Design and implementation of an IRM solution (IRMS) architecture

To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. Developing this understanding requires risk and security leaders to address all six IRM attributes".

Obecnie (w roku 2025) Garner nie używa tego pojęcia (definicja na stronie została zastąpiona poniższą):

„Integrated Risk Management (IRM) is an organizationwide discipline informed by certain attributes, including strategy, assessment, response, communication and reporting, monitoring and technology. IRM is underpinned by a framework of practices, processes and enabling technologies that support a risk-aware culture, improved decision making and performance. This discipline delivers an integrated view of how well an organization manages its unique set of risks. *Gartner no longer recognizes IRM as a market and future work from Gartner analysts will no longer reference it as such*". Źródło: https://www.gartner.com/en/information-technology/glossary/integrated-risk-management-irm (dostęp: 5 stycznia 2025).

22 Zob. np.: M. Rasmussen, *The IRM Emperor Has No Clothes*, https://www.linkedin.com/pulse/irm-emperor-gartner-has-clothes-michael-rasmussen (dostęp: 5 stycznia 2025).

Gartnera ma być ERM – *Enterprise Risk Management* obejmujące strategiczne zarządzanie ryzykiem włącznie z zadaniami kadry kierownicze i organów nadzoru korporacyjnego[23].

Z praktycznego punktu widzenia uporządkowaniu i systematyzacji podejścia do zarządzania bezpieczeństwem informacji służą liczne standardy i metodyki opracowane przez różne organizacje i dotyczących różnych elementów zarządzania bezpieczeństwem informacji. Niewątpliwie najistotniejszymi z praktycznego punktu widzenia są: rodzina norm ISO/IEC 27k oraz inicjatywy NIST[24], w szczególności Cybersecurity Framework[25], NICE Cybersecurity Workforce Framework[26], Privacy Framework[27], Cyber-Physical Systems (CPS) Framework[28] i szereg innych. Wśród innych popularnych obecnie można wymienić dla przykładu IRAM2 (Information Risk Assessment Methodology 2) – metodykę zarządzania ryzykiem bezpieczeństwa informacji opracowaną przez ISF[29], COBIT (Control Objectives for Information and related Technology)[30] – zbiór dobrych praktyk i wskazówek

23 Według słownika Gartnera: „Enterprise risk management is identifying, analyzing and treating the exposures an organization faces as seen by the executive levels of management. This means looking at exposures in finance, credit, fraud, strategic and operational matters for the company. Most matters at the enterprise level only peripherally consider technological risk, and that's when they are looking at how technology increases or decreases those business exposures". Źródło: https://www.gartner.com/en/information-technology/glossary/enterprise-risk-management (dostęp: 5 stycznia 2025).

24 National Institute of Standard and Technology jest amerykańską agencją rządową, działającą w ramach U.S. Department of Commerce, zajmującą zajmującą się rozwijaniem i promowaniem standardów, technologii oraz badań naukowych w celu zwiększenia produktywności, ułatwienia handlu i poprawy jakości życia. Część rekomendacji NIST została przetłumaczona i dostosowana do polskich warunków jako Narodowe Standardy Cyberbezpieczeństwa. Zostały one udostępnione przez Depatrament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów pod adresem https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber (dostęp: 5 stycznia 2025).

25 Zob. National Institute of Standard and Technology Cybersecurity Framework, https://www.nist.gov/cyberframework (dostęp: 5 stycznia 2025).

26 Workforce Framework for Cybersecurity (zwany NICE Framework – National Initiative for Cybersecurity Education) opisany jest w dokumencie NIST SP 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf (dostęp: 5 stycznia 2025).

27 Zob. NIST Privacy Framework, A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0, January 16, 2020, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf (dostęp: 5 stycznia 2025); Witryna NIST poświęcona Privacy Framework: https://www.nist.gov/privacy-framework (dostęp: 5 stycznia 2025).

28 Zob. Cyber Physical Systems Public Working Group: Framework for Cyber-Physical Systems, Release 1.0, May 2016, https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf (dostęp: 5 stycznia 2025); Witryna NIST poświęcona Cyber-Physical Systems Framework: https://pages.nist.gov/cpspwg/ (dostęp: 5 stycznia 2025).

29 Zob. https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/ (dostęp: 5 stycznia 2025).

30 Zob. https://www.isaca.org/resources/cobit (dostęp: 5 stycznia 2025).

z zakresu zarządzania procesami IT, opracowanych przez ISACA[31], a utrzymywany przez będący jej częścią IT Governance Institute, obejmujący również zagadnienia bezpieczeństwa i zgodności, metodykę szacowania ryzyka CIS RAM (The Center for Internet Security Risk Assessment Method)[32] wraz z zestawem CIS CSC (Critical Security Controls), EBIOS RM (Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager)[33] opracowany przez francuską ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Interesujące zestawienie metodyk zarządzania ryzykiem można znaleźć na stronach ENISA Risk Management Inventory, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods. Sama ENISA dostarcza również rozmaite narzędzia, np. zestaw mapowań pojęć związanych z bezpieczeństwem informacji na pojęcia dotyczące go w kontekście interoperacyjności (ENISA Interoperable EU Risk Management Toolbox, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox).

Warto przy tym zauważyć, że wymieniane powyżej metodyki czy ramy postępowania są często bardzo obszerne (dokumentacja obejmująca dziesiątki i setki stron), a ich praktyczne stosowanie wymaga szeregu szkoleń i dużego doświadczenia.

Niezależnie od tego, jaką metodyką i którym podejściem do zagadnień związanych ze zgodnością, nadzorem i ryzykiem posługuje się organizacja, biorąc pod uwagę wspomnianą wcześniej złożoność i dynamikę zdarzeń związanych z bezpieczeństwem informacji, dla zarządzania nim konieczne jest wykorzystanie narzędzi informatycznych, w tym dedykowanego oprogramowania wspomagającego zarządzanie ryzykiem (we wspomnianej wyżej terminologii Gartnera – IRMS – IRM Solution). Rynek narzędzi wspierających GRC (lub IRM/ERM) obejmuje liczne narzędzia i platformy oferowane przez wiele znanych firm. Firma G2 zajmująca się zbieraniem i udostępnianiem opinii i informacji o oprogramowaniu na swojej stronie[34] zamieszcza informacje i oceny platform GRC (116 w sierpniu 2023 r., 84 w grudniu 2023 r., 92 we wrześniu 2024 r., 97 w grudniu 2024 r.). Są one pozycjonowane w „magicznym kwadracie" wzorowym na metodzie Gartnera na podstawie doświadczenia uczestników platformy. Przykładowe wyniki w kategorii wszystkich firm (niezależnie od wielkości) pokazuje rysunek 4.

Oczywiście, konkretne oprogramowanie musi zachowywać zgodność z którąś z metodyk bądź standardów (nierzadko zresztą związek ten jest dwustronny, w tym sensie, że nie tylko zmiany w metodyce wymuszają rozwój

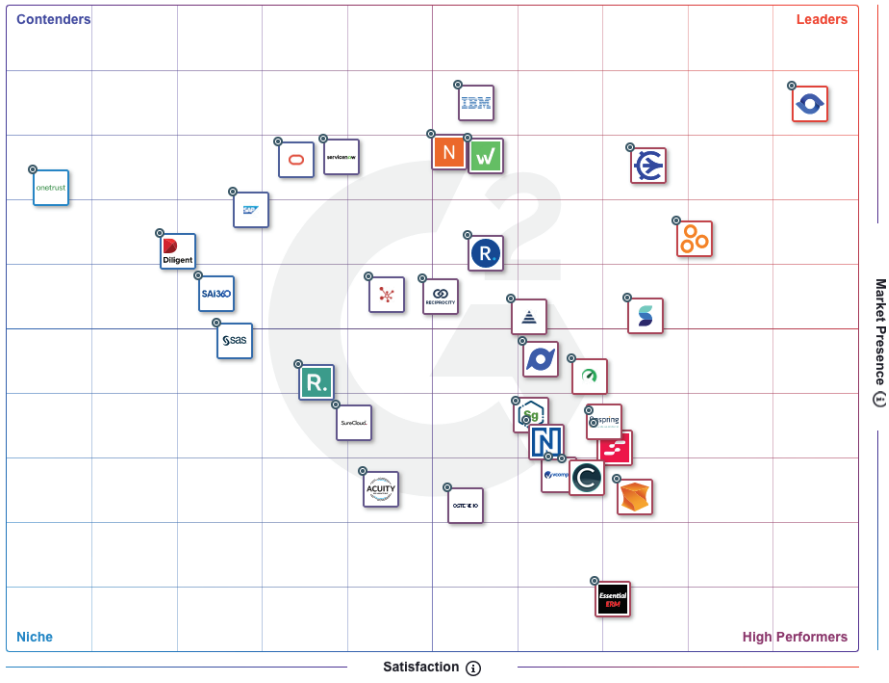
31 ISACA (dawniej nazwa była tłumaczona jako skrót od Information Systems Audit and Control Association, obecnie rozwinięcie to nie jest używane) – międzynarodowe stowarzyszenie osób zajmujących się audytem i systemów informatycznych, bezpieczeństwem informacji, prywatnością, ryzykiem i pokrewnymi zagadnieniami.

32 https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method (dostęp: 5 stycznia 2025).

33 EBIOS RM, https://cyber.gouv.fr/publications/ebios-risk-manager-method (dostęp: 5 stycznia 2025).

34 Zob. https://www.g2.com/categories/grc-platforms (dostęp: 5 stycznia 2025).

oprogramowania, ale i rozwój konkretnego oprogramowania prowadzi do zmian w kolejnych wersjach metodyki).



Rysunek 4. „Magiczny kwadrat" narzędzi GRC opracowany i uaktualniany na podstawie informacji zebranych od użytkowników platformy G2. Stan na sierpień 2023 roku
Źródło: https://www.g2.com/categories/grc-platforms#grid (dostęp: 5 stycznia 2025).

W popularnych opracowaniach rozszerza się często pojęcie ram postępowania (*frameworks*[35]), na wszystkie normy i metodyki, przyjęcie których określa – w obrębie danej organizacji – sposób zarządzania bezpieczeństwem informacji, począwszy od rozumienia przyjętej terminologii a skończywszy na uporządkowaniu poszczególnych procesów. Można spotkać się z różnymi zestawieniami i porównaniami tak rozumianych „ram postępowania", np. Birlasoft, https://www.birlasoft.com/articles/the-a-z-of-cybersecurity-compliance-frameworks wymienia dziesięć takich „ram":

- NIST Cybersecurity Framework: Ramy postępowania (ang. Cybersecurity Framework, zwane też CSF lub NCF), obecnie dostępne w wersji 2.0 obejmują szereg dokumentów opartych o zharmonizowane podejście dzielące funkcje związane cyberbezpieczeństwem na kilka grup; w wersji 1.1 było to pięć grup: identify, protect, detect, respond oraz recover, w wersji 2.0 wyodrębniono jako osobną funkcje govern,

35 Innym możliwym tłumaczeniem jest „platforma", choć takie tłumaczenie jest stosowane raczej w odniesieniu do konkretnych zestawów narzędzi.

- IASME Governance, obecnie IASME Cyber Assurance (ang. Information Assurance for Small and Medium Enterprises). Jest to standard opracowany i utrzymywany przez IASME Consortium Ltd przy współpracy z brytyjską Radą ds. Strategii Technologicznej Rządu (ang. *Government's Technology Strategy Board*) przedstawiany jako alternatywa dla ISO/IEC 27001 przeznaczona dla małych firm[36],
- COBIT (Control Objectives for Information and related Technology) jest to opracowany przez stowarzyszenie ISACA zestaw wskazówek i najlepszych praktyk dotyczących zarządzania i nadzoru nad techniką informatyczną,
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) opracował model zarządzania ryzykiem i kontrolą wewnętrzną w organizacjach (COSO framework). Istnieją dwie wersje tego modelu: COSO I oraz COSO II, wraz z podwersją z 2013 roku[37],
- TC Cyber – Mowa o komitecie technicznym (Technical Committee) Europejskiego Instytutu Norm Telekomunikacyjnych (European Telecommunications Standards Institute, ETSI), który opracował wiele standardów obejmujących różne dziedziny cyberbezpieczeństwa[38],
- CISQ – The Consortium for Information & Software Quality opracowało szereg standardów, m.in. dotyczący ochrony danych standard ASCDPM (Automated Source Code Data Protection Measure)[39],
- FredRAMP – Federal Risk and Authorization Management Program to program ustanowiony w 2011 roku w celu zapewnienia opłacalnego, opartego na ryzyku podejścia do korzystania z usług w chmurze przez rząd federalny USA. W grudniu 2022 roku podpisano FedRAMP Authorization Act jako część ustawy FY23 National Defense Authorization Act (NDAA). Kodyfikuje ona program FedRAMP jako autorytatywne, ujednolicone podejście do oceny bezpieczeństwa i autoryzacji produktów i usług przetwarzania w chmurze, które przetwarzają niejawne informacje federalne[40],
- FISMA (*Federal Information Security Management Act*) to federalne prawo Stanów Zjednoczonych uchwalone w 2002 roku jako Tytuł III ustawy E-Government Act z 2002 roku obejmujące zagadnienia dotyczące bezpieczeństwa informacji w kontekście interesów gospodarczych i bezpieczeństwa narodowego USA, znowelizowane przez – mający ten sam skrót Federal Information Security Management Act z 2014 roku[41],

36 Zob. https://iasme.co.uk/ (dostęp: 5 stycznia 2025).

37 Zob. np. https://coso.org; R. Skrzynecki, *Model Coso – czym jest i jakie korzyści przynosi organizacjom?*, https://eventis.pl/artykul/model-coso-czym-jest-i-jakie-korzysci-przynosi-organizacjom-id179 (dostęp: 5 stycznia 2025).

38 Zob. TC Cyber roadmap, https://www.etsi.org/cyber-security/tc-cyber-roadmapTC (dostęp: 5 stycznia 2025).

39 CISQ. Zob. https://www.omg.org/spec/ASCDPM, https://www.it-cisq.org/ (dostęp: 5 stycznia 2025).

40 Zob. https://www.fedramp.gov/program-basics/ (dostęp: 5 stycznia 2025).

41 Zob. https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act (dostęp: 5 stycznia 2025).

- SCAP – *Security Content Automation Protocol* został opracowany przez NIDET, a jego specyfikację zawiera dokument NIST SP 800-126 Rev. 3 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. Na najwyższym poziomie SCAP składa się z kilku komponentów, m.in.:
  - bazy mierników dla znanych konfiguracji oprogramowania powodujących problemy Common Configuration Enumeration (CCE) oraz Common Configuration Scoring System (CCSS),
  - ustrukturyzowanego schematu opisu dla systemów informatycznych, oprogramowania i pakietów Common Platform Enumeration (CPE),
  - systemu mierników dla podatności Common Vulnerability Scoring System (CVSS),
  - bazy podatności Common Vulnerabilities and Exposures (CVE). Najpopularniejszą bazą jest baza CVE (Common Vulnerabilities and Exposures) prowadzona przez organizację MITRE[42], w maju 2025 roku została uruchomiona alternatywna baza EUVD prowadzona przez ENISA[43].

Secureframe zestawia poszczególne ramy postępowania w tabeli (tabela 8), wymieniając, oprócz niektórych z powyższych dodatkowo:

- SOC 2 – Service and Organization Controls 2 to standard oceny procesów i procedur bezpieczeństwa przygotowany przez Amerykański Instytut Biegłych Rewidentów (obecnie od 2017 roku AICPA&CIMA)[44]. Definiuje on pięć kluczowych obszarów: *security* – bezpieczeństwo fizyczne i logiczne, *availability* – dostępność, *processing integrity* – integralność danych, *confidentiality* – poufność oraz *privacy* – prywatność, według których pogrupowane są poszczególne kryteria (*Trust Services Criteria*, TSC), obok SOC2 istnieją standardy SOC1 oraz SOC3,
- HIPAA,
- PCI DSS,
- GDPR[45],
- HITRUST CSF – *Common Security and Privacy Framework* – opracowane przez firmę Hitrust Alliance Inc. wspólne ramy bezpieczeństwa i prywatności mające zapewnić organizacjom pewność tworzenia, uzyskiwania dostępu, przechowywania i przesyłania informacji w bezpieczny sposób[46],
- NERC-CIP – zbiór standardów opracowanych przez North American Electric Reliability Corporation (NERC) dotyczących ochrony infrastruktury

42 Zob. np.: M. Szmit, A. Szmit, *Kilka uwag o zarządzaniu*…

43 Zob. https://euvd.enisa.europa.eu/ (dostęp: 5 stycznia 2025).

44 Zob. https://www.aicpa-cima.com/ (dostęp: 5 stycznia 2025).

45 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (General Data Protection Regulation), czyli Ogólne rozporządzenie o ochronie danych (RODO).

46 Zob. https://hitrustalliance.net/hitrust-framework (dostęp: 5 stycznia 2025).

krytycznej. CIP (*The Critical Infrastructure Protection*) to zbiór przepisów i wytycznych dotyczących cyberbezpieczeństwa systemów masowego zasilania elektrycznego (*Bulk Electric System*, BES) w Ameryce Północnej[47],

- IAB CCPA – opracowane przez Interactive Advertising Bureau (mająca siedzibę w Nowym Jorku organizacja zrzeszająca firmy medialne, reklamowe i technologiczne) ramy branżowe (*industry framework*) wspierające zapewnienie zgodności z ustawą o ochronie prywatności konsumentów w Kaliforni (CPPA – *The California Consumer Privacy Act*)[48].

Tabela 8. Porównanie wybranych ram postępowania według Secureframe

Framework	Purpose	Best Suited For	Certification	Certification Method	Audit Duration	Audit Frequency
SOC 2	Manage customer data	Companies and their third-party partners	N/A	Authorized CPA firms	6-month period	Every year
ISO 27001	Build and maintain an information security management system (ISMS)	Any company handling sensitive data	Yes	Accredited third-party	1 week–1 month	Every year
NIST Cybersecurity Framework	Comprehensive and personalized security weakness identification	Anyone	N/A	Self	N/A	N/A
HIPAA	Protect patient health information	The healthcare sector	Yes	The Department of Health and Human Services (third-party)	12 weeks	6 per year
PCI DSS	Keep card owner information safe	Any company handling credit card information	Yes	PCI Qualified Security Assessor (third-party)	18 weeks	Every year
GDPR	Protect the data of people in the EU	All businesses that collect the data of EU citizens	Yes	Third-party	About 30 days	Depends on preference

47 Zob. https://www.nerc.com (dostęp: 5 stycznia 2025).
48 Zob. https://www.iab.com/guidelines/ccpa-framework/ (dostęp: 5 stycznia 2025).

Framework	Purpose	Best Suited For	Certi-fication	Certification Method	Audit Duration	Audit Frequency
HITRUST CSF	Enhance security for healthcare organizations and technology vendors	The healthcare sector / Anyone	Yes	Third-party	3–4 months	Every year
COBIT	Alignment of IT with business goals, security, risk management, and information governance	Publicly traded companies	Yes	ISACA (third-party)	N/A	N/A
NERC-CIP	Keep North America's bulk electric systems operational	The utility and power sector	Yes	Third-party	Up to 3 years	Every 5 years
FISMA	Protect the federal government's assets	The federal government and third parties operating on its behalf	Yes	The FISMA Center	12 weeks	Every year
NIST Special Publication 800-53	Compliance with the Federal Information Processing Standards' (FIPS) 200 requirements and general security advice	Government agencies	N/A	Self	N/A	N/A
NIST Special Publication 800-171	Management of controlled unclassified information (CUI) to protect federal information systems	Contractors and subcon-tractors of federal agencies	N/A	Self	N/A	N/A

Tab. 8 (cd.)

Framework	Purpose	Best Suited For	Certi-fication	Certification Method	Audit Duration	Audit Frequency
IAB CCPA	Protecting California consumers' data	California businesses and advertising tech companies	N/A	Self	N/A	N/A
CIS Controls	General protection against cyber threats	Anyone	Yes	Third-party	N/A	N/A

Źródło: Secureframe: Essential Guide to Security Frameworks & 14 Examples, https://secureframe.com/blog/security-frameworks (dostęp: 5 stycznia 2025).

Complianceforge przy okazji omawiania własnych ram SCF (Secure Controls Framework) proponuje uporządkowanie ram postępowania według zakresu stosowalności (*scope applicability*) oraz stopnia szczegółowości (*depth of coverage*) jak na rysunku (zob. rysunek 5), przy czym oprócz niektórych wymienionych wcześniej umieszcza tamże:

- Essential 8 (*Essential Eigth*) – zestaw zabezpieczeń technicznych (takich jak wykonywanie kopii bezpieczeństwa czy stosowanie uwierzytelniania wieloskładnikowego) mających mitygować ryzyka związane z cyberbezpieczeństwem stworzony przez Australian Cyber Security Centre (ACSC) w celu ochrony australijskich firm przed dzisiejszymi cyberzagrożeniami[49],
- OWASP Top 10 – OWASP Open Worldwide Application Security Project jest fundacją stawiającą sobie za cel poprawę bezpieczeństwa oprogramowania, zaś Top 10 Web Application Security Risks (lista dziesięciu największych ryzyk dla aplikacji webowych) jest jej najbardziej znanym projektem[50],
- CSA CCM – Cloud Control Matrix jest ramami zabezpieczeń (*cybersecurity control framework*) dla architektur chmurowych opracowanymi przez organizację Cloud Security Alliance[51],
- BSI 200-1 (na oryginalnym rysunku pomyłkowo „BIS"). Mowa o standardzie BSI 200-1 Managementsysteme für Informationssicherheit (ISMS), wydanym przez niemiecki Federalny Urząd Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik). Jest to podstawowy dokument metodyki IT-Grundschutz, obejmującej wiele dokumentów zgodnych z podejściem danym normami ISO/IEC 27k i zawierających ich interpretację

49 Zob. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-explained (dostęp: 5 stycznia 2025).

50 Zob. https://owasp.org/ (dostęp: 5 stycznia 2025).

51 Zob. https://cloudsecurityalliance.org/research/cloud-controls-matrix (dostęp: 5 stycznia 2025).

i propozycje odnośnie do sposobu stosowania, jak również odnośnie do zarządzania ciągłością działania[52],

- IEC 62443 – seria norm, które dotyczą cyberbezpieczeństwa dla technologii operacyjnej w systemach automatyki przemysłowej. Ich twórcami są Międzynarodowe Towarzystwo Automatyzacji (International Society of Automation, ISA) oraz Międzynarodowa Komisja Elektrotechniczna IEC,
- UL 2900 – seria standardów opublikowanych przez UL Solutions (dawniej występującą pod nazwą Underwriters Laboratories), globalną firmę konsultingową zajmującą się cyberbezpieczeństwem, dotyczących bezpieczeństwa oprogramowania urządzeń sieciowych oraz systemów używanych w specyficznych zastosowaniach (w ochronie zdrowia, przemysłowych systemach sterowania itd.)[53],
- NISPOM – National Industrial Security Program Operating Manual jest podręcznikiem operacyjnym zbierającym zasady Narodowego Programu Bezpieczeństwa Przemysłowego przygotowanym i kodyfikowanym przez Departament Obrony (Department of Defence DoD) rządu USA opisującym wymogi dotyczące ochrony informacji niejawnych w zakresie bezpieczeństwa przemysłowego[54].

Niekiedy rozróżnia się trzy typy tak rozumianych ram na: control[55] frameworks (które mają dostarczać i porządkować tylko informacje o zabezpieczeniach), program frameworks (które mają działać na wyższym poziomie zarządzania, dostarczając środków oceny bieżącego sposobu zarządzania bezpieczeństwem i jego dojrzałości oraz jego poprawy i komunikacji z zarządem) oraz risk frameworks, które mają dostarczać już w pełni dojrzałych środków zarządzania ryzykiem bezpieczeństwa informacji[56].

Ujęcie takie, choć może być przydatne z praktycznego punktu widzenia, nie jest ścisłe: poszczególne akty prawne (np. wspomniane wyżej rozporządzenie RODO) dostarczają pewnych wymagań odnośnie do sposobu zarządzania niektórymi elementami bezpieczeństwa informacji, z natury rzeczy obejmując przede wszystkim ten fragment zagadnień, który jest istotny z punktu widzenia samej ustawy czy rozporządzenia (np. w wypadku RODO – ochronę danych osobowych), poszczególne metodyki czy protokoły mogą – w zależności od decyzji ich autorów – prezentować podejście bardziej całościowe (np. IRAM2, na którym można oprzeć w zasadzie całościowe zarządzanie ryzykiem związanym z bezpieczeństwem informacji w organizacji, czy COBIT,

52 Zob. https://www.IT-Grundschutz.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html (dostęp: 5 stycznia 2025).

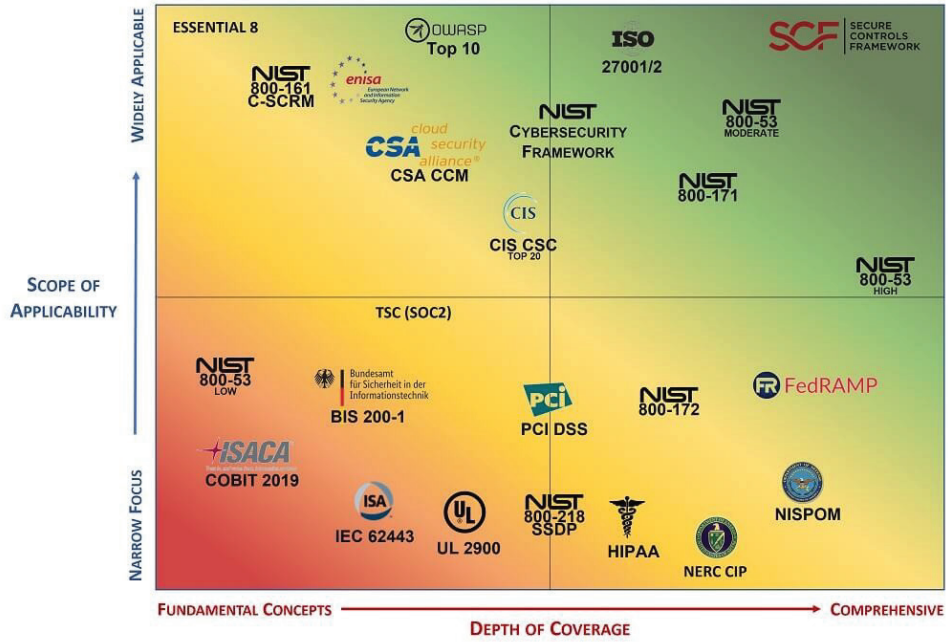
53 Zob. https://www.ul.com/ (dostęp: 5 stycznia 2025).

54 Zob. https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom (dostęp: 5 stycznia 2025).

55 Pojęcie „control" tłumaczone jest w zarządzaniu bezpieczeństwem informacji najczęściej jako „zabezpieczenie", ewentualnie „mechanizm zabezpieczający".

56 Zob. np. K. Dalao, *Understanding IT security frameworks: Types and examples*, https://www.onetrust.com/blog/security-framework-types/ (dostęp: 5 stycznia 2025).

który dostarcza ram postępowania dla całościowego zarządzania IT w organizacji), bądź też koncentrować się na jakimś konkretnym zagadnieniu. Normy ISO, a w szczególności rodzina norm ISO/IEC 27k, są natomiast międzynarodowymi standardami, które mogą zarówno stać się bezpośrednim wsparciem przy budowaniu i certyfikowaniu systemów zarządzania bezpieczeństwem informacji, jak i przede wszystkim odgrywają ogromną rolę jako zbiory dobrych praktyk i punkty odniesienia dla twórców poszczególnych metodyk, ram postępowania i narzędzi.



Rysunek 5. Ramy postępowania secure controls według complianceforge
Źródło: https://www.complianceforge.com/scf/secure-controls-framework-scf-download/ (dostęp: 5 stycznia 2025).

W uzupełnieniu do ram postępowania, metodyk i norm należy jeszcze wspomnieć o modelach dojrzałości (*maturity*), które również znalazły zastosowanie[57] do zagadnień związanych z bezpieczeństwem informacji. Wśród modeli tych można wymienić:

- CCMM – Cybersecurity Capability Maturity Model[58] dostępny obecnie w wersji 2.1,

57 Pierwotnie mówi się o dojrzałości organizacji bądź o dojrzałości procesowej. W normach ISO pojęcie dojrzałości odnośnie do systemu zarządzania jakością wprowadziła norma ISO 9004:2000, wykorzystując pięciopoziomowy model dojrzałości.

58 Zob. Office of Cybersecurity, Energy Security, and Emergency Response: Cybersecurity Capability Maturity Model (C2M2), version 2.1, June 2022, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf (dostęp: 5 stycznia 2025);

- Capability Maturity Model Integration CMMI[59] w wersji 2.0 oraz
- rozszerzający je COBIT[60] Performance Management (CPM), czy
- The Community Cyber Security Maturity Model (CCSMM) opracowany przez Center for Infrastructure Assurance and Security of Texas University at San Antonio.

Modele te mogą służyć do oceny poziomu dojrzałości procesów związanych z bezpieczeństwem informacji (benchmarkingowi), umieszczając go na jednym z kilku (zazwyczaj od czterech do sześciu) ustalonych poziomów[61], bądź też być traktowane jako sugestie odnośnie do kierunku rozwoju systemów zarządzania bezpieczeństwem informacji.

Rekapitulując: obecnie (rok 2024) na rynku funkcjonuje około setki różnych narzędzi komputerowych wspierających zarządzanie GRC, w literaturze i w praktyce znanych jest kilkadziesiąt metodyk, kilka różnych ram postępowania, a nawet kilka różnych modeli dojrzałości procesowej bezpieczeństwa informacji. Zagadnienia bezpieczeństwa informacji próbuje się dzielić na pewne obszary, takie jak np. prywatność, bezpieczeństwo infrastruktury krytycznej, cyberbezpieczeństwo, bezpieczeństwo rozwiązań CPS itp., w obrębie różnych standardów (głównie ISO oraz NIST) i aktów prawnych, przy czym również w tym zakresie czasami przyjmowane są rozwiązania arbitralne i nie do końca ze sobą zgodne. Sytuacja taka potwierdza wspomnianą wcześniej konieczność podjęcia kwestii bezpieczeństwa informacji na poziomie zarządczym, już na poziomie wyboru właściwej do zastosowania w obrębie danej organizacji (a także grup organizacji współpracujących ze sobą) metodyki, ram postępowania czy narzędzi wspierających zarządzanie jak i późniejszego odpowiedniego wsparcia ze strony kierownictwa organizacji w procesie ich wdrożenia, użytkowania i rozwoju.

Strona Office of Cybersecurity, Energy Security, and Emergency Response poświęcona Cybersecurity Capability Maturity Model (C2M2), https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (dostęp: 5 stycznia 2025).

59 CMMI jest obecnie rozwijany przez ISACA CMMI Institute, https://cmmiinstitute.com/ (dostęp: 5 stycznia 2025).

60 Zob. https://www.isaca.org/resources/cobit (dostęp: 5 stycznia 2025).

61 Obszerne porównanie modeli dojrzałości można znaleźć w artykule A. Kaczmarek, *Wybrane modele dojrzałości zarządzania bezpieczeństwem informacji – analiza porównawcza*, [w:] *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni*, Akademia Pomorska w Słupsku, Słupsk 2021, s. 73. Zob. też: P. Albright, *The Capability Maturity Model and ISO 9000 Standards: Similarities and Differences*, https://www.umsl.edu/~sauterv/analysis/488_f01_papers/albright.htm (dostęp: 5 stycznia 2025); A. Rot, *Zastosowanie modeli dojrzałości w zarządzaniu ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2011, nr 159, Informatyka Ekonomiczna, z. 19, https://dbc.wroc.pl/Content/119349/Rot_Zastosowanie_modeli_dojrza%C5%82osci.pdf (dostęp: 5 stycznia 2025).

3. Cyfrowa gotowość śledcza – przegląd wybranych źródeł

3.1. Działania postincydentalne i gotowość śledcza w normach ISO/IEC

Zagadnieniom związanym z obsługą incydentów bezpieczeństwa w rodzinie norm ISO/IEC 27k poświęcone zostały m.in. normy:

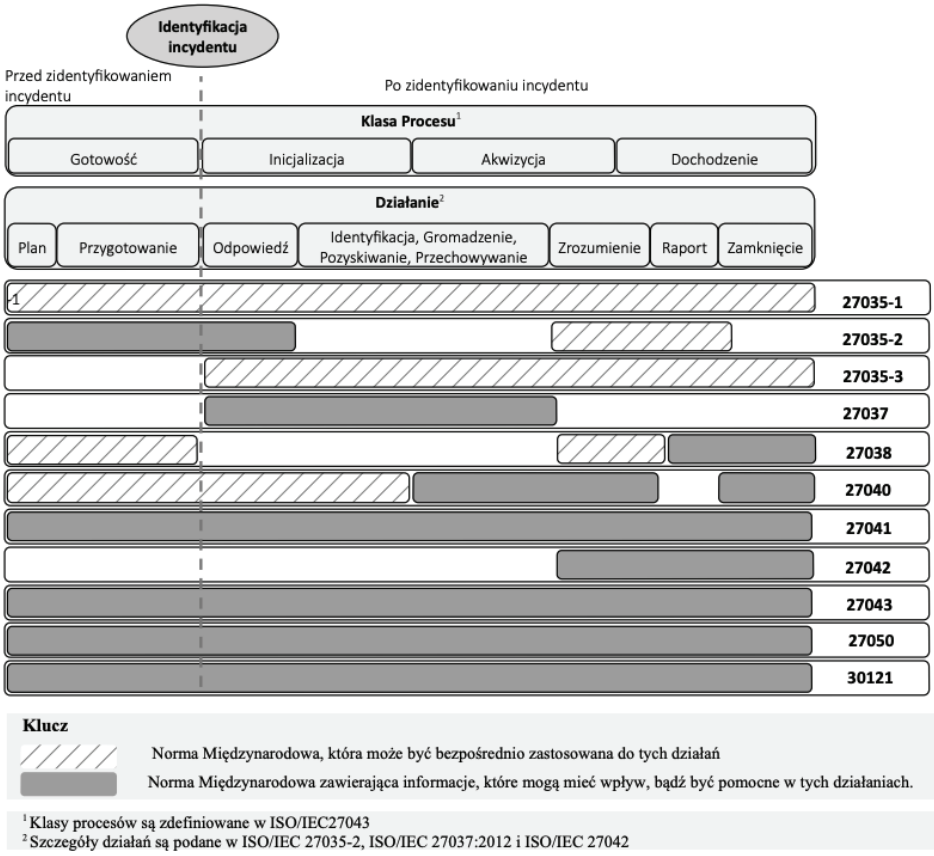
- ISO/IEC 27035-x (Zarządzanie incydentami),
- ISO/IEC 27037 (Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego),
- ISO/IEC 27040 (Bezpieczeństwo pamięci masowych),
- ISO/IEC 27041 (Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem),
- ISO/IEC 27042 (Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego),
- ISO/IEC 27043 (Pryncypia i procesy w dochodzeniach związanych z incydentami). Specyficzne znaczenie ma grupa norm
- ISO/IEC 27050-x (Elektroniczne ujawnienie) oraz
- związana z nimi norma ISO/IEC 27038 (Metody cyfrowe trwałego usuwania).

Użyte w normie ISO/IEC 27050-x pojęcie ujawnienia („discovery" lub – po zmianach w prawie Anglii i Walii z 1999 roku – „disclosure") odnosi się do procedury nakłonienia i przymuszenia stron sporu cywilnego do wyjawienia przeciwnikowi znanych stronie istotnych okoliczności faktycznych oraz środków dowodowych, która służy do ustalenia prawdy materialnej w procesie cywilnym[1]. W polskim procesie cywilnym nie istnieje instytucja ujawnienia (choć można doszukiwać się analogii w wyjawieniu majątku, wyjawieniu bądź wydaniu środka

1 Zob. K. Kubień, *Disclosure w prawie angielskim jako narzędzie wyrównania szans stron oraz ustalenia prawdy w postępowaniu cywilnym, cz. I*, „Polski Proces Cywilny" 2015, nr 4, s. 555–582.

dowodowego oraz wezwaniu do udzielenia informacji), stąd też trudno mówić o bezpośrednim zastosowaniu norm ISO/IEC 27050-x. Z drugiej strony pewne elementy tych norm mogą znaleźć zastosowanie przy ujawnianiu informacji pomiędzy zainteresowanymi stronami w postępowaniach pozasądowych czy też w postępowaniach toczonych przed sądami obcymi.

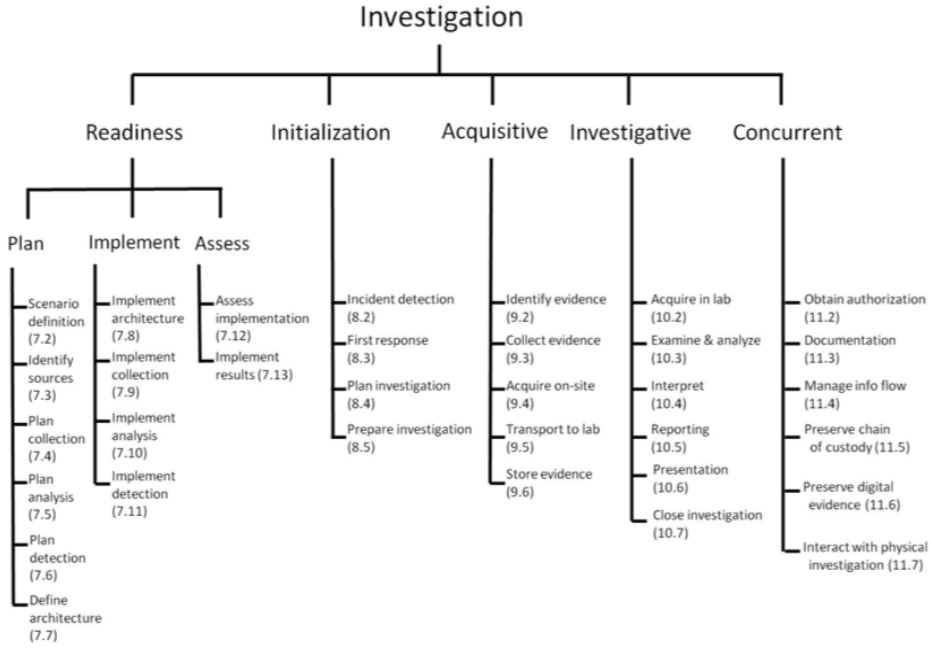
Pojęcie „trwałe usuwanie" (*digital redaction*) dotyczy trwałego (nieodwracalnego) usuwania informacji z dokumentów. Działanie takie może dotyczyć poszczególnych rodzajów danych wrażliwych (np. anonimizacja – modyfikacja bądź usunięcie danych osobowych w taki sposób, aby niemożliwa była identyfikacja ich posiadacza), co może mieć znaczenie zarówno w badaniach naukowych, jak i w procesie cyfrowego ujawnienia śladów w postępowaniu dowodowym.



Rysunek 6. Zastosowanie norm do badania klas procesów i działań
Źródło: P. Rybicki, *Normalizacja w obszarze zwalczania cyberprzestępczości*, „Cybersecurity & Cybercrime" 2023, Vol. 1, No. 2, s. 109–130, https://c2.amw.gdynia.pl/article/01.3001.0053.8024/pl (dostęp: 5 stycznia 2025).

Poza rodziną ISO/IEC 27k znajduje się – również poświęcona informatyce śledczej – norma ISO/IEC 30121 (początkowo PKN wprowadził błędne tłumaczenie normy „Nadzór nad strukturą ryzyka związanego z informatyką śledczą", obecnie – po zgłoszonej poprawce – już prawidłowe „Ramy nadzoru ryzyka związanego z informatyką śledczą").

Wzajemny stosunek tych norm oraz całościowa koncepcja ich znaczenia zostały przedstawione w normie ISO/IEC 27041, przy czym prace nad normą ISO/IEC 27044, która miała nosić tytuł Guidelines for Security Information and Event Management (SIEM), zostały zarzucone w sierpniu 2015, a projekt (na etapie Working Draft) wycofany. Szczegółowe omówienie zawartości poszczególnych standardów zostało opisane m.in. w artykule P. Rybickiego[2]. Tamże zamieszczono tłumaczenie poszczególnych terminów na język polski (zob. rysunek 6).



Rysunek 7. Procesy zdefiniowane w normie ISO/IEC 27043:2016 w podziale na klasy
Źródło: T. Grant, E. van Eijk, H.S. Venter, *Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time*, ICCWS 2016 Boston, MA.

Jakkolwiek klasy procesów podzielone są na te występujące przed wykryciem (zidentyfikowaniem) incydentu i po jego wykryciu, a schemat działań również sugeruje kolejność ich podejmowania, jest oczywiste, że niektóre z działań,

2 P. Rybicki, *Normalizacja w obszarze zwalczania cyberprzestępczości*, „Cybersecurity & Cybercrime" 2023, t. 1, nr 2, s. 109–130, https://c2.amw.gdynia.pl/article/01.3001.0053.8024/pl (dostęp: 5 stycznia 2025).

niezależnie od procesu, do którego zostały przypisane, powinny być prowadzone równolegle z innymi bądź obejmować całość procesu obsługi incydentu, tak aby np. niewłaściwa reakcja na incydent nie prowadziła do zanieczyszczenia czy nawet trwałego usunięcia śladów dowodowych. Według ISO/IEC 27043 **proces** to zbiór działań mających wspólny cel i ograniczony czas trwania (z uwagą, że podobne definicje zawierają normy ISO/IEC 27000 i ISO 9000)[3]. Norma ISO/IEC 27043 definiuje zharmonizowany model ramowy[4] śledztwa wykorzystującego cyfrowe ślady dowodowe (*Digital investigation proces schema*) dla wszystkich etapów dochodzeń, wyróżniający 33 procesy, przypisane do poszczególnych czterech klas przedstawionych na rysunkach powyżej oraz do piątej klasy procesów prowadzonych równocześnie (*concurrent*) z innymi. Przyporządkowanie procesów do poszczególnych klas pokazano na rysunku (rysunek 7).

Gotowość zdefiniowano w normie jako proces polegający na przygotowaniu na dochodzenie z wykorzystaniem śladów cyfrowych zanim będzie miał miejsce incydent[5]. Można tu zauważyć pewną niespójność nomenklaturową, z jednej bowiem strony gotowość jest klasą procesów, a z drugiej – procesem. Z natury rzeczy gotowość śledcza jest wpisana w zagadnienia związane z śledztwem wykorzystującym ślady cyfrowe. Schemat (model) takiego śledztwa pokazano na rysunku (rysunek 8).

Z punktu widzenia zagadnień rozważanych w niniejszej książce interesujące są użyte pojęcia:

- **łańcucha dowodowego** (*chain of custody*[6]) rozumianego jako dające się wykazać posiadanie, przemieszczanie, prowadzenie czynności z materiałem i jego lokalizacja od jednego momentu do innego oraz sposoby postępowania (*handling*) ze śladami dowodowymi[7];
- **gromadzenia** (*collection*) materiału dowodowego, czyli procesu zbierania przedmiotów zawierających potencjalny cyfrowy materiał dowodowy[8];
- **przejmowania** (*acquisition*) materiału dowodowego, zwanego czasami akwizycją, czyli procesu tworzenia kopii danych z określonego zbioru[9].

---

3 **Process** – set of activities that have a common goal and last for a limited period of time. Note 1 to entry: Also see ISO/IEC 27000 and ISO 9000 for similar definitions of a process. ISO/IEC 27043:2015-3.14.

4 W załączniku normatywnym A Comparison of existing models and the harmonized model zestawiono tenże model z 10 różnymi modelami porządkującymi etapy postępowania.

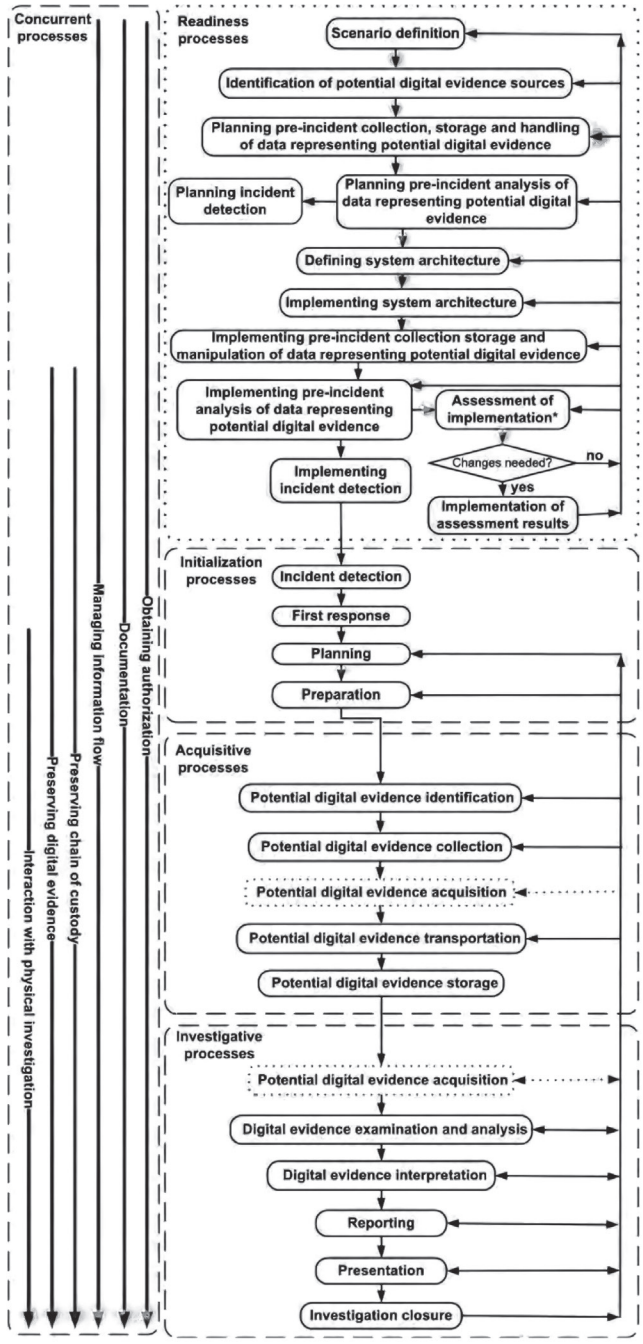
5 **Readiness** – process of being prepared for a digital investigation before an incident has occurred. ISO/IEC 27043-3.15.

6 **Chain of custody** – demonstrable possession, movement, handling, and location of material from one point in time until another, ISO/IEC 27050-1:2019-3.1.

7 W praktyce mowa o dokumentach, które poświadczają w sposób pewny, że materiał przedstawiony przed organem prowadzącym postępowanie (np. przed sądem) jest tym samym materiałem, który został znaleziony w miejscu wystąpienia incydentu (przestępstwa).

8 PN ISO/IEC 270737:2016-12-3.3.

9 **Acquisition** – process of creating a copy of data within a defined set NOTE The product of an acquisition is a digital evidence copy. ISO/IEC 27037:2016-12-3.1. W tłumaczeniu polskim przyjęto pojęcie „gromadzenia", natomiast w literaturze przedmiotu często mówi się o „akwizycji".



Rysunek 8. Zharmonizowany model dochodzenia wykorzystującego ślady cyfrowe w normie ISO/IEC 27043
Źródło: ISO/IEC 27043:2015(E).

W ramach prowadzonego śledztwa należy zagwarantować odpowiedni sposób postępowania z cyfrowymi śladami dowodowymi, tak aby nie dopuścić do ich degradacji (*spoliation*[10]), zwanej również kontaminacją[11], w tym celowej manipulacji (*tampering*)[12] czy utraty danych ulotnych (*volataile data*)[13] – co oczywiście wymaga odpowiedniego zaplanowania całości działań związanych ze zbieraniem (przejmowaniem, akwizycją) i przechowywaniem (*preservation*[14]), czyli procesem utrzymywania i ochrony integralności i/lub oryginalnego stanu potencjalnego cyfrowego materiału dowodowego, tak aby zapewnić ciągłość łańcucha dowodowego oraz możliwość przeprowadzenia w odpowiedni sposób badania i prezentacji wyników, w szczególności z zapewnieniem takich własności jak powtarzalność (*repeatability*), odtwarzalność (*reproducibility*) itd.

Oczywiście kwestie te powinny być rozważone, a odpowiednie mechanizmy przygotowane i przetestowane przed wystąpieniem incydentu, bowiem decyzje podejmowane *ad hoc* obarczone są znacznie większym ryzykiem popełniania błędów. Już sama początkowa decyzja o tym, jaki jest właściwy sposób postępowania z potencjalnym cyfrowym śladem dowodowym (czy będzie to gromadzenie materiału, kiedy należy potraktować jako dowód fizyczny nośnik danych, czy też akwizycja – przygotowanie cyfrowej kopii zapisanych danych), jest jedną z najważniejszych decyzji w procesie postępowania z cyfrowym materiałem dowodowym.

---

10 **Spoliation** – act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value, ISO/IEC 27037:2016-12-3.18.

11 Pojęcie kontaminacji (łac. *contaminatio* – zbrukanie, zanieczyszczenie) używane w literaturze fachowej wzięte jest z kryminalistyki, przy czym oczywiście w przypadku zapisu danych mowa jest nie o jego fizycznym zanieczyszczeniu, ale o dokonaniu w nim zmian. Samo pojęcie jest zdefiniowane w normie ISO 21043-1:20183.3 **contamination** – undesirable introduction of a substance to an item at any point in the forensic proces.
Note 1 to entry: This includes undesirable transfer of a substance within an item or between items (also referred to as cross-contamination), jakkolwiek normy 21043-x odnoszą się do kryminalistyki „klasycznej" a nie cyfrowej.

12 **Tampering** – act of deliberately making or allowing change(s) to a digital evidence (i.e. intended or purposeful spoliation) ISO/IEC 27037:2016-12-3.20.

13 **Volatile data** – data that is especially prone to change and can be easily modified.
NOTE A change can be switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses, ISO/IEC 27037:2016-12-3.25.

14 PN ISO/IEC 27037:2016-12-3.15. W tłumaczeniu tego terminu na polski (jak i całej Polskiej Normie PN ISO/IEC 27037:2016-12) nie użyto narzucającego się słowa „zabezpieczanie", ponieważ w profesjolekcie policyjnym ma on niezwykle szeroki zakres pojęciowy. Używa się go na oznaczenie szeregu najrozmaitszych czynności podejmowanych, czy to w miejscu wystąpienia zdarzenia w związku z zapewnieniem jego bezpieczeństwa (np. zabezpieczenie miejsca wypadku drogowego), czy to w związku z utrwaleniem informacji o samym zdarzeniu (np. zabezpieczenie śladów dowodowych, w sensie gromadzenia czy przejmowania dowodów, np. wykonanie pomiarów długości śladów hamowania pojazdu, wykonanie zdjęć w miejscu wypadku drogowego, fizyczne zabranie z miejsca zdarzenia narzędzia służącego do popełnienia przestępstwa), czy wreszcie w związku z zapewnieniem trwałości dowodów w czasie ich przechowywania w magazynie dowodów rzeczowych.

Warunkowana jest ona zarówno względami technicznymi (odłączenie niektórych nośników danych, np. pamięci RAM może powodować utratę danych ulotnych), organizacyjnymi (pozbawienie organizacji dostępu do zasobów może zagrozić ciągłości jej działania, szczególnie jeśli mówimy np. o dostawcy usług chmurowych), jak i prawnymi (polskie przepisy prawa nie przewidują instytucji kopii dowodu rzeczowego, a przy – z zasady słusznym – traktowaniu danych zapisanych na nośniku cyfrowym jako dokumentu wątpliwości może rodzić sposób uwierzytelnienia wykonanej kopii, stąd koncepcje np. notarialnego potwierdzania wyglądu strony www czy istnienia wpisu na forach internetowych w określonym czasie). Normy ISO/IEC 27k, jak w zasadzie wszystkie współczesne normy z zakresu zarządzania, wymagają ciągłego doskonalenia[15], zagadnienia DFR nie są w tym względzie wyjątkiem.

Normy ISO/IEC 27k mówią o gotowości technicznej (*technical readiness*[16]) rozumianej jako stan posiadania wiedzy, umiejętności, procesów i technologii potrzebnych do rozwiązania konkretnego problemu lub wyzwania, której to gotowości poświęcona jest norma ISO/IEC 27050-4. W normie tej zdefiniowano również pojęcie zobowiązań dotyczących zgodności z wymaganiami prawnymi i innymi, przez które rozumie się odpowiednio wymagania ustawowe bądź wynikające z przepisów wykonawczych, które organizacja musi spełnić oraz inne wymagania (takie jak standardy organizacyjne i branżowe, relacje umowne, kodeksy postępowania i umowy z grupami społecznymi lub organizacjami pozarządowymi), które organizacja musi lub postanawia spełnić[17]. W ósmym rozdziale tejże normy wymienia się jako elementy wymagające rozważenia: prywatność, ochronę danych, retencję danych, niszczenie informacji przechowywanej elektronicznie[18] oraz zagadnienia ciągłości działania (*business continuity*).

---

15 W niektórych normach (np. ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements) w tym kontekście przywołuje się model Demminga (cykl Plan-Do-Check-Act, PDCA), natomiast obecne wersje norm 27k nie odwołują się do niego.

16 **Technical readiness** – state of having the knowledge, skills, processes and technologies needed to address a particular issue or challenge, ISO/IEC 27050-4:2021-3.2.

17 **Compliance obligations legal requirements and other requirements** – legal requirements that an organization has to comply with and other requirements that an organization has to or chooses to comply with Note 1 to entry: Compliance obligations can arise from mandatory requirements, such as applicable laws and regulations, or voluntary commitments, such as organizational and industry standards, contractual relationships, codes of practice and agreements with community groups or non-governmental organizations. ISO/IEC 27050-4:2021-3.1.

18 To – wątpliwe z językowego punktu widzenia – pojęcie obejmuje wszelkie dane bądź informacje przechowywane na urządzeniach techniki komputerowej: **Electronically Stored Information ESI** – data or information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium.
Note 1 to entry: ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated metadata (3.19) such as timestamps, revision history, file type, etc.
Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements. ISO/IEC 27040:2015, 3.16.

Ramy nadzoru (przez odpowiedni organ nadzorczy, reprezentujący interesariuszy organizacji) nad zagadnieniami związanymi z informatyką śledczą zawiera norma ISO/IEC 30121. Wymienia ona sześć zasad, stanowiących ogólne wytyczne w kwestiach pewności i zgodności, którymi powinien kierować się organ nadzorczy:

- odpowiedzialność (*Responsibility*),
- strategię (*Strategy*),
- pozyskiwanie zasobów IT (*Acquisition*),
- wydajność (*Performance*),
- zgodność z wymaganiami prawa i regulacjami (*Conformance*) oraz
- poszanowanie zachowań ludzkich (*Human behaviour*).

Same ramy dotyczą pięciu działań (*actions*), które powinny być podjęte dla zapewniania odpowiedniego strategicznego kierunku dla organizacji. Są to:

- zapewnienie odpowiedniego mandatu ze strony interesariuszy (*Stakeholder mandate*),
- ustanowienie (*establishment*) zasad pracy organu nadzorczego, zgodnie z cyklem EDM (*Evaluate-Direct-Monitor*),
- ocenianie (*evaluate*) obecnych i przyszłych potrzeb odnośnie do zagadnień związanych z informatyką śledczą (strategii, planów, wsparcia itd.),
- sterowanie *(direct*) obejmujące przydział odpowiedzialności za przygotowanie i wdrożenie planów, strategii i polityk oraz nadzór nad zapewnianiem przez osoby zarządzające organizacją dostarczania we właściwym czasie informacji odnośnie do zgodności ze strategiami oraz kryteriami odnośnie do ryzyka,
- monitorowanie (*monitor*) – poprzez system odpowiednich mierników – wydajności i zgodność systemów informatycznych wykorzystywanych do postępowania ze śladami dowodowymi, z uwzględnieniem planów strategicznych i poziomu ryzyka spełniającego kryteria organizacji.

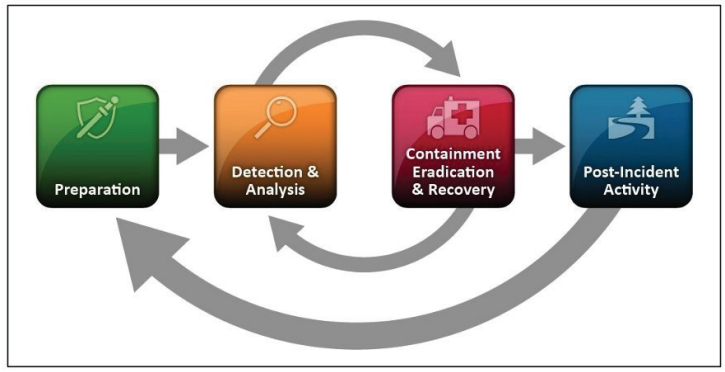
W normie wyróżniono pięć procesów strategicznych, za realizację których odpowiada zarząd organizacji (*management*), obejmujących strategie:

- retencji danych (*Archival strategy*),
- wykrywania (*Discovery strategy*),
- ujawniania (*Disclosure strategy*),
- zdolności do śledztwa wykorzystującego ślady cyfrowe (*Digital forensic capability strategy*),
- zgodności ryzyka (*Risk compliance strategy*).

Do oceny propozycji planów oraz monitorowania wydajności oraz do zarządzania strategiami i politykami norma zaleca użycie trzech rodzajów mierników: celów *(Key Goal Indicators*, KGI), wydajności (*Key Performance Indicators*, KPI) oraz biznesu (*Key Business Indicators*, KBI) – mierzących różnice (*variation*) pomiędzy KGI a KPI. Jak można zauważyć, norma operuje pojęciami i koncepcjami podobnymi do stosowanych w metodyce COBIT.

3.2. Cyfrowa gotowość śledcza w dokumentach NIST

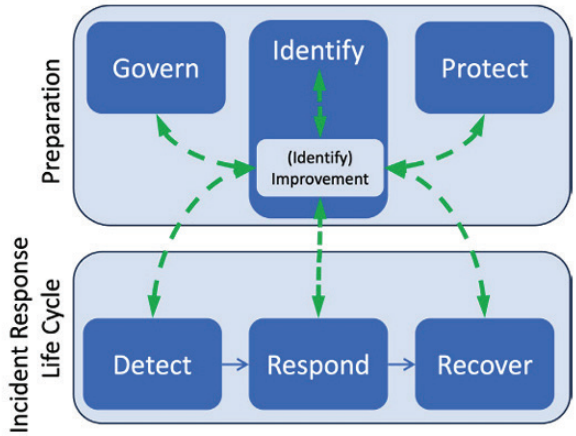
Spośród innych – poza normami – dokumentów dotyczących działań postincydentalnych należy zwrócić uwagę przede wszystkim na dokument NIST SP 800-61. W chwili pisania niniejszej książki obowiązywała wersja 2.0 zatytułowana *NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide*, natomiast trzecia wersja, zatytułowana *Incident Response Recommendations and Considerations for Cybersecurity Risk Management A CSF Community Profile*, znajdowała się na etapie Initial Public Draft. W wersji tej proponuje się wprowadzenie szeregu zmian (w stosunku do wersji 2.0) w samym podejściu do zarządzania incydentami, tak aby harmonizowały z pozostałymi elementami ram postępowania Cybersercurity Framework 2.0 (CSF 2.0). Zmiany te obejmują m.in. inny model cyklu odpowiedzi na zdarzenia. W miejsce istniejącego czteroetapowego cyklu (rysunek 9) proponowany jest model sześcioetapowy oparty na sześciu funkcjach CSF 2.0 (rysunek 10), sam bowiem CSF 2.0 operuje właśnie sześcioma funkcjami podstawowymi (funkcje te dzielone są później na kategorie), jak na rysunku 11.



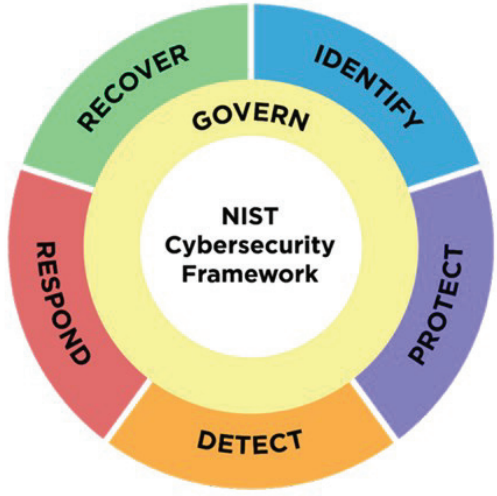
Rysunek 9. Model cyklu życia odpowiedzi na incydenty (Incident Response Life Cycle) według NIST.SP 800-61r2
Źródło: NIST.SP 800-61r2, s. 21.

Dokumenty NIST CSF 2.0 nie zajmują się gotowością śledczą jako osobnym pojęciem, istnieje jednak wiele dokumentów zajmujących się kwestiami informatyki śledczej, również w szerszym kontekście. Można tu wymienić np. dokument NISTIR 8428 Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT) definiujący ramowy schemat reakcji na incydenty obejmujący również działania śledcze czy NIST Cloud Computing Forensic Reference Architecture: SP 800-201, https://doi.org/10.6028/NIST.SP.800-201, który

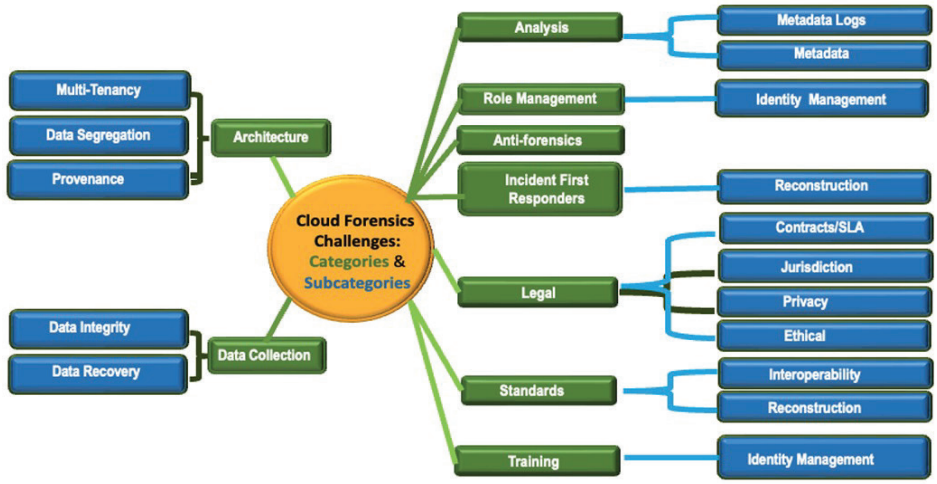
definiuje referencyjny model architektury chmurowej, mający na celu zapewnienie możliwości spełnienia wymagań (*challenges*) związanych z dochodzeniami wykorzystującymi ślady cyfrowe w środowisku chmury obliczeniowej. Zagadnienia te opisane są w dokumencie NISTIR 8006 NIST Cloud Computing Forensic Science Challenges i schematycznie przedstawione na rysunku 12.



Rysunek 10. Model cyklu życia odpowiedzi na incydenty (Incident Response Life Cycle) według NIST.SP 800-61r3
Źródło: NIST.SP 800-61r3(IPD), s. 5.



Rysunek 11. Funkcje CSF
Źródło: The NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.CSWP.29 February 26, 2024, s. 5.



Rysunek 12. NIST Cloud Forensic Challenges
Źródło: NIST SP 800-201, s. 29.

Przedstawiony na rysunku 12 schemat przedstawia wyłącznie problemy dotyczące samego śledztwa wykorzystującego ślady cyfrowe (i to wyłącznie w odniesieniu do chmur obliczeniowych), a więc nie zajmuje się problemami ściśle zarządczymi, jak choćby zapewnieniem odpowiednich zasobów do przeprowadzenia dochodzenia, przygotowaniem odpowiednich polityk i procedur itd. Pozwala jednak na uzmysłowienie wieloaspektowości problematyki. Obejmuje ona szerokie spektrum zagadnień: począwszy od analizy metadanych (a więc informacji o czasie utworzenia i modyfikacji poszczególnych plików czy dokumentów, o ich autorstwie, o miejscu z których był do nich uzyskiwany dostęp itd.), w tym kwestie zapewniania wiarygodności tych metadanych, poprzez zabezpieczenie przed działaniami *anti-forensic*[19], aspekty prawne i etyczne, aż po różne aspekty techniczne związane z architekturą czy gromadzeniem śladów dowodowych.

3.3. Cyfrowa gotowość śledcza w literaturze naukowej

Zagadnienie gotowości śledczej z punktu widzenia zarzadzania jest obecne w anglojęzycznej literaturze przedmiotu od wielu lat, przy czym sporo (w stosunku do liczby artykułów naukowych) jest na ten temat publikacji książkowych i stron

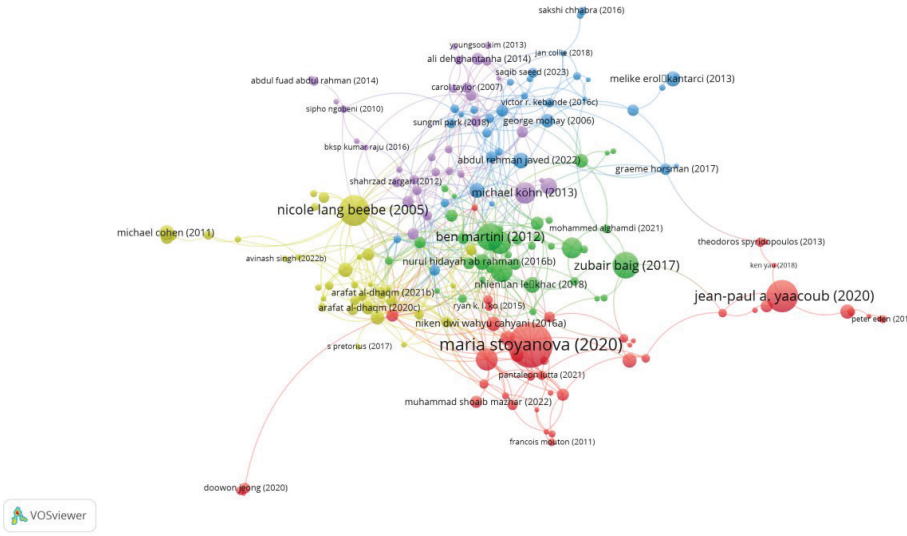
19 Narzędzia *anti-forensic* mają za zadanie utrudnić bądź zaburzyć proces akwizycji i analizy danych przez informatyków śledczych (np. poprzez trwałe usuwanie zapisów, ich szyfrowanie, ukrywanie zawartości, fałszowanie zapisów czy destrukcyjne akcje podejmowane w przypadku wykrycia działań informatyków śledczych).

internetowych. Jest to zresztą charakterystyczne dla zagadnień, które z jednej strony mają charakter mocno praktyczny, a z drugiej są stosunkowo nowe. W tabeli 9 zebrano wyniki kwerendy poszczególnych haseł w popularnych bazach bibliograficznych.

Tabela 9. Wyniki kwerendy w bazach SCOPUS, Web of Science oraz Google Scholar (stan na 20 grudnia 2024).

	Forensic readiness	**Forensic readiness management**	**Forensic readiness**	**Forensic readines management**
Web of Science[a]	184	14	278	52
Scopus[b]	302	69	461	102
Google Scholar	2570	2620	141 000	58 400
Google (wyszukiwarka stron)	34 300	27 000	6 010 000	269 000 000
Open Alex	243	2	559	10
Lens.org[c]	429	82	1141	459
ECU Libraries[d]	430	137	905	246

[a] Wyszukiwanie w polach Abstract or Author Keyword or Keyword Plus®.
[b] Wyszukiwanie w polu Article title, Abstract, Keywords.
[c] Wyszukiwanie w polu Title, Abstract or Full Text.
[d] Wyszukiwanie według hasła OneSearch.
Źródło: opracowanie własne.



Rysunek 13. Wizualizacja klasteryzacji bibliografii dotyczącej pojęcia *forensic readiness* (opis w tekście) w programie VOSviewer
Źródło: opracowanie własne.

Na rysunku 13 pokazano wizualizację klasteryzacji bibliografii w programie VOSviewer na podstawie liczby cytowań we wszystkich dokumentach, w których w tekście wystąpiło sformułowanie *forensic readiness* (bez cudzysłowów) z bazy Open Alex (559 wyników) dla dokumentów cytowanych przynajmniej 10 razy (227 dokumentów).

Publikacje naukowe dotyczące DFR (obok wielu artykułów dotyczących raczej specyficznych zagadnień z zakresu informatyki śledczej[20] czy analizy kryminalnej[21]) w znacznej mierze poświęcone są kwestiom technicznym związanym z projektowaniem bądź modyfikacjami sprzętu i oprogramowania narzędziowego i systemowego, takiego jak np.:

- identyfikatory radiowe RFID[22],
- sieci samochodowe (Car Area Network, CAN)[23],
- systemy nadzoru nad procesami technologicznymi (*Supervisory Control And Data Acquisition*, SCADA)[24],
- inteligentne budynki i inteligentne sieci energetyczne[25],
- bezzałogowe statki powietrzne (*Unmanned Aerial Vehicle*, UAV)[26] i inne systemy cyberfizyczne[27].

---

20 Choć i w części z nich przewidziano odpowiednie miejsce dla DFR zob. np. N. Lang Beebe, J. Guynes Clark, *A hierarchical, objectives-based framework for the digital investigations process*, „Digital Investigation" 2005, Vol. 2, Issue 2, s. 147–167, https://doi.org/10.1016/j.diin.2005.04.002, https://www.sciencedirect.com/science/article/pii/S1742287605000307 (dostęp: 5 stycznia 2025).

21 Np. Kim Jaechun, Son Youngjun, Chung Mokdong, *A design of evaluation framework for the assets and insolvency prediction depending on the industry type using data standardization based on the forensic readiness*, https://gvpress.com/journals/IJMUE/vol10_no4/33.pdf; D. Quick, R. Choo Kim-Kwang, *Big forensic data management in heterogeneous distributed systems: quick analysis of multimedia forensic data*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84995755337&doi=10.1002%2fspe.2429&origin=inward&txGid=14179b5dd7bdde49660847ff680618dc

22 Zob. B. Cusack, A.K. Ayaw, *Evidential recovery in a RFID business system*, [w:] *Proceedings of the 8th Australian Digital Forensics Conference 2010*, s. 46–56; M. Grobler, *Digital forensic standards: International progress*, [w:] *Proceedings of the South African Information Security Multi-Conference*, SAISMC 2010, s. 261–271.

23 A. Koch, R. Altschaffel, S. Kiltz, M. Hildebrandt, J. Dittmann, *Exploring the processing of personal data in modern vehicles – A proposal of a testbed for explorative research to achieve transparency for privacy and security*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85057357117&doi=10.1109%2fIMF.2018.00009&origin=inward&txGid=f0aaf355f13b6d977f6892f406d22ba3

24 Zob. J. Li, E. Bajramovic, Y. Gao, M. Parekh, *Graded security forensics readiness of SCADA systems*, https://www.scopus.com/record/display.uri?eid=2=-2s0.85031295459-&origin=inward&txGid-302b284ca073668b6bd3e77f2db6825f

25 E. Bajramovic, K. Waedt, A. Ciriello, D. Gupta, *Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests*, https://www.scopus.com/record/display.uri?eid=2=-2s0.84994106565-&doi10=1109.2%fIS2C2016.07580754.&origin=inward&txGid-7495c1532fe7b68fd65c114fc7610bae (dostęp: 5 stycznia 2025).

26 Y. Yu, D. Barthaud, B. Price, A. Bandara, A. Zisman, B. Nuseibeh, *LiveBox: A self-adaptive forensic-ready service for drones*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85077749703&doi=-10.1109%2fACCESS.2019.2942033&origin=inward&txGid=8bcdb5e12efde1d6c9c17ec82621b359

27 Zob. np. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, *A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues*, „IEEE Communications Surveys & Tutorials" 2020, Vol. 22, No. 2, s. 1191–1221, https://doi.org/10.1109/

Specyficzne wymagania odnośnie do informatyki śledczej mają rozwiązania oparte na chmurach obliczeniowych, w których przetwarzanie i przechowywanie danych zachodzi w miejscach fizycznie odległych od miejsc ich powstawania, stąd też wiele artykułów poświęconych zagadnieniom dotyczącym DFR tych architektur[28]. Często postulowane jest, aby już na etapie projektowania[29] zapewnić wiarygodność zbieranych przez nie informacji (dzienników systemowych, plików historii) na potrzeby ewentualnych dochodzeń elektronicznych[30]. Pliki historii i logi systemowe są zazwyczaj tworzone nie dla potrzeb informatyków śledczych, ale inżynierów zajmujących się

COMST.2019.2962586; J.-P.A. Yaacoub, O. Salman, H.N. Noura, N. Kaaniche, A. Chehab, M. Malli, *Cyber-physical systems security: Limitations, issues and future trends*, „Microprocessors and Microsystems" 2020, Vol. 77, 103201, https://doi.org/10.1016/j.micpro.2020.103201

28 Zob. np. C. Vidal, K.-K.R. Choo, *Cloud security and forensic readiness: The current state of an IaaS provider*, „The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues" 2015, s. 401–428, https://doi.org/10.1016/B978-0-12-801595-7.00018-5; R. Ab, H. Nurul, W.B. Glisson, Y. Yang, R. Choo Kim-Kwang, *Forensic-by-design framework for cyber-physical cloud systems*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84963728330&doi=10.1109%2fMCC.2016.5&origin=inward&txGid=fb14ac75c450336537505f88c9f2adfa; V. Kebande, H. Venter, *Towards a model for characterizing potential digital evidence in the cloud environment during digital forensic readiness process*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84994187863&origin=inward&txGid=14a04e6a5e372f9de836b71cd5785388 (dostęp: 5 stycznia 2025).; Y. Yu, D. Barthaud, B. Price, A. Bandara, A. Zisman, B. Nuseibeh, *LiveBox*…

29 Jest to jeden z elementów podejścia zwanego *security by design*.

30 Tematyce tej poświęcone są np. artykuły: F. Rivera-Ortiz, L. Pasquale, *Towards automated logging for forensic-ready software systems*, [w:] *Proceedings – 2019 IEEE 27th International Requirements Engineering Conference Workshops*, REW 2019, art. no. 8933538, s. 157–163, https://doi.org/10.1109/REW.2019.00033 oraz wiele artykułów współautorstwa L. Daubnera: L. Daubner, R. Matulevičius, B. Buhnova, T. Pitner, *Business process model and notation for forensic-ready software systems*, [w:] *International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE – Proceedings* 2022, s. 95–106, https://doi.org/10.5220/0011041000003176; L. Daubner, R. Matulevičius, B. Buhnova, T. Pitner, *BPMN-4FRSS: An BPMN extension to support risk-based development of forensic-ready software systems*, [w:] *Communications in Computer and Information Science* 2023, 1829 CCIS, s. 20–43, https://doi.org/10.1007/978-3-031-36597-3_2, których autorzy posługują się pojęciem *Forensic-ready software systems* i proponują rozszerzenie notacji BPMN (*Business Process Model and Notation*) o elementy dotyczące gotowości śledczej (BPMN for Forensic-Ready Software Systems, BPMN4FRSS), artykuł L. Daubner, R. Matulevičius, B. Buhnova, *A model of qualitative factors in forensic-ready software systems*, [w:] *Lecture Notes in Business Information Processing* 2023, 476 LNBIP, s. 308–324, https://doi.org/10.1007/978-3-031-33080-3_19, w którym zaproponowano jakościowy model referencyjny określający gotowość śledczą oprogramowania, który to model umożliwia sformułowanie konkretnych wymagań dla systemów informatycznych oraz artykuł L. Daubner, R. Matulevičius, *Risk-oriented design approach for forensic-ready software systems*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85113244166&doi=10.1145%2f3465481.3470052&origin=inward&txGid=e3121b36fb495736093c417f735eea7e który prezentuje zorientowane na ryzyko podejście do DFR obejmujące proces wspierający identyfikację potencjalnych źródeł dowodów oraz propozycję rozszerzenia notacji BPMN w celu rejestracji potencjalnych źródeł dowodów i ich relacji na podstawie przykładowego scenariusza implementacji takiego podejścia dla systemu automatycznego parkowania Automated Valet Parking (AVP).

procesami diagnostyki i usuwania problemów na etapie eksploatacji poszczególnych systemów, stąd też konieczność odpowiedniego zapewnienia zarówno integralności, dostępności, poufności i innych własności bezpieczeństwa[31] tych plików i zapisów, jak i użyteczności z punktu widzenia śledztwa (kryminalistyka posługuje się pojęciem tzw. siedmiu złotych pytań: co, gdzie, kiedy, w jaki sposób, czym, dlaczego, kto; w logach systemowych często można znaleźć tylko informację o tym, co się stało i ewentualnie, kiedy, przy czym już zapewnienie wiarygodności tej ostatniej informacji wymaga użycia niejednokrotnie zaawansowanych mechanizmów, np. znaczników czasu opartych na rozwiązaniach kryptograficznych), przy czym stosunkowo często przy tej okazji pojawia się bardziej usystematyzowane podejście, łączące proponowane rozwiązania z jakąś szerszą metodyką czy standardami[32].

Druga grupa artykułów dotyczy koncepcji modyfikacji lub rozszerzeń poszczególnych klas systemów zarówno związanych z bezpieczeństwem (jak systemy zarządzania tożsamością cyfrową – Digital Identity Management Systems, DIMS[33], systemy wykrywania włamań – Intruder Detection Systems, IDS[34] czy systemy zarządzania incydentami[35]), jak i poszczególnych systemów wspierających różne

31 Ciekawe podejście zaproponowano w artykule F. Rivera-Ortiz, *Engineering forensic-ready software systems using automated logging*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85128726859&origin=inward&txGid=8ce4c295955d47a2d946cdd474c86d48 (dostęp: 5 stycznia 2025), w którym omówiono koncepcję narzędzia programistycznego zwanego Forensic-Ready Logger, które w sposób półautomatyczny na podstawie scenariuszy możliwych incydentów dodawałoby do kodu programu polecenia odpowiedzialne za rejestrację śladów dowodowych.

32 Np. w artykule L. Daubner, R. Matulevičius, B. Buhnova, M. Antol, M. Růžička, T. Pitner, *A case study on the impact of forensic-ready information systems on the security posture*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85163948746&doi=10.1007%2f978-3-031-34560-9_31&origin=inward&txGid=73ed3d5a486411ee54aff1542c5cd324 przedstawiającym studium przypadku opisujące możliwości SensitiveCloud – czeskich usług chmurowych oferowanych przez centrum badawcze instytutu informatyki uniwersytetu Masaryka w Brnie, wykorzystujących podejście Forensic-Ready Information Systems Security Risk Management, DFR jest rozpatrywane w kontekście wymagań normy ISO/IEC 27001:2013 (rozdział A.12.4 – logging and monitoring oraz reagowania na incydenty oraz rozdział A.16.1 – Management of information security incident and improvement, w szczególności A 16.1.7 – Collection of evidence).

33 Zob. M. Tajbakhsh, E. Homayounvala, S. Shokouhyar, *Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage*, „International Journal of Electronic Security and Digital Forensics" 2017, Vol. 9(1), s. 62–83, https://doi.org/10.1504/IJESDF.2017.081781

34 Zob. A. Akremi, H. Sallay, M. Rouached, *An efficient intrusion alerts miner for forensics readiness in high speed networks*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84928032060&doi=10.4018%2fijisp.2014010104&origin=inward&txGid=16d5f875868bc9aef5aa3347187f2824 (w artykule zaproponowano szybki klasyfikator alertów wykorzystujący technikę wykrywania wartości odstających opartą na adaptacyjnych regułach skojarzeń).

35 Zob. S. Kurowski, S. Frings, *Computational documentation of IT incidents as support for forensic operations*, https://www.scopus.com/record/display.uri?eid=2-s2.0-79960740161&doi=10.1109%2fIMF.2011.18&origin=inward&txGid=336f4aed08d150c60fbe3a59613f354d

elementy działania organizacji (np. zarządzanie łańcuchem dostaw[36]), tak aby zarządzanie informacją konieczną do prowadzenia śledztwa stało się jedną z funkcji tych systemów. Również przy tej ostatniej okazji pojawia się zagadnienie systematyzacji podejścia oraz – przynajmniej częściowego – wykorzystania tak zebranych danych do wsparcia niektórych procesów zarządczych (choćby zarządzania ryzykiem).

Trzecia wreszcie grupa artykułów dotyczy DFR rozumianego bardziej całościowo, jako pewna własność nie poszczególnych programów czy systemów informatycznych, ale całego sytemu zarządzania bezpieczeństwem informacji, całości organizacji, a nawet kwestii bezpieczeństwa infrastruktury krytycznej państwa. Dla przykładu:

- W artykule L. Daubner, M. Macak, R. Matulevičius, B. Buhnova, S. Maksović, T. Pitner[37] autorzy sugerują włączenie FR w proces zarządzania ryzykiem związanym z bezpieczeństwem informacji (użyte jest pojęcie *Forensic-Ready Information Systems Security Risk Management* FR-ISSRM), proponując przykładowe mierniki i scenariusze działania w wypadku ataków.
- W artykule K. Reddy, H.S. Venter[38] zaproponowano wprowadzenie pojęcia *Digital Forensic Management Systems*, DFRMS, który to system miałby w sobie łączyć zarówno odpowiednie oprogramowanie (np. system IDS), jak i odpowiednie polityki organizacyjne. Autorzy na podstawie analizy literatury przedmiotu zaproponowali 16 wymaganych składowych DFRMS:
  1. Monitorowanie lub rejestracja aktywności sieci i hostów;
  2. Bezpieczne przechowywanie logów;
  3. System wykrywania włamań;
  4. Rozróżnianie, czy monitorowane są elementy sprzętowe czy programowe;
  5. Automatyczny alarm po wykryciu potencjalnego lub rzeczywistego incydentu;
  6. Procedury konfiguracji monitorowania i rejestrowania;
  7. Opisy zespołów śledczych (zespoły DF) i zespołów reagowania na incydenty;
  8. Wymagania szkoleniowe i szkolenia;
  9. Opisy procesów biznesowych;
  10. Polityki organizacyjne DF i polityki związane z DFR;
  11. Polityki dotyczące podejrzeń;

36 Zob. np. D. Masvosvere, H. Venter, *A conceptual model for digital forensic readiness in e-supply chains*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84940780779&origin=inward&txGid=a9ed347e74c6456e0f146ebfbe410328 (dostęp: 5 stycznia 2025),. Autorzy proponują integrację w łańcuchu dostaw elektronicznych niektórych procesów bezpieczeństwa, obejmujących monitorowanie łańcucha dostaw pod kątem incydentów i zbieranie danych mogących posłużyć za dowody elektroniczne możliwe do wykorzystania zarówno w sądzie, jak i do oceny ryzyka.

37 L. Daubner, M. Macak, R. Matulevičius, B. Buhnova, S. Maksović, T. Pitner, *Addressing insider attacks via forensic-ready risk management*, https://www.sciencedirect.com/science/article/pii/S2214212623000182?pes=vor&utm_source=scopus&getft_integrator=scopus (dostęp: 5 stycznia 2025),

38 K. Reddy, H.S. Venter, *The architecture of a digital forensic readiness management system*, https://www.scopus.com/inward/record.uri?eid=2-s2.0-84876568707&doi=10.1016%2fj.cose.2012.09.008&partnerID=40&md5=d8f1fb3db7e6646b65deeff11321e0c8

12. Polityki dotyczące kontaktów z organami wymiaru sprawiedliwości;
13. Procedura eskalacji;
14. Procedura reagowania na incydenty;
15. Procedura kontaktowania się z organami wymiaru sprawiedliwości;
16. Struktura organizacyjna i personel zaangażowany w DFR i reagowanie na incydenty

oraz propozycję architektury części takiego systemu.

- W artykule A. Almarzooqi, A. Jones[39] przedstawiono propozycję dość ogólnych ram postępowania nazwanych *Digital Forensic Organization Core Capability (DFOCC) Framework* mających wspierać budowanie gotowości śledczej przez organizację.
- Artykuł K. Reddy, H.S. Venter, M.S. Olivier[40] omawia kosztowe aspekty DFR na podstawie koncepcji rachunku kosztów działań TDABC (*Time Driven Activity-Based Costing*), co jest dość szczególnym, choć niewątpliwie bardzo istotnym aspektem zarządzania gotowością śledczą.
- W artykule L. Englbrecht, S. Meier, G. Pernul[41] zaproponowano pięciostopniowy model oceny dojrzałości DFR analogiczny do modelu CMMI wraz z cechami charakterystycznymi określającymi poszczególne poziomy dojrzałości:
  - Poziom 1: brak zdefiniowanych mierników i formalizacji, dochodzenie jest przeprowadzane chaotycznie i niestrukturalnie. Nie ma standardów ani dokumentacji określającej, w jaki sposób powinno się je prowadzić. Wiedza na temat informatyki śledczej i właściwego sposobu postępowania ze śladami cyfrowymi nie jest obecna w organizacji.
  - Poziom 2: istnieją podstawowe elementy prowadzenia działań związanych z DFR. Na przykład w przypadku dochodzenia wykorzystującego ślady cyfrowe występuje minimalna formalizacja procedur. Procesy mają charakter powtarzalny, obecna jest podstawowa dokumentacja. W organizacja funkcjonują pewne drobne elementy DFR, choć sama gotowość śledcza nie jest traktowana jako istotny temat w organizacji. Jest to poziom niewystarczający dla prowadzenia poważnych dochodzeń.
  - Poziom 3: organizacja ma ujednolicone procedury kryminalistyczne, udokumentowane procesy i formalne szkolenia. Zaangażowany personel

39 A. Almarzooqi, A. Jones, *A framework for assessing the core capabilities of a digital forensic organization*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84990047940&doi=10.1007%2f978-3-319-46279-0_3&origin=inward&txGid=8e92edb86f6a294018de510f7393ef62

40 K. Reddy, H.S, Venter, M.S. Olivier, *Using Time-Driven Activity-Based Costing to manage digital forensic readiness in large organisations*, https://www.scopus.com/record/display.uri?eid=2=-2s0.84874604833-&doi10=1007.2%f10796s011-9333--x&origin=inward&txGid-27224546d0b6c048598bb438a5715a27

41 L. Englbrecht, S. Meier, G. Pernul, *Towards a capability maturity model for digital forensic readiness*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85090513654&doi=10.1007%2f978-3-030-03898-4_10&origin=inward&txGid=0408dd034dfd57fd83a86390039ed979

właściwie rozumie znaczenie i konsekwencje śledztwa wykorzystującego ślady cyfrowe. Daje to organizacji możliwość zapobiegania potencjalnym niepowodzeniom już na wczesnym etapie dochodzenia.
  - Poziom 4: zaawansowana DFR. Oprócz poprzednich poziomów i aspektów, ten poziom charakteryzuje się profesjonalną implementacją DFR. Jest ona traktowana jako kwestia strategiczna. Zapewnione jest wsparcie kierownictwa, wdrożone są różne środki usprawniające procesy.
  - Poziom 5: pełna DFR, w tym ciągłe doskonalenie środków i struktur związanych z DFR. Zdefiniowanie celów doskonalenia procesów, wdrożenie formalnego szkolenia personelu i odpowiedniej akredytacji.
- W artykule S.R. Lim[42] omówiono studium przypadku dotyczące sposobu wprowadzenia zmian w zarządzaniu incydentami przez Koreę Południową po incydencie z 2009 roku, w którym – na skutek problemów z czujnikami typu Machine-to-Machine (M2M) – podczas awaryjnego zrzutu wody z tamy Hwang Nam do rzeki Imjin grupa Koreańczyków z Korei Południowej zamieszkująca dolną rzekę Imjin nie została ewakuowana na czas. W opisywanym przypadku zastosowano model wielostronnej wspólnej analizy (*Multilateral Joint Analysis*, MJA), a do wyznaczenia ostatecznego modelu wykorzystano metodę Delphi oraz model równań strukturalnych (*Structural Equation Model*, SEM). W ramach tego procesu ustanowiono mechanizm (w tym zestaw mierników pozwalających zapobiegać nieprawidłowemu działaniu wdrożonych produktów) mający na celu zabezpieczenie przed ukrytymi defektami, które powstają w trakcie rozwoju środowisk cyfrowych. Gotowość śledcza była rozpatrywana zarówno w kontekście możliwości ustalenia odpowiedzialności po wystąpieniu incydentu, jak i elementu zwiększającego bezpieczeństwo systemu już na etapie jego projektowania. Choć sam artykuł omawia szczególny przypadek dotyczący bezpieczeństwa infrastruktury krytycznej, Autor słusznie zauważa, że konieczność zapewnienia trafności (*accuracy*), wiarygodności (*reliability*) i bezpieczeństwa (*safety*) mechanizmów zbierania potencjalnych śladów dowodowych przez systemy informatyczne znajduje także szersze zastosowanie. Na przykład w ochronie zdrowia trudno sobie wyobrazić lekarzy, którzy korzystaliby z narzędzi cyfrowych, gdyby te nie zapewniały odpowiednich mechanizmów wykrycia i wykazania przyczyn możliwych błędów i w konsekwencji to sami lekarze mogliby być pociągnięci do odpowiedzialności prawnej za nieprawidłowe działanie narzędzi[43].

42 S.R. Lim, *Identifying management factors for digital incident responses on Machine-to-Machine services*, https://www.sciencedirect.com/science/article/pii/S1742287615000845?pes=vor&utm_source=scopus&getft_integrator=scopus#kwrds0010

43 Informatyka medyczna jest zresztą kolejnym miejscem, w którym trudno przecenić znaczenie prawidłowego zapewnienia wiarygodności cyfrowych śladów dowodowych. Zob. np. M. Chernyshev, S. Zeadally, Z. Baig, *Healthcare data breaches: Implications for digital forensic readiness*, „Journal of Medical Systems" 2019, Vol. 43(7), https://doi.org/10.1007/s10916-018-1123-2; A. Kyaw, B. Cusack, R. Lutui, *Digital forensic readiness in wireless medical systems*,

- W artykule S. Quinna[44] przedstawiono wyniki badania ankietowego przeprowadzonego wśród menedżerów IT w Nowej Zelandii dotyczącego stanu świadomości kadry kierowniczej IT w Nowej Zelandii w zakresie szeroko pojętej kryminalistyki cyfrowej oraz stanu ich przygotowania do ochrony danych cyfrowych w przypadku wystąpienia zdarzenia wymagającego zastosowania informatyki śledczej.
- W artykule L. De Marco, F. Ferrucci, T. Kechadi[45] autorzy proponują model *Cloud Forensic Readiness Capability for SLA management* (SLACFR), w którym gotowość śledcza jest rozumiana jako zdolność do wykrywania i rejestrowania sytuacji i zdarzeń związanych z niedopasowaniem poziomu świadczonych usług chmurowych do odpowiednich klauzul umowy o świadczeniu usług określających wymagane parametry usługi (Service Level Agreement, SLA), np. procent dostępności usługi w czasie (*uptime*). W szczególności gotowość śledcza odpowiada za monitorowanie parametrów i rozpoznanie, czy nie mają miejsca zdarzenia mogące stanowić naruszenie warunków umowy i za rejestrację takich zdarzeń, co jest czynnością poprzedzającą dochodzenie.
- Artykuł M. Elyas, A. Atif, S.B. Maynard, A. Lonie[46] opiera się na wcześniejszej pracy[47], w której zaproponowano ramy DFR oparte na kompleksowej analizie literatury od czasu wprowadzenia tego terminu (J. Tan, *Forensic Readiness*, 2001, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f7e0e2ef046f7755d2f7e6d) i omówiono wyniki badania trzech grup fokusowych składających się w sumie z 11 ekspertów informatyki śledczej z doświadczeniem biznesowym, akademickim, konsultingowym, wymiaru sprawiedliwości i wojskowym od trzech do pięciu uczestników związanych z różnymi organizacjami australijskimi. W konsekwencji badania zaproponowane zostały zmiany ram, które ostatecznie przybrały postać jak na rysunku 14.

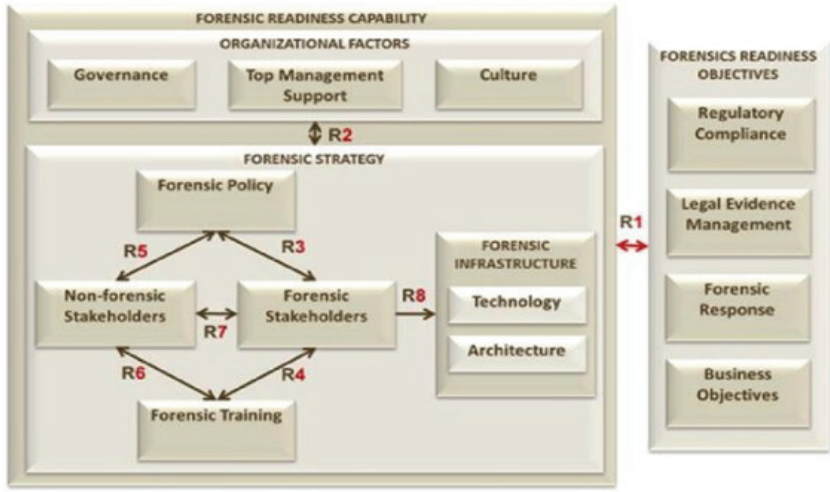
[w:] *29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand 2019, s. 1–6, https://doi.org/10.1109/ITNAC46935.2019.9078005

44 S. Quinn, *Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis*, https://www.sciencedirect.com/science/article/pii/S1742287605000873?pes=vor&utm_source=scopus&getft_integrator=scopus

45 L. De Marco, F. Ferrucci, T. Kechadi, *A Cloud Forensic readiness model for service level agreements management*, https://www.researchgate.net/profile/Lucia-De-Marco/publication/283106352_A_Cloud_Forensic_readiness_model_for_service_level_agreements_management/links/5637302908ae88cf81bd4f9d/A-Cloud-Forensic-readiness-model-for-service-level-agreements-management.pdf (dostęp: 5 stycznia 2025).

46 M. Elyas, A. Atif, S.B. Maynard, A. Lonie, *Digital forensic readiness: Expert perspectives on a theoretical framework*, „Computers and Security" 2015, Vol. 52.

47 M. Elyas, A. Atif, S.B. Maynard, A. Lonie, *Forensic readiness: Is your organisation ready?*, „Digital Forensics Magazine" 2014, Vol. 18, s. 58–62.



Rysunek 14. Ramy DFR zaproponowane w artykule M. Elyas, A. Atif, S.B. Maynard, A. Lonie, *Digital forensic readiness: Expert perspectives on a theoretical framework*
Źródło: M. Elyas, A. Atif, S.B. Maynard, A. Lonie, *Digital forensic readiness: Expert perspectives on a theoretical framework*, „Computers and Security" 2015, Vol. 52.

- Artykuł H.A. Nugroho, O.C. Briliyant, S.U. Sunaringtyas[48] zawiera porównanie dwóch ram DFR zaproponowanych wcześniej w pracach Elyas *et al.* (patrz wyżej) oraz przez I.P. Claimsa[49], a także propozycję ich połączenia w nowe ramy i opis przypadku ich zastosowania w lokalnej organizacji rządowej w zachodniej Jawie w Indonezji, co doprowadziło do stworzenia polityki bezpieczeństwa dla cyfrowej gotowości śledczej, która składa się z 8 rozdziałów i 33 artykułów odpowiadającym zidentyfikowanym parametrom DFR.
- W artykule R. Rowlingstona[50] zaproponowano 10 kroków:
  - Zdefiniuj scenariusze biznesowe, które wymagają dowodów cyfrowych.
  - Zidentyfikuj dostępne źródła i różne rodzaje śladów dowodowych.
  - Określ wymagania dotyczące gromadzenia[51] dowodów.

48 H.A. Nugroho, O.C. Briliyant, S.U. Sunaringtyas, *A novel Digital Forensic Readiness (DFR) framework for e-government*, [w:] *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, Bogor, Indonesia 2023, s. 184–189, https://doi.org/10.1109/ICoCICs58778.2023.10276423

49 W pracy I.P. Claims, *Digital Forensic Readiness: Proposing a Maturity Assessment Model*, 2015, https://www.goodreads.com/book/show/25333716-digital-forensic-readiness (dostęp: 5 stycznia 2025).

50 R. Rowlingson, *Ten step process for forensic readiness*, „International Journal of Digital Evidence" 2004, Vol. 2, Issue 3A, Winter, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=40baa64f868d9dc6c5a6111c4d3c757a7879754a

51 W oryginale *collection*, ale oczywiście, jak wszędzie w takich wypadkach, należy pod tym pojęciem rozumieć również przejmowanie (*acquisition*), czyli wykonywanie kopii bez fizycznego zbierania nośników. Niewątpliwie natomiast należy w takich sytuacjach zawsze decydować,

- Określ możliwość bezpiecznego gromadzenia prawnie dopuszczalnych dowodów w celu spełnienia wymagań.
- Ustanów zasady bezpiecznego przechowywania i obsługi potencjalnych dowodów.
- Upewnij się, że monitorowanie jest ukierunkowane na wykrywanie i zapobieganie poważnym incydentom[52].
- Określ okoliczności, w których uruchomić formalne dochodzenia (które może wykorzystywać dowody cyfrowe).
- Przeszkol personel w zakresie świadomości incydentów[53], aby wszystkie zaangażowane osoby rozumiały swoją rolę w procesie gromadzenia dowodów cyfrowych i prawną wrażliwość dowodów.
- Udokumentuj przypadek (w sposób) oparty na dowodach, opisujący incydent i jego wpływ[54].
- Zapewnij przegląd prawny w celu ułatwienia[55] podjęcia działań w odpowiedzi na incydent.

Jak widać z powyższego krótkiego przeglądu, autorzy zajmujący się DFR od strony zarządczej prezentują z punktu widzenia metodologii nauk o zarządzaniu paradygmat neopozytywistyczno-funkcjonalistyczno-systemowy i proponują bądź to traktowanie DFR jako części Systemu Zarządzania Bezpieczeństwem Informacji lub procesu zarządzania ryzykiem, bądź to tworzenie osobnych ram pozwalających określić jej składniki i zasady jej osiągania. Ciekawym kierunkiem wydaje się też określanie stopnia dojrzałości DFR przez analogię do koncepcji dojrzałości procesowej, w szczególności CCMM[56].

---

czy planowane jest gromadzenie, czy przejmowanie danych, czy działania będą prowadzone w trybie *live* czy *post mortem*, czy mowa o pełnych danych czy o wytypowanych wcześniej danych częściowych (*procedury triage*) itd. Por. np. M. Szmit, *Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence – a basic guide for First Responders*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2015, s. 101–110.

52 Zalecenie to dotyczy dwóch kwestii: po pierwsze, bieżące monitorowanie źródeł, które mogą dostarczać informację cenną z punktu widzenia śledztwa może pełnić rolę analogiczną do roli systemów wykrywania włamań, warto więc je wdrożyć nie tylko po to, żeby po wystąpieniu incydentu mieć możliwość jego analizy, ale i aby móc nań na bieżąco reagować, po wtóre, zawsze tego rodzaju rozwiązania generują pewną liczbę alarmów fałszywie pozytywnych (błędy I rodzaju), sensowne jest więc skupienie się na sytuacjach mających potencjalnie duży wpływ na cele organizacji.

53 W oryginale *awareness*, mowa więc nie tylko o wiedzy na temat tego, że incydenty mogą się wydarzyć ale również o umiejętności właściwego zachowania się w razie ich wystąpienia. W zakresie DFR warto zwrócić szczególną uwagę na możliwość mimowolnego zatarcia śladów cyfrowych, zwłaszcza w odniesieniu do danych ulotnych.

54 Mowa o przygotowaniu dokumentacji, która będzie mogła być użyteczna dla potrzeb postępowania prokuratorskiego, sądowego czy dyscyplinarnego, ale także dostarczy informacji zwrotnej pozwalającej uniknąć na przyszłość wystąpienia incydentów bezpieczeństwa.

55 W oryginale *facilitate*, mowa jest o ocenie prowadzonych działań przez doradców prawnych.

56 Por. np. E.H.S.S. Al Hanaee, R. Awais, *DF-C²M²: A comprehensive capability maturity model for digital forensics organisations*, PhD thesis, Lancaster University, 2016, https://eprints.lancs.ac.uk/id/eprint/82480/ (dostęp: 5 stycznia 2025).

4. Cyfrowa gotowość śledcza w Polsce – wybrane przykłady

4.1. Rekomendacje krajowe

W tekstach pisanych w języku polskim pojęcia: „gotowości śledczej" i „gotowości dochodzeniowej" występują sporadycznie[1]. Wyrażenie „gotowość dochodzeniowa" *explicite* można znaleźć w dwóch dokumentach: materiałach Narodowego Banku Polskiego z lipca 2024 roku zatytułowanych *Materiał opracowany na podstawie CROE przez Departament Stabilności Finansowej* oraz w polskiej wersji tychże *Wymagań*…[2] Pojęcie gotowości dochodzeniowej CROE definiuje jako „zdolność IRF do maksymalizacji wykorzystania dowodów cyfrowych w celu identyfikacji charakteru ataku cybernetycznego" (IRF oznacza Infrastruktury Rynku Finansowego), podając jako źródło wytyczne CPMI-IOSCO[3].

W dokumencie EBC zdefiniowano trzy poziomy dojrzałości cybernetycznej, nazwane poziomem rozwojowym, zaawansowanym oraz innowacyjnym. Wymagania podzielono na dziewięć podrozdziałów, z czego pięć dotyczy kategorii zarządzania ryzykiem (zarządzanie[4], identyfikacja, ochrona, wykrywanie oraz reagowanie i odzyskiwanie), zaś cztery – elementów nadrzędnych[5] (testowania,

1 Wyszukiwarka Google (21.12.2024) zwraca osiem wyników zapytania „Gotowość śledcza", z czego cztery prowadzą do tekstów reklamowych form consultingowych a cztery pozostałe nie są związane z tematyką gotowości do śledztwa cyfrowego.

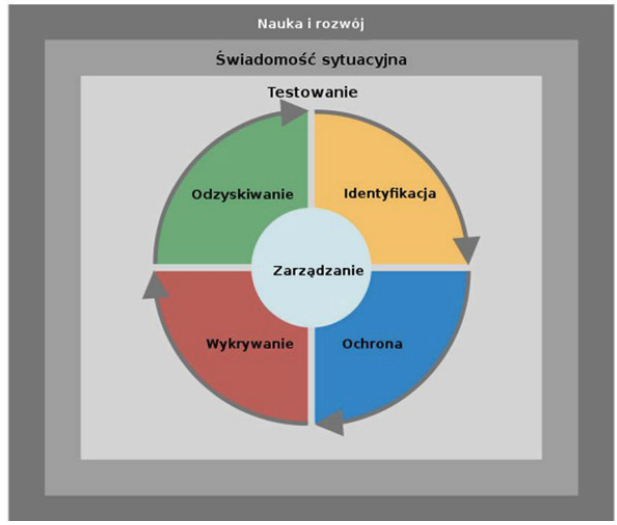
2 Dalej CROE (*Cyber resilience oversight expectations for financial market infrastructures*) – dokument „Wymagania nadzorcze w zakresie cyberodporności dla infrastruktur rynku finansowego" wydany przez Europejski Bank Centralny w grudniu 2018 roku.

3 International Organization of Securites Commissions and the Committee on Payments and Market Infrastructures, https://www.iosco.org/v2/about/?subsection=cpmi_iosco (dostęp: 5 stycznia 2025).

4 W oryginale *goveranance*, polskie tłumaczenie jest więc o tyle nieszczęśliwe, że kategorią zarządzania ryzykiem jest zarządzanie ryzykiem, podczas gdy w dokumencie dalej mowa o nadzorze (np. rozdział 2.1.2.2 *Role of the Board and senior management* przetłumaczone jako „Rola Organu Zarządzającego IRF i kadry kierowniczej wyższego szczebla").

5 Ang. *overarching components*.

świadomości sytuacyjnej oraz nauki i rozwoju). Wzajemny stosunek tych elementów został pokazany na rysunku 15.



Rysunek 15. Struktura wymagań CROE
Źródło: EBC, Wymagania nadzorcze w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego, 2018, https://nbp.pl/wp-content/uploads/2022/07/Wymagania-nadzorcze-wz-odpornosci-cybernetycznej.pdf (dostęp: 5 stycznia 2025).

Można zauważyć podobieństwo tej struktury z modelem NIST CSF 2.0 (por. rysunek 11).

W rozdziale 2.5 (*Reagowanie i odzyskiwanie*) zdefiniowano poszczególne poziomy dojrzałości gotowości dochodzeniowej, jak następuje[6]:

> 2.5.2.4 Gotowość dochodzeniowa
> POZIOM ROZWOJOWY
> 45. IRF powinna określić scenariusze zagrożeń, które mogą potencjalnie wpłynąć na jej działalność i określić, które elementy dowodów cyfrowych (np. rodzaje dzienników zdarzeń) powinny być zebrane w celu ułatwienia dochodzenia kryminalistycznego.
> 46. IRF powinna zidentyfikować i udokumentować cyfrowe dowody dostępne w jego systemach i jego pomieszczeniach oraz zrozumieć, w jaki sposób należy postępować z dowodami przez cały okres ich istnienia.
> 47. Na podstawie oczekiwań nr 45 i nr 46 IRF powinna opracować i wdrożyć politykę gotowości dochodzeniowej oraz posiadać możliwości wsparcia dochodzenia kryminalistycznego. Polityka powinna także zawierać politykę rejestrowania zdarzeń systemowych wskazująca rodzaj dzienników zdarzeń, które mają być utrzymywane, oraz okresy ich przechowywania. IRF może zlecić prowadzenie wymienionych dochodzeń zewnętrznym usługodawcom.

6 Zachowano oryginalną pisownię, wraz z błędami.

48. IRF powinna ustanowić procedury bezpiecznego gromadzenia dowodów cyfrowych w sposób niebudzący wątpliwości, co do ich wiarygodności, zgodnie z wymogami określonymi w polityce gotowości dochodzeniowej i właściwymi przepisami prawa obowiązującymi w danej jurysdykcji. Procedury te powinny opisywać, w jaki sposób personel dochodzeniowy powinien, punkt po punkcie, wytworzyć dokumentację wszystkich aktywności dokonanych na dowodach cyfrowych, oraz ich wpływ.
49. IRF powinna opracować zasady bezpiecznego postępowania z zebranymi dowodami cyfrowymi oraz bezpiecznego ich przechowywania, zapewniając ich autentyczność i integralność. IRF powinna opracować procedury, by wykazać, że zachowano integralność dowodów podczas każdorazowego uzyskiwania do nich dostępu, użytkowania ich i ich przenoszenia tzw. łańcuch nadzoru (ang. *chain of custody*).
50. IRF powinna przeszkolić swój personel tak, aby wszyscy jego członkowie powiązani z incydentem rozumieli swoje zakresy odpowiedzialności związane z obsługą dowodów cyfrowych, upewniając się, że nie zostały one naruszone i nie budzą wątpliwości, co do ich wiarygodności zgodnie z właściwymi przepisami prawa obowiązującymi w danej jurysdykcji.
51. IRF powinna zapewnić, by personel zaangażowany w dochodzenie kryminalistyczne posiadał odpowiedni poziom kompetencji w zakresie obsługi dowodów cyfrowych i potrafił zapewnić autentyczność, integralność oraz wiarygodność dowodów cyfrowych zgodnie z właściwymi przepisami prawa obowiązującymi w danej jurysdykcji.
POZIOM ZAAWANSOWANY
52. IRF powinna ściśle zintegrować swoją politykę gotowości dochodzeniowej z planami reagowania na incydenty cybernetyczne i innymi powiązanymi działaniami w zakresie planowania biznesowego.
POZIOM INNOWACYJNY
53. IRF powinna dysponować procesem zarządczym, którego celem jest regularny przegląd i aktualizacja polityki gotowości dochodzeniowej zgodnie z doświadczeniem i nową wiedzą.
54. IRF powinna wykazać się gotowością do współpracy w ramach ekosystemu w celu usprawnienia metod stosowanych w dochodzeniach kryminalistycznych oraz metodologii i narzędzi do obsługi incydentów[7].

Należy uznać, że wszystkie zawarte w dokumencie postulaty są słuszne, nie tylko dla podmiotów działających na rynku finansowym, ale w ogólności dla organizacji pragnących zbudować gotowość śledczą. Odnośnie do poszczególnych punktów warto zwrócić uwagę na kwestie takie jak:

- Ad. 45. Nie zawsze jest możliwe szczegółowe opracowanie scenariuszy materializacji zagrożeń, może się zdarzyć – choć nie powinno – że pojawi się zagrożenie nie zidentyfikowane na etapie analizy ryzyka. Właściwe jest

7 Źródło: NBP: Materiał opracowany na podstawie CROE* Departament Stabilności Finansowej, 2024, https://nbp.pl/wp-content/uploads/2024/10/Materialy_pomocnicze_CROE_lipiec_2024.pdf (dostęp: 5 stycznia 2025).

natomiast opracowanie scenariuszy działania na wypadek materializacji różnych ryzyk. Niektóre ślady dowodowe mogą być na pewno użyteczne w przypadku, gdy pojawią się problemy z poszczególnymi zasobami. W tym sensie odniesienie do dzienników zdarzeń – gromadzonych przecież nie dla zagrożeń, ale dla zasobów jest słuszne. Warto jednak pamiętać, że – zgodnie z tym, o czym wspomniano wcześniej – dzienniki zdarzeń nie są zazwyczaj tworzone w celu ułatwienia postępowania dowodowego, ale w celu usprawnienia procesu rozwiązywania problemów technicznych z konkretnym systemem, stąd też celowe może być ich uzupełnienie o odpowiednie kopie bezpieczeństwa danych bądź metadanych, które mogą mieć znaczenie śledcze.

- Ad. 47 i 48: zasady postępowania z materiałem dowodowym powinny dotyczyć zarówno jego gromadzenia jak i przejmowania (w tym wykonywania kopii cyfrowych)
- Ad. 49: mowa o ciągłości łańcucha dowodowego. Nie jest ona formalnie wymagana w polskich przepisach, ale jej brak może uczynić dowód zupełnie niewiarygodnym.

Wydaje się, że jeśli mowa o możliwości stosowania tych zaleceń w innych organizacjach, należałoby – przy okazji integracji planów (a nie polityk, jak to przetłumaczono w polskiej wersji dokumentu) gotowości dochodzeniowej z planami reagowania na incydenty cybernetyczne i innymi powiązanymi działaniami w zakresie planowania biznesowego (p. 52) – wspomnieć o planach ciągłości działania, być może nie dopiero na zaawansowanym, ale już na podstawowym (rozwojowym) poziomie dojrzałości. O ile bowiem w przypadku infrastruktury rynku finansowego jest raczej mało prawdopodobne, aby organy ścigania zdecydowały się na gromadzenie materiału dowodowego w sposób mogący naruszyć ciągłość działania tegoż rynku, o tyle w przypadku mniejszych lub mniej ważnych organizacji (jak również w przypadku gdy szybkość pozyskanie dowodów może mieć charakter krytyczny dla zdrowia bądź życia, ewentualnie dla bezpieczeństwa państwa), ewentualnie gdy ciągłość działania organizacji zostanie oceniona jako wartość mniejsza niż dobro postępowania dowodowego może dojść do takich sytuacji (np. zarekwirowania komputerów jako dowodów rzeczowych w śledztwie, co oczywiście może zaburzyć ciągłość działania organizacji).

Do kwestii gotowości śledczej odnosi się również – nie używając wprawdzie tego terminu – Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego[8] Wer. 1.0. Jest to jeden z dokumentów Narodowych Standardów Cyberbezpieczeństwa – zbioru rekomendacji dla podmiotów chcących efektywnie zarządzać systemami bezpieczeństwa informacji opracowanych przez Departament Cyberbezpieczeństwa w Ministerstwie Cyfryzacji na podstawie

8 Narodowy Standard Cyberbezpieczeństwa NSC 800-61 wer. 1.0. Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego, https://www.gov.pl/attachment/c38e6fd7-c561-4c97-945b-57a72a4a100f (dostęp: 5 stycznia 2025).

dokumentów NIST. Na stronie 72 w rozdziale 3.4.3. *Retencja dowodów* zawarte są następujące zalecenia:

> Organizacje powinny ustalić zasady dotyczące tego, jak długo należy przechowywać dowody z incydentu. Większość organizacji decyduje się na przechowywanie wszystkich dowodów przez okres zgodny z obowiązującymi przepisami prawnymi. Podczas opracowywania zasad należy wziąć pod uwagę następujące czynniki:
> - Ściganie. Jeśli jest prawdopodobne, że atakujący zostanie postawiony przed sądem, może być konieczne przechowywanie dowodów do czasu zakończenia wszystkich czynności prawnych. W niektórych przypadkach może to zająć kilka lat. Ponadto dowody, które wydają się teraz nieistotne, mogą stać się kluczowe w przyszłości. Na przykład, jeśli atakujący jest w stanie wykorzystać wiedzę zebraną podczas jednego ataku, aby później przeprowadzić poważniejszy atak, dowody z pierwszego ataku mogą być kluczowe dla wyjaśnienia, w jaki sposób drugi atak został dokonany.
> - Retencja danych. Większość organizacji ma ustalone zasady retencji danych, które określają, jak długo można przechowywać określone typy danych. Na przykład organizacja może określić, że wiadomości e-mail powinny być przechowywane tylko przez 180 dni. Jeśli obraz dysku zawiera tysiące wiadomości e-mail, organizacja może nie chcieć, aby był przechowywany dłużej niż 180 dni, chyba że jest to absolutnie konieczne. Jak omówiono w rozdziale 3.4.2, W podmiotach realizujących zadania publiczne czas retencji określają przepisy.
> - Koszty. Oryginalny sprzęt (np. dyski twarde, systemy, których zabezpieczenia zostały naruszone), który jest przechowywany jako dowód, a także dyski twarde i nośniki wymienne używane do przechowywania obrazów dysków są na ogół niedrogie. Jeśli jednak organizacja przechowuje wiele takich komponentów przez lata, koszt może być znaczny. Organizacja musi również zachować funkcjonujące komputery, które mogą korzystać z magazynowanego sprzętu i nośników.

oraz kilka punktów z rozdziału 3.6. *Rekomendacje*[9]:

- Ustanowienie mechanizmów umożliwiających stronom zewnętrznym zgłaszanie incydentów.
- Wymaganie podstawowego poziomu rejestrowania i audytowania we wszystkich systemach oraz wyższego poziomu dla wszystkich systemów krytycznych.
- Utworzenie zasad retencji dzienników
- Synchronizacja wszystkich zegarów hosta
- Rozpoczęcie rejestrowania wszystkich informacji, gdy tylko zespół zacznie
- podejrzewać, że doszło do incydentu
- Zabezpieczenie danych z incydentów

9 Tam, gdzie mowa o „zegarach hosta", chodzi zapewne o synchronizacji zegarów lokalnych w różnych systemach i programach, bowiem nieprawidłowo działające zegary powodują zapisanie niewłaściwych informacji o czasie różnych zdarzeń, co uniemożliwia np. korelację zdarzeń czy ustalenie ich kolejności.

- Ustalenie priorytetów obsługi incydentów na podstawie istotnych czynników
- Uwzględnienie w zasadach reagowania na incydenty organizacji postanowień dotyczących zgłaszania incydentów
- Przestrzeganie ustalonych procedur gromadzenia i postępowania z dowodami
- Retencja ulotnych danych z systemów jako dowodów
- Uzyskiwanie z systemu wstępnych zrzutów pełnych obrazów dysków do badań sądowych, a nie z kopii zapasowych systemu plików
- Organizowanie spotkań na temat zdobytego doświadczenia po poważniejszych incydentach.

Choć – podobnie jak dokumenty NIST – opracowania NSC nie dotyczą zarządczych aspektów gotowości śledczej, a w tym wypadku odnoszą się do obsługi incydentów bezpieczeństwa informacji, należy powyższe zalecenia uznać za bardzo trafne i zasługujące na wdrożenie w różnych organizacjach. Kwestia retencji danych jest bardzo istotna, praktyka pokazuje bowiem, że w przypadku informacji o krótkim czasie retencji (np. nagraniach z monitoringu CCTV) zbyt powolne prowadzenie śledztwa powoduje, że dane są usuwane zanim okazuje się, że mogą być potrzebne w śledztwie. Osobną kwestią – również poruszoną w samym dokumencie, wprawdzie w odniesieniu do kopii bitowych (obrazów) wolumenów – jest możliwość wykorzystania nośników jednokrotnego zapisu (*Write Once Read Many*, WORM). Warto zauważyć, że może to być również – w przypadku kopii zapasowych – dodatkowe zabezpieczenie przed atakami typu randsomware, szyfrującymi dane użytkownika i żądającymi okupu za dostęp do nich. Z drugiej strony istniejące przepisy i regulacje mogą budzić wątpliwości odnośnie do możliwości przechowywania (lub przechowywania przez dłuższy czas) np. informacji wrażliwych a nawet odnośnie do możliwości ich wykorzystania: w polskim systemie prawnym istnieje wiele przepisów ograniczających możliwość przetwarzania różnego rodzaju danych. Można wspomnieć tu choćby o tajemnicy państwowej, adwokackiej, radcowskiej, lekarskiej, tajemnicy postępowania przygotowawczego, tajemnicy skarbowej, tajemnicy dziennikarskiej itd. Szczegółowe przepisy określają również czas retencji danych bankowych czy telekomunikacyjnych. Oczywiście należy również pamiętać o tajemnicy korespondencji, a także o ograniczeniach odnośnie do możliwości gromadzenia i przetwarzania szczególnych rodzajów informacji (np. na mocy art. 202 § 4a. KK nie wolno nawet uzyskiwać dostępu do materiałów pornograficznych, nie mówiąc już o ich posiadaniu czy przechowywaniu, a przecież incydent bezpieczeństwa informacji może się wiązać również z umieszczeniem tego rodzaju treści na maszynie będącej własnością organizacji), ograniczenia w możliwości zbierania i przetwarzania informacji do celów śledczych są więc duże i często nieintuicyjne jest więc to kolejne zagadnienie, przy którym do budowy DFR konieczne jest zachowanie zgodności z przepisami prawa, a więc i wsparcie ze strony prawników organizacji[10].

10 Por. np. W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Wolters Kluwer, Warszawa 2021, s. 108.

4.2. Przykłady praktyczne

W naukach o zarządzaniu i jakości, tak jak przynajmniej w części innych nauk społecznych, praktycznym kryterium oceny jakości postępowania często jest zgodność z tzw. najlepszymi (ewentualnie dobrymi) praktykami. Praktyki te często są skodyfikowane (np. pod postacią reguł postępowania zawodowego, standardów czy metodyk), niejednokrotnie posiadają też odpowiednią podbudowę teoretyczną, a przynajmniej statystycznie uwiarygodnione współwystępowanie faktu ich stosowania z sukcesem działań, których dotyczą i szeroki consensus wśród osób zawodowo i naukowo zajmujących się nimi. Oczywiście postępowanie w zgodzie z takimi regułami nie jest gwarancją sukcesu (bywa też, że same reguły po jakimś czasie okazują się niesłuszne), niemniej wobec braku takich praktyk (a nawet prac studialnych zmierzających do ich opracowania) można spodziewać się, że krajowa praktyka w tym względzie będzie bardzo odbiegać od stanu pożądanego.

Trudno jest gotowość organizacji do przeprowadzenia dochodzenia wykorzystującego ślady cyfrowe oceniać *ex ante*, szczególnie z pozycji zewnętrznej w stosunku do organizacji, bez dostępu do jej wewnętrznych dokumentów. Z jednej strony organizacje nie są zainteresowane ujawnianiem swojego braku gotowości, zgodnie ze wspomnianym wcześniej podejściem „bezpieczeństwo przez niejawność", z drugiej brak jednolitych kryteriów oceny czy nawet zasad zapewniania takiej gotowości utrudniałby przeprowadzenie miarodajnych porównań. Można natomiast spróbować odnieść się do sytuacji, w których brak takiej gotowości się – w mniej lub bardziej widowiskowy sposób – ujawnił. Tylko w ostatnich latach doszło do kilku takich zdarzeń, świadczących nie tylko o braku DFR w poszczególnych organizacjach, ale o głębszych problemach natury systemowej. Jako przykłady można wymienić tu – obok niewątpliwie nośnych medialnie, ale stosunkowo niegroźnych w skutkach, włamań na konta społecznościowe różnych[11] polityków – choćby sprawy kopalni kryptowalut w budynku Naczelnego Sądu Administracyjnego czy domniemanej instalacji bomb logicznych w pociągach Impuls firmy Newag. Ponieważ obie sytuacje opisane są poniżej wyłącznie na podstawie źródeł wtórnych (w dużej mierze artykuły w prasie popularnej i na portalach internetowych), bowiem

11 Zob. np. *Minister Cyfryzacji zhackowany na Twitterze*, https://niebezpiecznik.pl/post/minister-cyfryzacji-zhackowany-na-twitterze (dostęp: 5 stycznia 2025); *Zdjęcia kobiety w bieliźnie. Włamanie na twitterowe konto Marka Suskiego*, https://www.polsatnews.pl/wiadomosc/2021-01-18/zdjecia-kobiety-w-bieliznie-wlamanie-na-twitterowe-konto-marka-suskiego/ (dostęp: 5 stycznia 2025); W. Karpieszczuk, *Wulgarny wpis o strajkujących kobietach na Facebooku minister Maląg. Znowu włamanie na konto polityka PiS*, https://warszawa.wyborcza.pl/warszawa/7,54420,26610927,wulgarny-wpis-o-strajkujacych-kobietach-na-facebooku-minister.html (dostęp: 5 stycznia 2025); K. Winogrodzki, *Włamanie na twitterowe konto senatora PiS. Polityk zabrał głos*, https://wiadomosci.wp.pl/wlamanie-na-twitterowe-konto-senatora-pis-polityk-zabral-glos-6612088347249600a (dostęp: 5 stycznia 2025).

wykorzystanie akt sądowych[12], a tym bardziej prokuratorskich w trakcie trwania postępowania[13] byłoby niedopuszczalne prawnie, stąd też należy je potraktować nie jako pełnoprawne studia przypadków czy analizy, ale jedynie jako pewne egzemplifikacje samego zjawiska braku gotowości śledczej i jego implikacji.

Sytuacja kopalni kryptowalut została opisana w artykule A. Węgrzynowicza i K. Ziółkowskiej: „Urządzenia o dużej mocy obliczeniowej wykorzystywane w obrocie kryptowalutami odkryto w siedzibie Naczelnego Sądu Administracyjnego w Warszawie. Miejsce ich ukrycia wskazał pracownik techniczny sądu, który wcześniej był związany z firmą zewnętrzną odpowiadającą za serwis techniczny budynku. Komputery pobierające mnóstwo energii elektrycznej ukryte były w kanale wentylacyjnym oraz w podłodze technicznej”[14].

Obecnie NSA złożył pozew przeciwko firmie remontowej[15], trwa natomiast postępowanie dowodowe[16], choć nikomu nie postawiono zarzutów.

Sytuacja dotycząca pociągów Impuls została opisana po raz pierwszy w artykule A. Haerle w sposób następujący:

> […] wiosną 2022, […] kończy się serwis pierwszego z jedenastu pociągów Newag Impuls 45WE, eksploatowanych przez Koleje Dolnośląskie. Serwis prowadzi firma Serwis Pojazdów Szynowych […]. SPS wygrał przetarg na przeprowadzenie obowiązkowego przeglądu pociągów po pokonaniu dystansu 1 000 000 kilometrów. W przetargu na przeprowadzenie przeglądu startował także producent pociągu, polska firma Newag, jednak oferta producenta była o 3 mln zł wyższa i ostatecznie przetarg wygrał SPS, który zaproponował, że serwis przeprowadzi za 22 mln zł. […] SPS przeprowadza przegląd zgodnie z odpowiednią instrukcją (o objętości ok. 20 000 stron), dostarczoną przez producenta, lecz pociąg po poskładaniu nie rusza […] Drugi pociąg przechodzi identyczny serwis, z identycznym skutkiem […] Trzeci nie trafia na przegląd na skutek awarii akumulatorów, więc zamiast niego do serwisu przysłany zostaje pociąg czwarty […] Po podłączeniu czwartego (jeżdżącego) do jednego z nieruchomych, nieruchomieje także jeżdżący […] Na dokładkę w innym warsztacie, w Szczecinie, inny Impuls psuje się w bardzo podobnych okolicznościach […] Skoro mechanicy ani elektrycy nie dają rady, to w końcu ktoś wpisuje w Google „polscy

12 W sprawie pociągów część zeznań została utajniona. Zob. P. Makowiec, *Blokady w pociągach Newagu. Zwrot w sprawie?*, https://cyberdefence24.pl/cyberbezpieczenstwo/blokady-w-pociagach-newagu-zwrot-w-sprawie (dostęp: 5 stycznia 2025).

13 Z uwagi na tajemnicę postępowania przygotowawczego (art. 241 KK).

14 A. Węgrzynowicz, *Kopalnia kryptowalut w budynku NSA. Miejsce ukrycia komputerów wskazał były pracownik firmy konserwatorskiej*, https://tvn24.pl/najnowsze/warszawa-kopalnia-kryptowalut-odkryta-w-budynku-naczelnego-sadu-administracyjnego-st7429795 (dostęp: 5 stycznia 2025).

15 Zob. *Milionowa strata i pozew. Reakcja NSA po odkryciu kopalni kryptowalut w jego siedzibie*, https://tvn24.pl/tvnwarszawa/srodmiescie/warszawa-kopalnia-kryptowalut-w-siedzibie-naczelnego-sadu-administracyjnego-kara-dla-firmy-swiadczacej-uslugi-i-pozew-st7827103 (dostęp: 5 stycznia 2025).

16 *Kopalnia kryptowalut w siedzibie NSA. Nowe informacje*, https://www.rp.pl/prawo-karne/art39543671-kopalnia-kryptowalut-w-siedzibie-nsa-nowe-informacje (dostęp: 5 stycznia 2025).

hakerzy" i na szczycie listy wyników trafia na artykuł o sukcesach grupy Dragon Sector […] Do terminu zakończenia prac pozostaje mniej niż doba, gdy odnajdują konfigurację flag, która daje szansę uruchomienia pociągu. Niestety w trakcie eksperymentów płonie ostatni działający komputer pokładowy […] Po kolejnej burzy mózgów i wielu próbach poskładania dwóch uszkodzonych komputerów w jeden udaje się naprawić ten spalony i o 2 w nocy, w noc poprzedzającą godzinę sądu ostatecznego, badacze konfigurują komputer, który ma uruchomić pociąg […]. W końcu rano badacz z komputerem dociera na miejsce, podłącza módlmy-się-aby-zadziałał-komputer do popsutego pociągu, ale pociąg nie rusza. Kolejna burza mózgów pozwala zidentyfikować jedną flagę, o której zapomniano i o 8:42 pociąg udaje się uruchomić. […] Miesiące analiz i inżynierii wstecznej pozwoliły na odkrycie niezwykle ciekawych warunków zapisanych w kodzie oprogramowania różnych pociągów dostarczonych przez Newag. Znalezione w kodzie komputera wartości liczbowe […] są to koordynaty GPS wskazujące na okolice Dworca Kolejowego Bydgoszcz Główna, a konkretnie znajdującego się tuż obok serwisu firmy PESA. Wkrótce odnaleziono także koordynaty innych serwisów, które mogłyby prowadzić naprawy i przeglądy pociągów w Polsce […] W kodzie komputera zapisano warunek nakazujący wyłączenie możliwości uruchomienia pociągu, jeśli spędzi przynajmniej 10 dni w jednym z tych warsztatów […] Niespodzianki czyhały nie tylko w oprogramowaniu komputerów. Badacze w jednym ze składów odkryli urządzenie podpisane jako „konwerter UDP<->CAN", przypuszczalnie umożliwiające zdalną komunikację z pociągiem. Jego wymontowanie nie sprawiło, że cokolwiek przestało działać. Analiza wykazała, że pokładowy komputer wysyłał do tego urządzenia informacje o stanie blokad, a samo urządzenie było podłączone do modemu GSM[17].

Do dzisiaj (a więc w ponad dwa lata po opisywanych zdarzeniach i w rok od opisania jej w mediach) nie postawiono nikomu żadnych zarzutów, za to firma Newag złożyła trzy pozwy: Jeden – w Sądzie Okręgowym w Warszawie przeciwko firmie SPS i analitykom z grupy Dragon Sector dotyczący naruszenia praw autorskich[18], drugi w Sądzie Okręgowym w Gdańsku – dotyczący naruszenia dobrego imienia oraz aktu nieuczciwej konkurencji[19] oraz trzeci – przeciwko posłance Paulinie Matysiak zarzucając jej naruszanie dobrego imienia firmy[20]. Część komentatorów

17 A. Haerle, *O trzech takich, co zhakowali prawdziwy pociąg – a nawet 30 pociągów*, https://zaufanatrzeciastrona.pl/post/o-trzech-takich-co-zhakowali-prawdziwy-pociag-a-nawet-30-pociagow (dostęp: 5 stycznia 2025).

18 Zob. R. Kędzierski, *Rusza proces wytoczony przez Newag. Istotna zmiana zarzutów*, https://www.money.pl/gospodarka/rusza-proces-wytoczony-przez-newag-istotna-zmiana-zarzutow-7066384013548128a.html, https://tvn24.pl/biznes/najnowsze/newag-kontra-hakerzy-z-dragon-sector-zarzucili-spolce-celowe-wylaczanie-pociagow-teraz-dostali-pozew-st7984811 (dostęp: 5 stycznia 2025).

19 Zob. P. Makowiec, *Sprawa blokad w Impulsach. Newag po raz drugi pozywa Dragon Sector i SPS*, https://cyberdefence24.pl/polityka-i-prawo/sprawa-blokad-w-impulsach-newag-po-raz-drugi-pozywa-dragon-sector-i-sps (dostęp: 5 stycznia 2025).

20 Zob. J. Świder, *Newag pozywa posłankę Paulinę Matysiak. „Naruszanie dobrego imienia"*, https://biznes.interia.pl/gospodarka/news-newag-pozywa-poslanke-pauline-matysiak-naruszanie-dobrego-im,nId,7872162 (dostęp: 5 stycznia 2025).

wskazuje, że działania takie mogą być pozwami zmierzającymi do stłumienia debaty publicznej (SLAPP – *Strategic Lawsuit Against Public Participation*). Samo zjawisko SLAPP zostało dostrzeżone przez europejskiego prawodawcę[21], ale nie znalazło jeszcze odpowiedniego miejsca w prawodawstwie krajowym (na marginesie warto zauważyć, że pozywanie uczestników procesu nie ogranicza się ani do kwestii dowodów cyfrowych, ani do stron procesu, pozywani bywają biegli[22], a nawet sędziowie, fakt pozostawania biegłego lub sędziego w sporze cywilnym ze stroną może być bowiem przesłanką o wnioskowanie o jego wyłączenie z procesu, co może mieć znaczenie taktyczne, np. w sytuacji, gdy pojawia się możliwość przedawnienia lub przeciągnięcia biegu sprawy; oczywiście nie każdy taki pozew musi być bezzasadny).

Nie rozstrzygając o meritum obu, warto zauważyć, że obie sprawy powinny być istotne z punktu widzenia bezpieczeństwa państwa: sama możliwość nieautoryzowanego unieruchomienia pociągów jest niewątpliwie poważnym zagrożeniem funkcjonowania infrastruktury krytycznej (zdalne unieruchomienie pociągu może prowadzić do zablokowania magistrali kolejowej, przy czy mowa nie tylko o jednorazowym zatrzymaniu pociągu[23], ale o możliwości jego długotrwałego unieruchomienia), kwestią znacznie ważniejszą od – szacowanych na ponad milion złotych – strat jakie poniósł skarb państwa za energię zużytą do zasilania koparek kryptowalut w NSA jest kwestia bezpieczeństwa fizycznego budynków NSA, w których możliwa okazała się nieautoryzowana instalacja i eksploatacja koparek oraz ich skuteczne ukrycie w obrębie budynku. Łatwo sobie wyobrazić bowiem scenariusze zainstalowania urządzeń znacznie bardziej niebezpiecznych.

Z punktu widzenia zarządzania gotowością (zarówno biorąc pod uwagę ewentualne działania typu SLAPP, jak i przede wszystkim dla skutecznego udowodnienia przed sądem swoich racji) śledczą narzucają się dwa wnioski:

- po pierwsze: już sam czas trwania dochodzeń zdaje się potwierdzać przedstawione w pierwszym rozdziale uwagi o niskiej skuteczności prawnokarnej ochrony bezpieczeństwa informacji, a więc z punktu widzenia zarządzania należy rozważyć potrzebę wdrożenia zabezpieczeń natury organizacyjnej czy technicznej, które pozwolą organizacji zmniejszyć czy to prawdopodobieństwo czy skutki ewentualnego naruszenia bezpieczeństwa, bez nadmiernej ufności w skuteczność mechanizmów prawnych, a w szczególności w efektywność działania organów ścigania i mechanizmy prawa karnego. W takiej

21 Zob. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1069 z dnia 11 kwietnia 2024 r. w sprawie ochrony osób, które angażują się w debatę publiczną, przed oczywiście bezzasadnymi roszczeniami lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej") PE/88/2023/REV/1, Dz. U. L, 2024/1069, 16.4.2024.

22 Zob. np. M. Szmit, *O pewnym nowym przepisie i jednym precedensowym wyroku*, „Rocznik Bezpieczeństwa Morskiego" 2021, s. 195–208.

23 Tego rodzaju nadużycia, np. związane z podatnościami systemu Radiostop, zdarzają się ponad sto razy rocznie. Zob. np. Rynek Kolejowy, *Nieuprawnione użycie Radiostop. Pierwsze dane za 2024 rok mało optymistyczne*, https://www.rynek-kolejowy.pl/wiadomosci/nieuprawnione-uzycie-radiostop-120148.html (dostęp: 5 stycznia 2025).

gotowość śledcza organizacji może być istotna o tyle, że dla wszczęcia procesu cywilnego nie jest konieczne zakończenie ewentualnego postępowania karnego czy nawet dowodowego przez organy ścigania i można dla jego potrzeby posłużyć się dowodami zgromadzonymi przez stronę. Pamiętać należy jednak, że o ile można myśleć o takich mechanizmach w przypadku „klasycznych" przestępstw przeciwko mieniu (kradzież, zniszczenie), o tyle trudno jest naprawić oszacować i straty wizerunkowe (*reputational damage*), które organizacja ponosi na skutek naruszenia jej bezpieczeństwa. Dodatkowo negatywne skutki naruszeń bezpieczeństwa mogą być powiązane nie tylko z celowymi atakami przeciwko zasobom informacyjnym organizacji, ale i ze skutkami błędów i pomyłek czy z następstwami wykorzystana infrastruktury organizacji do działań nielegalnych czy nieetycznych. W takich przypadkach DFR może być pomocna w naprawie reputacji organizacji o tyle, że odpowiednia polityka informacyjna może przekonać interesariuszy, że fachowo i szybko ustalono przyczyny zaistniałego problemu i usunięto je kompetentnie w sposób uniemożliwiający jego powtórzenie się w przyszłości;

- po wtóre, konieczne jest zadbanie o zebranie i o odpowiednią jakość śladów dowodowych, zwłaszcza gdy mowa o „śledztwie wewnętrznym" prowadzonym przez ekspertów prywatnych, zatrudnionych przez stronę, jak i o właściwe przeprowadzenie i udokumentowanie samego procesu badawczego w perspektywie jego użyteczności dla potrzeb postępowań przed sądami zarówno karnymi, jak i cywilnymi.

Warto też zwrócić uwagę, że nawet szybkie i jednoznaczne ustalenie sprawcy czynu zabronionego oraz jego skazanie (i później ewentualna wygrana w sprawie cywilnej) nie gwarantują w żaden sposób naprawienia szkody powstałej na skutek jego działania. Często kradzieże „komputerowe" dokonywane są przez wyspecjalizowane grupy przestępcze, a ukradzione pieniądze transferowane są poprzez system pośredników poza zasięg krajowego systemu prawnego. Ustalenie osoby, która dokonała oszustwa czy włamania, nie pozwala na pokrycie strat – np. wizerunkowych (przy podszywaniu się pod organizację) czy utraconych korzyści (np. związanych z niedostępnością systemów w wypadku ataków DoS), te bowiem mogą przekraczać majątek osądzonego przestępcy, a on sam nie jest skłonny lub nie ma możliwości ujawnienia danych pozwalających na skuteczne ściganie reszty grupy przestępczej na zlecenie której działał. Podobnie beznadziejna może być kwestia w wypadku, gdy organizacja pada ofiarą ataku służb wrogiego państwa. Nieco lepiej może wyglądać kwestia odpowiedzialności odszkodowawczej przy stosunkach pomiędzy podmiotami gospodarczymi, o ile strona (która zawiniła powstaniu szkody, przy odpowiedzialności na zasadzie winy lub może odpowiadać cywilnie na zasadzie ryzyka) dysponuje odpowiednio wysokim majątkiem[24].

Odnośnie do jakości śladów dowodowych, jak wspomniano wcześniej – patrząc z punktu widzenia zarządzania organizacją – można mówić nie tylko o śledztwach

24 Zob. np. J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015, passim.

czy dochodzeniach stricto sensu, realizowanych przez wymiar sprawiedliwości, ale również o działaniach śledczych podejmowanych przez odpowiednie działy w firmie, czy też – na zlecenie organizacji – przez wyspecjalizowane firmy komercyjne. Sytuacje takie, choć z jednej strony dają organizacji prowadzącej działania śledcze większą swobodę, to z drugiej – wymuszają uwzględnienie ograniczeń krajowego systemu prawnego, który raczej nie wspiera samodzielnego prowadzenia takich działań. Jeśli organizacja ma dostarczyć ślady dowodowe, które mają być wykorzystane dla potrzeb postępowania sądowego, należy zwrócić uwagę, że w polskim prawie nie istnieje teoria dowodów formalnych, a wszystkie dowody podlegają zasadzie swobodnej ich oceny przez organ procesowy[25], nie można więc z góry ustalić, nie tylko jaka jest „moc dowodowa" poszczególnych środków dowodowych, ale nawet co może być dowodem (w polskim systemie prawnym katalog środków dowodowych ma charakter otwarty), ani co nie może nim być – w różnych rodzajach postępowań funkcjonują bowiem różne zakazy dowodowe, a nawet różne reguły odnośnie do możliwości wykorzystani dowodów zdobytych „nielegalnie" tj. z naruszeniem prawa. Na przykład w postępowaniu administracyjnym (zob., art. 75. § 1. Kodeksu Postępowania Administracyjnego) obowiązuje zasada, że jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem (analogiczna zasada znajduje się w art. 180 § 1. Ordynacji Podatkowej), natomiast w przepisach postępowania cywilnego nie sformułowano *explicite* zakazu posługiwania się dowodami sprzecznymi z prawem (i istnieją w tej kwestii różne linie orzecznicze); w postępowaniu karnym istnieją zakazy dowodowe, ale – art. 168a KPK dopuszcza wykorzystanie dowodów uzyskanych z naruszeniem prawa, choć w orzecznictwie i w doktrynie nie ma zgody odnośnie do zakresu i możliwości stosowania tego artykułu[26]. W takim stanie rzeczy można zalecić zadbanie o taki sposób zbierania śladów, który od strony technicznej zapewni ich wiarygodność (np. opierając się na zaleceniach normy ISO/IEC 27037). Warto również zapoznać się z narzędziami, zaleceniami i najlepszymi praktykami stosowanymi w innych krajach, szczególnie w USA, w którym teoria dowodów formalnych wymusza ścisłe rygory postępowania ze śladami dowodowymi, należy jednak pamiętać o różnicach pomiędzy systemami prawnymi[27]), a od strony prawnej – dbałość o zgodność z zarówno z przepisami (i to odpowiednimi dla rodzaju planowanego postępowania, często bowiem czyny naruszające bezpieczeństwo

25 Por. np. J. Koredczuk, *Legalna teoria dowodowa i jej wpływ na rozwój inkwizycyjnego procesu karnego*, „Studia z Dziejów Państwa i Prawa Polskiego" 2009, t. 12, s. 85–92, http://bazhum.muzhp.pl/media//files/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12-s85-92/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12-s85-92.pdf (dostęp: 5 stycznia 2025).

26 Zob. np. M. Szmit, *O owocach zatrutego drzewa i kategoryczności opinii biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2019, s. 27–38.

27 Por. np. M. Szmit, *O standardach informatyki śledczej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 355, s. 81–91.

informacji mogą być tak deliktami prawa cywilnego, jak i karnego[28]), jak i najnowszymi trendami orzeczniczymi. Powyższą sytuację należy uwzględnić przy tworzeniu i aktualizacji planów DFR. Wymienione powyżej sugestie, proponowane ramy postępowania czy modele dojrzałości należy traktować w sposób pomocniczy, pamiętając, że mogą dotyczyć innej jurysdykcji albo innej sytuacji prawnej. Jednak gdy mowa o postępowaniach prowadzonych z udziałem organizacji należących do różnych jurysdykcji – należałoby zadbać o zgodność sposobu zbierania śladów z przepisami obowiązującymi w każdej z nich, co jest zadaniem jeszcze trudniejszym.

28 Zob. np. A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010, s. 292.

Zakończenie

Celem niniejszej monografii było rozpoznanie współczesnego rozumienia pojęcia cyfrowej gotowości śledczej i praktycznego podejścia do zarządzania nią przez różne organizacje.

Gotowość śledcza – pierwotnie rozumiana jako własność programów komputerowych czy systemów informatycznych – współcześnie rozpatrywana jest również z zarządczego, a nie tylko technicznego punktu widzenia, jako element organizacyjnego GRC. Nie jest ona niewątpliwie zagadnieniem najważniejszym z punktu widzenia całości zarządzania zgodnością i ryzykiem czy nadzoru zarządczego, niemniej w krajach o rozwiniętej gospodarce rynkowej można zauważyć istniejące zainteresowanie jej budowaniem, zarówno od strony praktycznej, jak i w literaturze naukowej oraz w pracach normalizacyjnych.

Patrząc z punktu widzenia rozwoju metod i narzędzi informatycznych wspomagających zarządzanie GRC, wielość różnych podejść (i wspierających je narzędzi) oraz zakres realizowanych przez nie funkcji świadczy o dojrzałości zarówno samej koncepcji, jak i o stanie rynku. Współcześnie rozwój różnych koncepcji w zarządzaniu przechodzi najpierw przez fazę burzliwego wzrostu, aby – po pewnym czasie współistnienia kilku, kilkunastu podejść o różnej dojrzałości i wspierających je szybko rozwijanych platform informatycznych – dojść do stanu stabilnego z kilkoma liderami rynku oprogramowania wspierającego zarządzenie jakimś aspektem działalności organizacji i sformalizowanymi metodykami obejmującymi większość bądź komplet wymaganych zagadnień. Można dopatrzeć się tu analogii do koncepcji Gartner *hype cycle*[1], choć ten dotyczy oryginalnie technologii IT, a nie koncepcji zarządzania. Zagadnienie cyfrowej gotowości śledczej, będące wąskim i bardzo specyficznym fragmentem GRC, jako koncepcja na świecie obecnie dość dynamicznie się rozwija (choć na pewno nie jest to już wczesny etap rozwoju), natomiast w realiach polskich daje się zaobserwować znaczne opóźnienie (czy może po prostu brak aktywności) w stosunku do rozwiązań amerykańskich czy brytyjskich: nie istnieje polskojęzyczna literatury na ten temat, nie ma też polskich narzędzi informatycznych. Kultura zarządzania bezpieczeństwem informacji

1 C. Edwards, *Waiting for the drop*, „Engineering & Technology" 2025, Vol. 10(4), s. 32–53.

w Polsce koncentruje się, jak można zauważyć, na podejściu reaktywnym, profilaktykę ograniczając do budowania świadomości sytuacyjnej (*cyber situational awareness*) znacznie częściej dotyczącej zapobiegania incydentom przez unikanie niewłaściwych zachowań niż właściwym reakcjom na materializację ryzyka. Jedynie specyficzne organizacje stykające się na co dzień z cyberprzestępczością (np. platformy aukcyjne, firmy telekomunikacyjne, obok oczywiście policji, profesjonalizacja działań której w ostatnich latach jest wyraźnie dostrzegalna, czy firm zajmujących się informatyką śledczą) wypracowały systemowe rozwiązania z zakresu gotowości śledczej, tak że potrafią w sposób zautomatyzowany wygenerować wartościową z punktu widzenia śledztwa informację o incydentach bezpieczeństwa.

Od strony naukowej tematyka ta również nie jest zbyt intensywnie w Polsce rozwijana. Jest to zresztą w pełni zrozumiałe: zagadnienia śledztwa wykorzystującego dowody cyfrowe powiązane są od strony procesowej z kondycją systemu prawnego, a ta jest obecnie w Polsce mocno wątpliwa i trudno spodziewać się, żeby w najbliższym czasie ta sytuacja uległa zmianie. Nie sposób uniknąć również refleksji szerszej: wśród pokazanych przykładowych narzędzi informatycznych i metodyk oraz ram postępowania dotyczących innych aspektów GRC również (poza Narodowymi Standardami Cyberbezpieczeństwa) nie ma w zasadzie rozwiązań krajowych. Polskie firmy w najlepszym razie korzystają z rozwiązań zachodnich, o ile w ogóle zajmują się kompleksowo tą tematyką. Korzystanie z gotowych rozwiązań z bardziej zaawansowanych rozwojowo państw (z ich adaptacją tam, gdzie to konieczne) jest w tej sytuacji działaniem racjonalnym, choć zapewne nie dla wszystkich satysfakcjonującym.

Wykaz skrótów

Wykaz skrótów	
ACSC	Australian Cyber Security Centre
ACTA	Anti-Counterfeiting Trade Agreement
AICPA&CIMA	American Institute of Certified Public Accountants and The Chartered Institute of Management Accountants
ASCDPM	Automated Source Code Data Protection Measure
AVP	Automated Valet Parking
BPMN	Business Process Model and Notation
BPMN4FRSS	BPMN for Forensic-Ready Software Systems
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCE	Common Configuration Enumeration
CCM	Cloud Control Matrix
CCMM	Cybersecurity Capability Maturity Model
CCPA	The California Consumer Privacy Act
CCSMM	The Community Cyber Security Maturity Model
CCSS	Common Configuration Scoring System
CCTV	Closed Circuit Television
CERT	Computer Emergency Readiness Team
CIA	Confidentionality, Integrity, Availability
CIS	The Center for Internet Security
CIS CSC	The Center for Internet Security Critical Security Controls CIS CSC
CIS RAM	The Center for Internet Security Risk Assessment Method
CISQ	The Consortium for Information & Software Quality
CMMI	Capability Maturity Model Integration
CMS	Compliance Management Systems
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPE	Common Platform Enumeration

Wykaz skrótów (cd.)

Wykaz skrótów	
CPMI	Committee on Payments and Market Infrastructures
CPS	Cyber-Physical Systems
CROE	Cyber resilience oversight expectations for financial market infrastructures
CSA	Cloud Security Alliance
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DFR	Digital Forensic Readiness
DIMS	Digital Identity Management Systems
DoD	Department of Defence
DoS	Denial of Service
DRDoS	Distributed Reflected Denial of Service
EBC	Europejski Bank Centralny
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager
EDM	Evaluate-Direct-Monitor
ENISA	European Union Agency for Cybersecurity
ERM	Enterprise Risk Management
ESI	Electronically Stored Information
ETSI	European Telecommunications Standards Institute
EU	European Union
FISMA	Federal Information Security Management Act
FORESTA	Forensic Technical Architecture Framework
FredRAMP	The Federal Risk and Authorization Management Program
FR-ISSRM	Forensic-Ready Information Systems Security Risk Management
GDPR	General Data Protection Regulation
GRC	Governance, Risk Management and Compliance
Hitrust CSF	Hitrust Alliance Inc. Common Security and Privacy Framework
IAB	Interactive Advertising Bureau
IASME	Information Assurance for Small and Medium Enterprises
IDS	Intruder Detection System
IEC	International Electrotechnical Commission

Wykaz skrótów	
IOSCO	International Organization of Securites Commissions
IRAM2	Information Risk Assessment Methodology ver. 2
IRF	Infrastruktura Rynku Finansowego
IRM	Integrated Risk Management
IRMS	Integrated Risk Management Solution
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
KBI	Key Business Indicator
KGI	Key Goal Indicator
KK	Kodeks Karny
KPA	Kodeks Postępowania Administracyjnego
KPI	Key Performance Indicator
KPK	Kodeks Postępowania Karnego
M2M	Machine to Machine
MJA	Multilateral Joint Analysis
MON	Ministerstwo Obrony Narodowej
NASK	Naukowa Akademicka Sieć Komputerowa
NATO	North Atlantic Treaty Organization
NCF	NIST Cybersecurity Framework
NERC-CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NICE	National Initiative for Cybersecurity Education
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standard and Technology
NSC	Narodowy Standard Cyberbezpieczeństwa
OWASP	Open Worldwide Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
PMI	Project Management Institute
PN	Polska Norma
RFC	Request for Comments

Wykaz skrótów (cd.)

Wykaz skrótów	
RFID	Radio-Frequency Identification
RODO	Ogólne Rozporządzenie o Ochronie Danych
SCADA	Supervisory Control And Data Acquisition
SCAP	Security Content Automation Protocol
SCF	Secure Controls Framework
SEM	Structural Equation Model
SLA	Service Level Agreement
SLACFR	Cloud Forensic Readiness Capability for SLA management
SLAPP	Strategic Lawsuit Against Public Participation
SOC 2	Service and Organization Controls 2
SOC 2 TSC	SOC 2 Trust Services Criteria
TDABC	Time Driven Activity-Based Costing
UAV	Unmanned Aerial Vehicle
UE	Unia Europejska
WORM	Write Once Read Many

Bibliografia

Ab R., Nurul H., Glisson W.B., Yang Y., Kim-Kwang R. Choo, *Forensic-by-design framework for cyber-physical cloud systems*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84963728330&doi=10.1109%2fMCC.2016.5&origin=inward&txGid=fb14ac75c450336537505f88c9f2adfa

AICPA&CIMA https://www.aicpa-cima.com/ (dostęp: 5 stycznia 2025).

Akremi A., Sallay H., Rouached M., *An efficient intrusion alerts miner for forensics readiness in high speed networks*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84928032060&doi=10.4018%2fijisp.2014010104&origin=inward&txGid=16d5f875868bc9aef5aa3347187f2824

Al Hanaee E.H.S.S., Awais R., *DF-C²M²: a comprehensive capability maturity model for digital forensics organisations*, PhD thesis, Lancaster University, 2016, https://eprints.lancs.ac.uk/id/eprint/82480/ (dostęp: 5 stycznia 2025).

Albright P., *The Capability Maturity Model and ISO 9000 Standards: Similarities and Differences*, https://www.umsl.edu/~sauterv/analysis/488_f01_papers/albright.htm (dostęp: 5 stycznia 2025).

Almarzooqi A., Jones A., *A framework for assessing the core capabilities of a digital forensic organization*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84990047940&doi=10.1007%2f978-3-319-46279-0_3&origin=inward&txGid=8e92edb86f6a294018de510f7393ef62

Arakis 2.0 Enterprise, https://www.arakis.pl (dostęp: 5 stycznia 2025).

Australian Cyber Security Centre, https://www.cyber.gov.au/ (dostęp: 5 stycznia 2025).

Automated Source Code Data Protection Measure, https://www.omg.org/spec/ASCDPM (dostęp: 5 stycznia 2025).

Bajramovic E., Waedt K., Ciriello A., Gupta D., *Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests*, https://www.scopus.com/record/display.uri?eid=2-s2.0=84994106565-&doi10=1109.2%fIS2C2016.07580754.&origin=inward&txGid-7495c1532fe7b68fd65c114fc7610bae

Baza EUVD, https://euvd.enisa.europa.eu/ (dostęp: 5 stycznia 2025).

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, https://sip.lex.pl/komentarze-i-publikacje/artykuly/pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym-151140647 (dostęp: 5 stycznia 2025).

Błachut J., *Problemy związane z pomiarem przestępczości*, Wolters Kluwer Polska, Kraków 2007.

Brezinski D., Killalea T., *Request for Comments 3227: Guidelines for Evidence Collection and Archiving*, https://www.ietf.org/rfc/rfc3227.txt (dostęp: 5 stycznia 2025).

BSI-200-1 *Managementsysteme für Informationssicherheit (ISMS)*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html (dostęp: 5 stycznia 2025).

Bukowska U., *Normalizacja w kształtowaniu jakości zasobów ludzkich*, [w:] B. Urbaniak (red.), *Efektywność zarządzania zasobami ludzkim*i, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2011, s. 515–527, https://doi.org/10.18778/7525-546-1.36

Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de (dostęp: 5 stycznia 2025).

Canadian Cybersecurity Startup Ecosystem, https://www.serene-risc.ca/en/canadian-cybersecurity-startup-ecosystem (dostęp: 5 stycznia 2025).

CERT Polska Raport 2013, https://cert.pl/uploads/docs/Raport_CP_2013.pdf (dostęp: 5 stycznia 2025).

CERT Polska Raport 2014, https://cert.pl/uploads/docs/Raport_CP_2014.pdf (dostęp: 5 stycznia 2025)

Chernyshev M., Zeadally S., Baig Z., *Healthcare data breaches: Implications for digital forensic readiness*, „Journal of Medical Systems" 2019, Vol. 43(7), https://doi.org/10.1007/s10916-018-1123-2

Chojnowski A., *Informatyka sądowa w praktyce*, Helion, Gliwice 2020.

CIS RAM, https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method (dostęp: 5 stycznia 2025).

Claims I.P., *Digital Forensic Readiness: Proposing a Maturity Assessment Model*, 2015, https://www.goodreads.com/book/show/25333716-digital-forensic-readiness (dostęp: 5 stycznia 2025).

The Consortium for Information & Software Quality, https://www.it-cisq.org/ (dostęp: 5 stycznia 2025).

COSO (Committee of Sponsoring Organizations of the Treadway Commission), https://coso.org (dostęp: 5 stycznia 2025).

CSA, https://cloudsecurityalliance.org (dostęp: 5 stycznia 2025).

Cusack B., Ayaw A.K., *Evidential recovery in a RFID business system*, [w:] *Proceedings of the 8th Australian Digital Forensics Conference*, 2010, s. 46–56.

Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems, Release 1.0, May 2016, https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf (dostęp: 5 stycznia 2025).

Czakon W., Komańda M. (red.), *Interdyscyplinarność w naukach o zarządzaniu*, Katowice 2011.

Dalao K., *Understanding IT security frameworks: Types and examples*, https://www.onetrust.com/blog/security-framework-types (dostęp: 5 stycznia 2025).

Daubner L., Matulevičius R., *Risk-oriented design approach for forensic-ready software systems*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85113244166&doi=10.1145%2f3465481.3470052&origin=inward&txGid=e3121b36fb495736093c417f735eea7e

Daubner L., Matulevičius R., Buhnova B., *A model of qualitative factors in forensic-ready software systems*, [w:] *Lecture Notes in Business Information Processing* 2023, 476 LNBIP, s. 308–324, https://doi.org/10.1007/978-3-031-33080-3_19

Daubner L., Matulevičius R., Buhnova B., Pitner T., *BPMN4FRSS: An BPMN Extension to Support Risk-Based Development of Forensic-Ready Software Systems*, [w:] *Communications in Computer and Information Science* 2023, 1829 CCIS, s. 20–43, https://doi.org/10.1007/978-3-031-36597-3_2

Daubner L., Matulevičius R., Buhnova B., Pitner T., *Business Process Model and Notation for Forensic-Ready Software Systems*, [w:] *International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE – Proceedings* 2022, s. 95–106, https://doi.org/10.5220/0011041000003176

Daubner L., Macak M., Matulevičius R., Buhnova B., Maksović S., Pitner T., *Addressing insider attacks via forensic-ready risk management*, https://www.sciencedirect.com/science/article/pii/S2214212623000182?pes=vor&utm_source=scopus&getft_integrator=scopus (dostęp: 5 stycznia 2025).

De Marco L., Ferrucci F., Kechadi T., *Cloud Forensic readiness model for service level agreements management*, https://www.researchgate.net/profile/Lucia-De-Marco/publication/283106352_A_Cloud_Forensic_readiness_model_for_service_level_agreements_management/links/5637302908ae88cf81bd4f9d/A-Cloud-Forensic-readiness-model-for-service-level-agreements-management.pdf (dostęp: 5 stycznia 2025).

Dobrowolski G., Filipkowski W., *Charakterystyka informatyki kryminalistycznej Polsce w ujęciu teoretycznym*, [w:] V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz (red.), *Kryminalistyka a nowoczesne technologie*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2019, s. 311–332.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1069 z dnia 11 kwietnia 2024 r. w sprawie ochrony osób, które angażują się w debatę publiczną, przed oczywiście bezzasadnymi roszczeniami lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej"), (PE/88/2023/REV/1 Dz. U. L, 2024/1069, 16.4.2024).

Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Wolters Kluwer, Warszawa 2021.

Dziwisz S., *Odpowiedzialność karna za przestępstwa popełnione w cyberprzestrzeni*, [w:] A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013.

EBC, Wymagania nadzorcze w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego, 2018, https://nbp.pl/wp-content/uploads/2022/07/Wymagania-nadzorcze-wz-odpornosci-cybernetycznej.pdf (dostęp: 5 stycznia 2025).

EBIOS RM, https://cyber.gouv.fr/publications/ebios-risk-manager-method (dostęp: 5 stycznia 2025).

Edwards C., *Waiting for the drop,* „Engineering & Technology" 2025, Vol. 10(4), s. 32–53, https://doi.org/10.1049/et.2015.041

e-government act of 2002, https://www.govinfo.gov/link/plaw/107/public/347?link-type=pdf&.pdf (dostęp: 5 stycznia 2025).

Elyas M., Atif A., Maynard S.B., Lonie A., *Digital forensic readiness: Expert perspectives on a theoretical framework*, „Computers and Security" 2015, Vol. 52.

Elyas M., Atif A., Maynard S.B., Lonie A., *Forensic readiness: Is your organisation ready?*, „Digital Forensics Magazine" 2014, Vol. 18, s. 58–62.

Englbrecht L., Meier S., Pernul G., *Towards a capability maturity model for digital forensic readiness*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85090513654&doi=10.1007%2f978-3-030-03898-4_10&origin=inward&txGid=0408dd034dfd57fd83a86390039ed979

ENISA Interoperable EU Risk Management Toolbox, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox (dostęp: 5 stycznia 2025).

ENISA Risk Manegement Inventory, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods (dostęp: 5 stycznia 2025).

FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown, https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive (dostęp: 5 stycznia 2025).

The Federal Risk and Authorization Management Program, https://www.fedramp.gov (dostęp: 5 stycznia 2025).

Forsytek M., *Audyt informatyczny*, Infoaudit, Warszawa 2005.

G2 Porównanie platform GRC, https://www.g2.com/categories/grc-platforms (dostęp: 5 stycznia 2025).

Gartner Glossary, *Enterprise Risk Management*, https://www.gartner.com/en/information-technology/glossary/enterprise-risk-management (dostęp: 5 stycznia 2025).

Gartner Glossary, *Integrated Risk Management*, https://www.gartner.com/en/information-technology/glossary/integrated-risk-management-irm (dostęp: 5 stycznia 2025).

Grant T., van Eijk E., Venter H.S., *Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time*, ICCWS, Boston, MA 2016.

Grobler M., *Digital forensic standards: International progress*, [w:] *Proceedings of the South African Information Security Multi-Conference*, SAISMC 2010, s. 261–271.

Grzenkowicz A., *Lessons Learned odczarowane. Jak zebrać wiedzę po zakończonym projekcie i dobrze ją wykorzystać?*, „Strefa PMI" 2016, nr 12, marzec, https://strefapmi.pl/pobierz/strefa-pmi-12-2016.pdf (dostęp: 5 stycznia 2025).

Haerle A., *O trzech takich, co zhakowali prawdziwy pociąg – a nawet 30 pociągów*, https://zaufanatrzeciastrona.pl/post/o-trzech-takich-co-zhakowali-prawdziwy-pociag-a-nawet -30-pociagow/ (dostęp: 5 stycznia 2025).

Health Insurance Portability and Accountability Act (HIPAA), https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (dostęp: 5 stycznia 2025).

Herman M., Iorga M., Salim A.M., Jackson R.H., Hurst M.R., Leo R.A., Mishra A.K., Landreville N.M., Wang Y., *NIST Cloud Computing Forensic Reference Architecture: SP 800-201*, https://doi.org/10.6028/NIST.SP.800-201

Herman M., Iorga M., Salim A.M., Jackson R.H., Hurst M.R., Leo R., Lee R., Landreville N.M., Mishra A.K., Wang Y., Sardinas R., *NISTIR 8006 NIST Cloud Computing Forensic Science Challenges*, https://doi.org/10.6028/NIST.IR.8006

Hitrust Common Security and Privacy Framework, https://hitrustalliance.net/hitrust-framework (dostęp: 5 stycznia 2025).

IASME Consortium Ltd., https://iasme.co.uk (dostęp: 5 stycznia 2025).

Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted, https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (dostęp: 5 stycznia 2025).

Informator Statystyczny Wymiaru Sprawiedliwości, https://isws.ms.gov.pl (dostęp: 5 stycznia 2025).

Interactive Advertising Bureau, https://www.iab.com/ (dostęp: 5 stycznia 2025).

Interaktywna mapa narodowych strategii cyberbezpieczeństwa, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (dostęp: 5 stycznia 2025).

International Organization of Securites Commissions and the Committee on Payments and Market Infrastructures, https://www.iosco.org/v2/about/?subsection=cpmi_iosco (dostęp: 5 stycznia 2025).

IRAM2 oficjalna strona, https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/ (dostęp: 5 stycznia 2025).

ISACA CMMI Institute, https://cmmiinstitute.com/ (dostęp: 5 stycznia 2025).

ISO 21043-1:2018 Forensic sciences – Part 1: Terms and definitions.

ISO 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002 (second edition).

ISO 37000:2021 Governance of organizations – Guidance.

ISO 37301:2021 – Compliance Management Systems – Requirements with Guidance.

ISO 9004:2000 Quality management systems — Guidelines for performance improvements, Second Ed. ISO 2000-12-15

ISO/IEC 13888-1:2020 Information security – Non-repudiation – Part 1: General.

ISO/IEC 2382:2015 Information technology – Vocabulary.

ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

ISO/IEC 27011:2024 / ITU-T X.1051 – Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations (third edition).

ISO/IEC 27032:2012 ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

ISO/IEC 27032:2023(en) Cybersecurity – Guidelines for Internet security.

ISO/IEC 27043:2016-12 wersja angielska Technika informatyczna -- Techniki bezpieczeństwa -- Pryncypia i procesy w dochodzeniach związanych z incydentami.

ISO/IEC 27102:2019 Information security management – Guidelines for cyber-insurance.

ISO/IEC 30121:2016-12 Technika informatyczna -- Nadzór nad strukturą ryzyka związanego z informatyką śledczą.

ISO/IEC TS 27100:2020 Information technology – Cybersecurity – Overview and concepts.

ISO/TS 27790:2009 Health informatics – Personalized digital health – Digital therapeutics health software systems.

The ISO Survey, 2022, International Organization for Standardization, https://www.iso.org/the-iso-survey.html (dostęp: 5 stycznia 2025).

Kaczmarek A., *Wybrane modele dojrzałości zarządzania bezpieczeństwem informacji – analiza porównawcza*, [w:] *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni*, Akademia Pomorska w Słupsku, Słupsk 2021.

Karpieszczuk W., *Wulgarny wpis o strajkujących kobietach na Facebooku minister Maląg. Znowu włamanie na konto polityka PiS*, https://warszawa.wyborcza.pl/warszawa/7,54420,26610927,wulgarny-wpis-o-strajkujacych-kobietach-na-facebooku-minister.html (dostęp: 5 stycznia 2025).

Kasprzak W.A., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015.

Kebande V., Venter H., *Towards a model for characterizing potential digital evidence in the cloud environment during digital forensic readiness process*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84994187863&origin=inward&txGid=14a04e6a5e372f9de836b71cd5785388

Kędzierski R., *Rusza proces wytoczony przez Newag. Istotna zmiana zarzutów*, https://www.money.pl/gospodarka/rusza-proces-wytoczony-przez-newag-istotna-zmiana-zarzutow-7066384013548128a.html (dostęp: 5 stycznia 2025).

Kim Jaechun, Son Youngjun, Chung Mokdong, *A design of evaluation framework for the assets and insolvency prediction depending on the industry type using data standardization based on the forensic readiness*, https://gvpress.com/journals/IJMUE/vol10_no4/33.pdf (dostęp: 5 stycznia 2025).

KNF. Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, 2013, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf (dostęp: 5 stycznia 2025).

Koch A., Altschaffel R., Kiltz S., Hildebrandt M., Dittmann J., *Exploring the processing of personal data in modern vehicles – A proposal of a testbed for explorative research to achieve transparency for privacy and security*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85057357117&doi=10.1109%2fIMF.2018.00009&origin=inward&txGid=f0aaf355f13b6d977f6892f406d22ba3

Kopalnia kryptowalut w siedzibie NSA. Nowe informacje, https://www.rp.pl/prawo-karne/art39543671-kopalnia-kryptowalut-w-siedzibie-nsa-nowe-informacje (dostęp: 5 stycznia 2025).

Korczowski A., *Zarządzanie ryzykiem w projektach informatycznych teoria i praktyka*, Helion, Gliwice 2010.

Koredczuk J., *Legalna teoria dowodowa i jej wpływ na rozwój inkwizycyjnego procesu karnego*, „Studia z Dziejów Państwa i Prawa Polskiego" 2009, t. 12, s. 85–92, http://bazhum.muzhp.pl/media//files/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12-s85-92/Studia_z_Dziejow_Panstwa_i_Prawa_Polskiego-r2009-t12-s85-92.pdf (dostęp: 5 stycznia 2025).

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, wyd. II, EAS, Warszawa 2017.

Korzeniowski L.F., *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, EAS, Kraków 2008.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Krótki Z., *Polskie leksemy o rdzeniu piecz-/piek- pochodne od piec się*, „Poznańskie Studia Polonistyczne" 2015, Seria Językoznawcza, t. 22 (42), nr 2, s. 69–88.

Kubień K., *Disclosure w prawie angielskim jako narzędzie wyrównania szans stron oraz ustalenia prawdy w postępowaniu cywilnym, cz. I*, „Polski Proces Cywilny" 2015, nr 4, s. 555–582.

Kurowski S., Frings S., *Computational documentation of IT incidents as support for forensic operations*, https://www.scopus.com/record/display.uri?eid=2-s2.0-79960740161&doi=10.1109%2fIMF.2011.18&origin=inward&txGid=336f4aed08d150c60fbe3a59613f354d

Kuziak K., *Zarządzanie ryzykiem prawnym w przedsiębiorstwie*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2008, nr 1196, Finanse, Bankowość, Rachunkowość, z. 6.

Kyaw A., Cusack B., Lutui R., *Digital forensic readiness in wireless medical systems*, [w:] *29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand 2019, s. 1–6, https://doi.org/10.1109/ITNAC46935.2019.9078005

Lang Beebe N., Guynes Clark J., *A hierarchical, objectives-based framework for the digital investigations process*, „Digital Investigation" 2005, Vol. 2, Issue 2, s. 147–167, https://doi.org/10.1016/j.diin.2005.04.002, https://www.sciencedirect.com/science/article/pii/S1742287605000307

Lemonnier R., *Model ubezpieczeń na francuskim rynku finansowym* (rozprawa doktorska, promotor: dr hab. Michał Mariański, prof. UWM), Uniwersytet Warmińsko-Mazurski w Olsztynie, maszynopis, https://wpia.uwm.edu.pl/sites/default/files/u12/model_ubezpieczen_na_francuskim_rynku_finansowym_watermarked.pdf (dostęp: 5 stycznia 2025).

Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2021.

Li J., Bajramovic E., Gao Y., Parekh M., *Graded security forensics readiness of SCADA systems*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85031295459&origin=inward&txGid=302b284ca073668b6bd3e77f2db6825f

Liderman K., O *zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową*, Konferencja „Cyberspace 2009".

Lim Sung Ryel, *Identifying management factors for digital incident responses on Machine-to-Machine services*, https://www.sciencedirect.com/science/article/pii/S1742287615000845?pes=vor&utm_source=scopus&getft_integrator=scopus#kwrds0010

Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, European Association for Security, Kraków 2016.

Makowiec P., *Blokady w pociągach Newagu. Zwrot w sprawie?*, https://cyberdefence24.pl/cyberbezpieczenstwo/blokady-w-pociagach-newagu-zwrot-w-sprawie (dostęp: 5 stycznia 2025).

Makowiec P., *Sprawa blokad w Impulsach. Newag po raz drugi pozywa Dragon Sector i SPS*, https://cyberdefence24.pl/polityka-i-prawo/sprawa-blokad-w-impulsach-newag-po-raz-drugi-pozywa-dragon-sector-i-sps (dostęp: 5 stycznia 2025).

Masvosvere D., Venter H., *A conceptual model for digital forensic readiness in e-supply chains*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84940780779&origin=inward&txGid=a9ed347e74c6456e0f146ebfbe410328 (dostęp: 5 stycznia 2025).

Milionowa strata i pozew. Reakcja NSA po odkryciu kopalni kryptowalut w jego siedzibie, https://tvn24.pl/tvnwarszawa/srodmiescie/warszawa-kopalnia-kryptowalut-w-siedzibie-naczelnego-sadu-administracyjnego-kara-dla-firmy-swiadczacej-uslugi-i-pozew-st7827103 (dostęp: 5 stycznia 2025).

Minister Cyfryzacji zhackowany na Twitterze, https://niebezpieczn0ik.pl/post/minister-cyfryzacji-zhackowany-na-twitterze/ (dostęp: 5 stycznia 2025).

Mitchell S., *GRC360: A framework to help organisations drive principled performance*, „International Journal of Disclosure and Governance" 2007, Vol. 4, s. 279–296, https://doi.org/10.1057/palgrave.jdg.2050066

MITRE CVE, Common Vulnerabilities and Exposures, Browse Vulnerabilities By Date https://www.cvedetails.com/browse-by-date.php (dostęp: 5 stycznia 2025).

Molski M., Łacheta M., *Podręcznik audytora systemów informatycznych*, Helion, Gliwice 2006.

Narodowe Standardy Cyberbezpieczeństwa, https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber (dostęp: 5 stycznia 2025).

Narodowy Standard Cyberbezpieczeństwa NSC 800-61 wer. 1.0. Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego, https://www.gov.pl/attachment/c38e6fd7-c561-4c97-945b-57a72a4a100f (dostęp: 5 stycznia 2025).

National Institute of Standard and Technology Cybersecurity Framework, https://www.nist.gov/cyberframework (dostęp: 5 stycznia 2025).

NBP, Materiał opracowany na podstawie CROE przez Departament Stabilności Finansowej, 2024, https://nbp.pl/wp-content/uploads/2024/10/Materialy_pomocnicze_CROE_lipiec_2024.pdf (dostęp: 5 stycznia 2025).

NERC-CIP, https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx (dostęp: 5 stycznia 2025).

NISPOM (National Industrial Security Program Operating Manual), https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom (dostęp: 5 stycznia 2025).

The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.CSWP.29

NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0, January 16, 2020, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

NIST SP 800-126 Rev. 3 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3, https://doi.org/10.6028/NIST.SP.800-126r3

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide, https://doi.org/10.6028/NIST.SP.800-61r2 (dostęp: 5 stycznia 2025).

NIST SP 800-61 Rev. 3 (Initial Public Draft) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, https://doi.org/10.6028/NIST.SP.800-61r3.ipd

Nugroho H.A., Briliyant O.C., Sunaringtyas S.U., *A Novel Digital Forensic Readiness (DFR) Framework for e-Government*, [w:] *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, Bogor, Indonesia 2023, s. 184–189, https://doi.org/10.1109/ICoCICs58778.2023.10276423

Office of Cybersecurity, Energy Security, and Emergency Response: Cybersecurity Capability Maturity Model (C2M2), version 2.1, June 2022, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf (dostęp: 5 stycznia 2025).

Olabode Gbenga A., *Impact of cyber security implementation in an economy driven by Cyber Physical System (CPS)*, [w:] *Cyber Secure Nigeria 2019 Conference April 9–11, 2019, Governance, Risk Management, and Compliance*, https://spara.ir/assets/en_css/files/GRC.pdf (dostęp: 5 stycznia 2025).

Olber P., *Prawno-kryminalistyczne aspekty zabezpieczenia i pozyskiwania dowodów elektronicznych z chmur obliczeniowych*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2021.

Open Worldwide Application Security Project, https://owasp.org/ (dostęp: 5 stycznia 2025)

Opozda D., *Interdyscyplinarność i intradyscyplinarność w pedagogice rodziny*, „Paedagogia Christiana" 2014, nr 2/34, https://doi.org/10.12775/PCh.2014-029

Pamuła A., Gontar B., Czerwonka P., *Korzyści i problemy implementacji systemów w środowisku chmury obliczeniowej studia przypadków polskich przedsiębiorstw*, „Annales Universitatis Mariae Curie-Skłodowska, Sectio H Oeconomia" 2018, t. 52, s. 127–140, https://doi.org/10.17951/h.2018.52.2.127-140

Parker D.B., *Fighting Computer Crime*, John Wiley & Sons, New York 1988.

PCI DSS – Payment Card Industry Data Security Standard.

The Periodic Table of Cybersecurity, https://www.cbinsights.com/research/periodic-table-cybersecurity (dostęp: 5 stycznia 2025).

Petersen R., Santos D., Smith M.C., Wetzel K.A., Witte G., *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181 Revision 1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf (dostęp: 5 stycznia 2025).

Piśniak M., *Ryzyko w teorii podejmowania decyzji*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 19, s. 116–126.

PN-EN ISO/IEC 27040:2016-12 Technika informatyczna -- Techniki bezpieczeństwa -- Bezpieczeństwo pamięci masowych.

PN-EN ISO/IEC 27041:2016-12 Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem.

PN-EN ISO/IEC 27042:2016-12 Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego.

PN-ISO/IEC 31000:2012 – Zarządzanie ryzykiem – Zasady i wytyczne.

Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006.

Popowska-Taborska H., *Dlaczego pol. bezpieczny nie znaczy 'niebezpieczny'?*, „Acta Universitatis Wratislaviensis" 2014, nr 3578, Slavica Wratislaviensis CLIX.

Quick D., Kim-Kwang R. Choo, *Big forensic data management in heterogeneous distributed systems: quick analysis of multimedia forensic data*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84995755337&doi=10.1002%2fspe.2429&origin=inward&txGid=14179b5dd7bdde49660847ff680618dc

Quinn S., *Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis*, https://www.sciencedirect.com/science/article/pii/S1742287605000873?pes=vor&utm_source=scopus&getft_integrator=scopus

Raport 2003 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2003, https://cert.pl/uploads/docs/Raport_CP_2003.pdf (dostęp: 5 stycznia 2025).

Raport 2004 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2004, https://cert.pl/uploads/docs/Raport_CP_2004.pdf (dostęp: 5 stycznia 2025).

Raport 2005 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2005, https://cert.pl/uploads/docs/Raport_CP_2005.pdf (dostęp: 5 stycznia 2025).

Raport 2006 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2006, https://cert.pl/uploads/docs/Raport_CP_2006.pdf (dostęp: 5 stycznia 2025).

Raport 2007 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2007, https://cert.pl/uploads/docs/Raport_CP_2007.pdf (dostęp: 5 stycznia 2025).

Raport 2008 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2008, https://cert.pl/uploads/docs/Raport_CP_2008.pdf (dostęp: 5 stycznia 2025).

Raport 2009 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2009, https://cert.pl/uploads/docs/Raport_CP_2009.pdf (dostęp: 5 stycznia 2025).

Raport 2010 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, https://cert.pl/uploads/docs/Raport_CP_2010.pdf (dostęp: 5 stycznia 2025).
Raport 2011 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011, https://cert.pl/uploads/docs/Raport_CP_2011.pdf (dostęp: 5 stycznia 2025).
Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, https://cert.pl/uploads/docs/Raport_CP_2012.pdf (dostęp: 5 stycznia 2025).
Raport CERT Orange Polska 2020, https://cert.orange.pl/pobierz-raport/19/1 (dostęp: 5 stycznia 2025).
Raport CERT Orange Polska 2021, https://cert.orange.pl/pobierz-raport/21/1 (dostęp: 5 stycznia 2025).
Raport CERT Orange Polska 2022, https://cert.orange.pl/pobierz-raport/22/1 (dostęp: 5 stycznia 2025).
Raport CERT Orange Polska 2023, https://cert.orange.pl/wp-content/uploads/2024/04/Raport_CERT_Orange_Polska_2023.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku, https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku, https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku, https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku, https://csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku, https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku, https://csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2016roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku, https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku, https://csirt.gov.pl/download/3/191/RaportostaniebezpieczenstwacyberprzestrzeniRPw2018roku.pdf (dostęp: 5 stycznia 2025).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, https://csirt.gov.pl/download/3/199/raportostaniebezpieczenstwacyberprzestrzenirp2019.pdf (dostęp: 5 stycznia 2025).

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku, https://csirt.gov.pl/download/3/201/RaportostaniebezpieczenstwacyberprzestrzeniRPw2020.pdf (dostęp: 5 stycznia 2025).

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku, https://csirt.gov.pl/download/3/204/RaportostaniebezpieczenstwacyberprzestrzeniRPw2021compressed.pdf (dostęp: 5 stycznia 2025).

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku, https://csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf (dostęp: 5 stycznia 2025).

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2015. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2015.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2016. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2016.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2017. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2017.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2018. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2018.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2019. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2019.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2020. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2020.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2021. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (dostęp: 5 stycznia 2025).

Raport roczny z działalności CERT Polska 2022. Krajobraz Bezpieczeństwa polskiego internetu, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 5 stycznia 2025).

Rasmussen M., *The IRM Emperor Has No Clothes*, https://www.linkedin.com/pulse/irm-emperor-gartner-has-clothes-michael-rasmussen (dostęp: 5 stycznia 2025).

Reddy K., Venter H.S., *The architecture of a digital forensic readiness management system*, https://www.scopus.com/inward/record.uri?eid=2-s2.0-84876568707&doi=10.1016%2fj.cose.2012.09.008&partnerID=40&md5=d8f1fb3db7e6646b65deeff11321e0c8

Reddy K., Venter H.S., Olivier M.S., *Using time-driven activity-based costing to manage digital forensic readiness in large organisations*, https://www.scopus.com/record/display.uri?eid=2-s2.0-84874604833&doi=10.1007%2fs10796-011-9333-x&origin=inward&txGid=27224546d0b6c048598bb438a5715a27

Revised Field of Science and Technology (FOS) Classification in The Frascati Manual, OECD, (wersja 2006), https://www.oecd.org/science/inno/38235147.pdf (dostęp: 5 stycznia 2025).

Risk Optics, *IRM, ERM, and GRC: Is There a Difference?*, 22.08.2002, https://reciprocity.com/irm-erm-and-grc-is-there-a-difference (dostęp: 5 stycznia 2025).

Rivera-Ortiz F., *Engineering forensic-ready software systems using automated logging*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85128726859&origin=inward&txGid=8ce4c295955d47a2d946cdd474c86d48

Rivera-Ortiz F., Pasquale L., *Towards automated logging for forensic-ready software systems*, [w:] *Proceedings – 2019 IEEE 27th International Requirements Engineering Conference Workshops*, REW 2019, art. no. 8933538, s. 157–163.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Rot A., *Zastosowanie modeli dojrzałości w zarządzaniu ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2011, nr 159, Informatyka Ekonomiczna, z. 19, https://dbc.wroc.pl/Content/119349/Rot_Zastosowanie_modeli_dojrza%C5%82osci.pdf (dostęp: 5 stycznia 2025).

Rowlingson R., *Ten step process for forensic readiness*, „International Journal of Digital Evidence" 2004, Vol. 2, Issue 3A, Winter, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=40baa64f868d9dc6c5a6111c4d3c757a7879754a

Rozporządzenie Ministra Edukacji i Nauki z dnia 11 października 2022 r. (Dz. U. z 2022 r. poz. 2202).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

Rybicki P., *Normalizacja w obszarze zwalczania cyberprzestępczości*, „Cybersecurity & Cybercrime" 2023, Vol. 1, No. 2, s. 109–130, https://c2.amw.gdynia.pl/article/01.3001.0053.8024/pl (dostęp: 5 stycznia 2025).

Rynek Kolejowy, *Nieuprawnione użycie Radiostop. Pierwsze dane za 2024 rok mało optymistyczne*, https://www.rynek-kolejowy.pl/wiadomosci/nieuprawnione-uzycie-radiostop-120148.html (dostęp: 5 stycznia 2025).

Sachowski J., *Implementing Digital Forensic Readiness*, Elsevier 2016.

Salfati E., Pease M., *NISTIR 8428 Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf (dostęp: 5 stycznia 2025).

Sarbanes-Oxley Act of 2002. Corporate responsibility, https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf (dostęp: 5 stycznia 2025).

Sewastianowicz M., *Grzywną w nieproszonego gościa na Zoom party*, Prawo.pl, 30.05.2020, https://www.prawo.pl/oswiata/grzywna-za-przerywanie-zdalnych-lekcji-wykroczenie,500657.html (dostęp: 5 stycznia 2025).

Skrzynecki R., *Model Coso – czym jest i jakie korzyści przynosi organizacjom?*, https://eventis.pl/artykul/model-coso-czym-jest-i-jakie-korzysci-przynosi-organizacjom-id179 (dostęp: 5 stycznia 2025).

Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E.K., *A survey on the Internet of Things (IoT) Forensics: Challenges, approaches, and open issues*, „IEEE Communications Surveys & Tutorials" 2020, Vol. 22, No. 2, s. 1191–1221.

Strona Office of Cybersecurity, Energy Security, and Emergency Response poświęcona Cybersecurity Capability Maturity Model (C2M2), https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (dostęp: 5 stycznia 2025).

Strona organizacji Centre for Internet Security, https://www.cisecurity.org/ (dostęp: 5 stycznia 2025).

Strona stowarzyszenia ISACA, https://www.isaca.org (dostęp: 5 stycznia 2025).

Sudoł S., *Zarządzanie jako dyscyplina naukowa*, „Przegląd Organizacji" 2016, nr 4(915), https://doi.org/10.33141/po.2016.04

Sułkowski Ł., *Funkcjonalistyczna wizja kultury organizacyjnej w zarządzaniu – dominujący paradygmat i jego krytyka*, „Problemy Zarządzania" 2013, t. 11, nr 4(44).

The Swiss Cybersecurity Start-Up Map, https://cysecmap.swiss/ (dostęp: 5 stycznia 2025).

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010.

Szmit A., Szmit M., *Bezpieczeństwo, cyberbezpieczeństwo, ryzyko w bezpieczeństwie informacji – próba uporządkowania pojęć*, [w:] I. Staniec (red.), *Natura i uwarunkowania ryzyka*, Wydawnictwo Politechniki Łódzkiej, Łódź 2014.

Szmit M., *Biegły informatyk w postępowaniu cywilnym*, „Zeszyty Naukowe Politechniki Łódzkiej" 2011, seria Elektryka, z. 121, nr 1078, s. 487–501.

Szmit M., *Cyberbezpieczeństwo jako zagadnienie interdyscyplinarne*, [w:] M. Chrabkowski, C. Tatarczuk, J. Tomaszewski, W. Wosek (red.), *Bezpieczeństwo w administracji i biznesie jako czynnik europejskiej integracji i rozwoju*, WSAiB, Gdynia 2015, s. 391–413.

Szmit M., *Informatyka śledcza*, [w:] S. Wrycza, J. Maślankowski (red.), *Informatyka ekonomiczna. Teoria i zastosowania*, Wydawnictwo Naukowe PWN, Warszawa 2019, s. 779–791.

Szmit M., *Jeszcze o statusie i odpowiedzialności biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2022, s. 211–223.

Szmit M., *Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence – a basic guide for First Responders*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2015, s. 101–110.

Szmit M., *O owocach zatrutego drzewa i kategoryczności opinii biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2019, s. 27–38.

Szmit M., *O pewnym nowym przepisie i jednym precedensowym wyroku*, „Rocznik Bezpieczeństwa Morskiego" 2021, s. 195–208.

Szmit M., *O standardach informatyki śledczej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 355, s. 81–91.

Szmit M., *O stanowczości opinii biegłego*, „Rocznik Bezpieczeństwa Morskiego" 2022, s. 149–155.

Szmit M., *Przestępczość teleinformatyczna – garść statystyk*, referat wygłoszony na 6 Konferencji Przestępczość Teleinformatyczna XXI w., Gdynia, 23 maja 2024 r.

Szmit M., *Wybrane zagadnienia opiniowania sądowo-informatycznego*, wyd. II rozszerzone i uzupełnione, Polskie Towarzystwo Informatyczne, Warszawa 2014.

Szmit M., *Zjawisko plagiatu programu komputerowego z punktu widzenia biegłego informatyka*, [w:] I. Staniec (red.), *Natura i uwarunkowania ryzyka*, Wydawnictwo Politechniki Łódzkiej, Łódź 2014, s. 338–348.

Szmit M., Politowska I., *Mierniki bezpieczeństwa informatycznego a niektóre przestępstwa komputerowe,* „Automatyka" 2007, t. 11, z. 3, s. 433–451.

Szmit M., Politowska I., *O artykule 267 Kodeksu Karnego oczami biegłego*, „Prawo Mediów Elektronicznych", nr 8, dodatek do „Monitora Prawniczego" 2008, nr 16, s. 34–40.

Szmit M., Szmit A., *Kilka uwag o zarządzaniu podatnościami*, [w:] L. Kiełtyka (red.), *Wykorzystanie technik informacyjnych w zarządzaniu*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023.

Szmit M., Szmit A., *O normatywnych definicjach cyberbezpieczeństwa*, [w:] K. Załęski, P. Polko (red.), *Bezpieczeństwo Polski w drugiej dekadzie XXI wieku*, Akademia WSB, Dąbrowa Górnicza 2019.

Szmit M. (red.), Baworowski A., Kmieciak A., Krejza P., Niemiec A., *Elementy Informatyki Sądowej*, Polskie Towarzystwo Informatyczne, Warszawa 2011.

Szulc M., *Pojęcie governance w piśmiennictwie na temat nauk o zarządzaniu*, „Studia i Prace Kolegium Zarządzania i Finansów" 2019, z. 176, s. 85–110.

Świder J., *Newag pozywa posłankę Paulinę Matysiak. „Naruszanie dobrego imienia"*, https://biznes.interia.pl/gospodarka/news-newag-pozywa-poslanke-pauline-matysiak-naruszanie-dobrego-im,nId,7872162 (dostęp: 5 stycznia 2025).

Tajbakhsh M., Homayounvala E., Shokouhyar S., *Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage*, „International Journal of Electronic Security and Digital Forensics" 2017, Vol. 9(1), s. 62–83, https://doi.org/10.1504/IJESDF.2017.081781

Tan J., *Forensic Readiness*, 2001, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f7e0e2ef046f7755d2f7e6d3a919a922097e912c

TC Cyber roadmap, https://www.etsi.org/cyber-security/tc-cyber-roadmapTC (dostęp: 5 stycznia 2025).

UL Solutions, https://www.ul.com/ (dostęp: 5 stycznia 2025).

University of Texas at San Antionio Center for Infrastructure Assurance and Security: Community Cyber Security Maturity Model, https://cias.utsa.edu/research/maturity-model/ (dostęp: 5 stycznia 2025).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560).

Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (t.j. Dz. U. z 2015 r. poz. 1341, z 2024 r. poz. 1222).

Ustawa z dnia 6 czerwca 1997 r. Kodeks Postępowania Karnego (t.j. Dz. U. z 2024 r. poz. 37).

Ustawa z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483).

Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854, z 2024 r. poz. 1089).

Ustawa z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2024 r. poz. 572).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j Dz. U. 2022. 1233).

Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz. U. z 2020 r. poz. 1086 ze zm.).

Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz. U. z 2020 r. poz. 1086 ze zm.).

Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2017 r. poz. 768).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (t.j. Dz. U. z 2021 r. poz. 386, z 2024 r, poz. 1254).

Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 1997 r. nr 137 poz. 926 z późn. zm.).

Vidal C., Choo K.-K.R., *Cloud security and forensic readiness: The current state of an IaaS provider*, „The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues" 2015, s. 401–428, https://doi.org/10.1016/B978-0-12-801595-7.00018-5

VII Sprawozdanie Okresowe Rzeczypospolitej Polskiej z realizacji postanowień Konwencji w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania obejmujące okres od 15 października 2011 r. do 15 września 2017 r. (ze szczególnym uwzględnieniem okresu od 22 listopada 2014 r. do 15 września 2017 r.)

Wala K., *Ratio legis oraz analiza ustawowych znamion wykroczenia z art. 107a k.w.*, „Prokuratura i Prawo" 2021, nr 3, s. 68–90.

Walczak M., *Czy możliwa jest wiedza interdyscyplinarna?*, „Zagadnienia Naukoznawstwa" 2016, nr 1(207).

Węgrzynowicz A., Ziółkowska K., *Kopalnia kryptowalut w budynku NSA. Miejsce ukrycia komputerów wskazał były pracownik firmy konserwatorskiej*, https://tvn24.pl/najnowsze/warszawa-kopalnia-kryptowalut-odkryta-w-budynku-naczelnego-sadu-administracyjnego-st7429795 (dostęp: 5 stycznia 2025).

Wilk D., *Telefony komórkowe i sieci telekomunikacyjne jako źródło informacji dla organów ścigania*, [w:] V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz (red.), *Kryminalistyka a nowoczesne technologie*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2019, s. 333–356.

Winogrodzki K., *Włamanie na twitterowe konto senatora PiS. Polityk zabrał głos*, https://wiadomosci.wp.pl/wlamanie-na-twitterowe-konto-senatora-pis-polityk-zabral-glos-6612088347249600a (dostęp: 5 stycznia 2025).

Witryna NIST poświęcona Cyber-Physical Systems Framework, https://pages.nist.gov/cpspwg/ (dostęp: 5 stycznia 2025).

Witryna NIST poświęcona Privacy Framework, https://www.nist.gov/privacy-framework (dostęp: 5 stycznia 2025).

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa*, wyd. II, CeDeWu, Warszawa 2019.

Yaacoub J.-P.A., Salman O., Noura H.N., Kaaniche N., Chehab A., Malli M., *Cyber-physical systems security: Limitations, issues and future trends*, „Microprocessors and Microsystems" 2020, Vol. 77, 103201, https://doi.org/10.1016/j.micpro.2020.103201

Yu Y., Barthaud D., Price B., Bandara A., Zisman A., Nuseibeh B., *LiveBox: A Self-adaptive forensic-ready service for drones*, https://www.scopus.com/record/display.uri?eid=2-s2.0-85077749703&doi=10.1109%2fACCESS.2019.2942033&origin=inward&txGid=8bcdb5e12efde1d6c9c17ec82621b359

Zalecenie Parlamentu Europejskiego z dnia 15 czerwca 2023 r. dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego (2023/2500(RSP)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_PL.html (dostęp: 5 stycznia 2025).

Załącznik C do Raportu z wykonywania wyroków Europejskiego Trybunału Praw Człowieka przez Polskę za 2020 r. Zarządzenie Ministra Sprawiedliwości z dnia 19 stycznia 2021 r. w sprawie wzorów formularzy statystycznych w sądach powszechnych i wojskowych (Dz. U. M. S. poz. 4).

Zdjęcia kobiety w bieliźnie. Włamanie na twitterowe konto Marka Suskiego, https://www.polsatnews.pl/wiadomosc/2021-01-18/zdjecia-kobiety-w-bieliznie-wlamanie-na-twitterowe-konto-marka-suskiego/ (dostęp: 5 stycznia 2025).

https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63633,Wytwarzanie-programu-komputerowego-do-popelnienia-przestepstwa-art-269b.html (dostęp: 5 stycznia 2025).

Spis tabel

Spis rysunków

Zarządzanie bezpieczeństwem informacji we współczesnych organizacjach obejmuje zapobieganie naruszeniom bezpieczeństwa, ich wykrywanie i reakcję. Ta ostatnia – poza usunięciem negatywnych skutków oraz zapewnieniem bezpiecznego działania na przyszłość – powinna również obejmować ustalenie mechanizmu i szczegółów incydentu, w tym postępowanie dowodowe wykorzystujące ślady cyfrowe. Aby tak pojmowane postępowanie dowodowe nie miało charakteru działań *ad hoc*, wskazane jest proaktywne przygotowanie organizacji na wystąpienie takiej sytuacji, czyli zbudowanie jej cyfrowej gotowości śledczej (ang. Digital Forensic Readiness, DFR). Prezentowana monografia ma na celu rozpoznanie współczesnego rozumienia tego pojęcia i praktycznego podejścia do zarządzania gotowością śledczą przez różne organizacje.

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

wydawnictwo.uni.lodz.pl
ksiegarnia@uni.lodz.pl
(42) 665 58 63

Książka dostępna również jako e-book

ISBN 978-83-8331-901-8