

Joanna Antczak

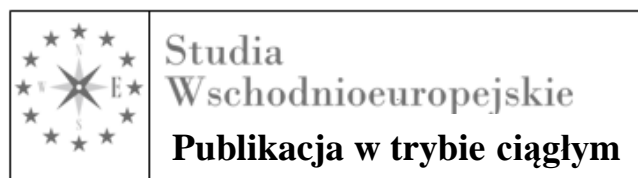
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego

Ewa Dębicka

Instytut Transportu Samochodowego

Joanna Nowakowska-Grunt

Politechnika Częstochowska



**Wybrane aspekty zarządzania bezpieczeństwem informacji
w organizacjach w świetle współczesnych wyzwań gospodarki.
Przykład przedsiębiorstw działających w Polsce**

Wprowadzenie

Zapewnienie bezpieczeństwa informacji w organizacji staje się coraz trudniejszym wyzwaniem. Należy stosować strategię, aby ukierunkować działania w zakresie bezpieczeństwa i jak najlepiej wykorzystać ograniczone zasoby w tym środowisku. Organizacja musi wdrożyć strategię bezpieczeństwa informacji poprzez ustanowienie kompleksowych ram, które umożliwiają rozwój, instytucjonalizację, ocenę i doskonalenie programu bezpieczeństwa informacji w celu uwzględnienia ryzyka związanego z zapewnieniem bezpieczeństwa. Strategia bezpieczeństwa informacji, w szczególności musi wspierać ogólne plany strategiczne organizacji¹.

Obecnie, jednym z największych wyzwań przed jakim stoją organizacje to zapewnienie cyberbezpieczeństwa. Jest ono rozumiane jako zarządzanie systemem informacyjnym przez osoby lub organizacje w celu zarządzania bezpieczeństwem użytkowników końcowych z

¹ D. Ghelani, *Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review*, "American Journal of Science, Engineering and Technology", Vol. 3, No. 6, 2022, s. 12-13.

zachowaniem bezpieczeństwa, na podstawie osobistych postrzeganych zachowań w kierunku potencjalnego naruszenia bezpieczeństwa w środowisku pracy i poza nim. Należy pamiętać, że bezpieczeństwo informacji nie może być osiągnięte poprzez samą technologię. Obejmuje ono również stosowanie procedur, polityki i ludzi. Ponadto trzeba zidentyfikować, kim są atakujący, jakie są ich inspiracje, gdzie znajdują się podatności i jak zabezpieczone są systemy².

W miarę jak świat staje się coraz bardziej zdigitalizowany i zarazem połączony, wzrastają wraz z nim zagrożenia cyberatakami. Organizacje potrzebują odpornych i zarazem bezpiecznych systemów oraz procesów, aby je chronić. Jednym ze sposobów zapobiegania jest implementacja międzynarodowych standardów w tym przede wszystkim wymagań norm z rodziny ISO 27000.

Zapewnienie bezpieczeństwa informacji w organizacji jest procesem złożonym. Wymaga świadomości zarządzających ryzykiem w obszarze bezpieczeństwa informacji przede wszystkim w kontekście dynamicznie pojawiających się nowych zagrożeń i wyzwań. Jednym ze skutecznych sposobów wzmocnienia odporności organizacji, a tym samym budowaniu bezpieczeństwa informacji, jest działanie według międzynarodowych standardów.

Celem niniejszej pracy jest odpowiedź na następujące pytania badawcze:

- Jakie są najważniejsze międzynarodowe standardy dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa?
- Jaka jest skala korzystania z norm ISO w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa w różnych krajach?
- Jaka jest skala korzystania z norm ISO w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa w Polsce?

W realizacji celu pracy punktem wyjścia była krótka charakterystyka rodziny norm ISO/IEC 27000, które mają międzynarodowy zasięg oraz zastosowanie do organizacji wszelkiego typu. Następnie w celu analizy rzeczywistej sytuacji rynkowej, przeanalizowane zostały raporty International Organization for Standardization w zakresie certyfikacji na potwierdzenie spełnienia wymagań międzynarodowej normy dotyczącej systemu zarządzania

² W. H. Tekleselase, *Emerging Cyber Security Threats in Organization*, "International Journal of Information and Communication Sciences". Vol. 5, No. 2, 2020, s. 12.

bezpieczeństwem informacji w zakresie globalnym, a ostatnim etapem badania jest analiza badań ankietowych zrealizowanych w przedsiębiorstwach działających na obszarze Polski.

W artykule wykorzystane zostały zarówno metody ilościowe jak i jakościowe: metody ankietowe, metody analityczne, metoda dedukcji jako forma uogólniająca i wnioskowa, analiza literatury.

W niniejszym artykule zaprezentowano część badań ankietowych dotyczących stosowania certyfikatów ISO/IEC 27001 oraz ISO/IEC 27032 w 250 przedsiębiorstwach działających na terytorium Polski. Największą próbą badawczą stanowiły przedsiębiorstwa z branży TSL³ (40%). Badania zostały zrealizowane na przestrzeni dwóch lat (listopad 2020 r. listopad 2022 r.). Badanie sondażowe metodą ankietową autorstwa jednej z Auterek niniejszego opracowania artykułu z wykorzystaniem wywiadu telefonicznego przeprowadziło na zlecenie Instytutem Badawczym IPC Sp. z o.o. z siedzibą we Wrocławiu. Badanie zostało zrealizowane metodą wywiadów telefonicznych wśród osób odpowiedzialnych za cyberbezpieczeństwo w firmach. Celem badań była analiza budowy systemu cyberbezpieczeństwa w przedsiębiorstwach.

Zarządzanie bezpieczeństwem informacji w świetle badań literaturowych

Analiza literatury przedmiotu wskazuje na szeroki aspekt problemów, które wiążą się z cyberbezpieczeństwem. Jak wskazuje wielu autorów, w dzisiejszych czasach bezpieczeństwo informacji jest ważnym problemem dla wszystkich przedsiębiorstw, gdyż działają one na globalnym rynku, są w dużym stopniu uzależnione od technologii informatycznych i są w pełni obecne w Internecie⁴.

Zarządzanie bezpieczeństwem informacji jest kluczowym wyzwaniem dla firm, ponieważ mają one na celu zapobieganie narażeniu na zagrożenia bezpieczeństwa i prywatności systemów informatycznych i infrastruktury sieciowej. Dlatego organizacje podejmują działania, aby ich przedsiębiorstwa, procesy, polityki i zachowania pracowników pozwalają im na zminimalizowanie i złagodzenie niektórych ryzyk, które są związane z ich systemami

³ C. Mańkowski TSL definiuje jako „działalność gospodarcza polegająca na oferowaniu i realizacji na rynku, a więc w stosunku do innych podmiotów, usług: przemieszczania osób i dóbr materialnych (transport), organizacji przewozu ładunków (spedycja) oraz kompleksowego zarządzania i realizacji wszelkich procesów przepływu, włącznie z transportem, spedycją, magazynowaniem (logistyka).

⁴ G. Stoneburner, A. Goguen, A. Feringa, *Risk management guide for information technology systems*. Nist Spec. Publ. 2002, p. 800–830; S. Bell, *Cybersecurity is not just a 'big business' issue*. Gov. Dir. 2017, 69, 536–539; W. Stallings, *Cryptography and Network Security*, 4th ed.; Pearson Education India: Delhi, India, 2006.

informacyjnymi i infrastrukturą IT⁵. Główne filary zarządzania bezpieczeństwem informacji to poufność, integralność i dostępność, stanowią one model projektowy służący do określenia polityki organizacji w zakresie bezpieczeństwa informacji. Ponieważ dane służą do wielu operacji wewnątrz organizacji, ich poufność jest głównym problemem, wymagającym zastosowania zestawu procedur i zasad wewnątrzorganizacyjnych, określających kto i w jakim zakresie ma dostęp do danych i informacji. Integralność i dostępność wymagają wiarygodności i dokładności danych, do których dostęp mają upoważnione osoby. Stąd, standardy i ramy bezpieczeństwa informacji opierają się na wdrożeniu polityki i kontroli, aby zarządzać bezpieczeństwem i ryzykiem na poziomie organizacyjnym. Najlepsze praktyki stosowane w organizacji mają kluczowe znaczenie i stanowią pierwszą barierę chroniącą przedsiębiorstwa w zakresie bezpieczeństwa informacji. Definicja polityki bezpieczeństwa cybernetycznego powinna być pierwszym wyzwaniem dla menedżerów, aby chronić dane organizacyjne i zdefiniować procedury, których należy przestrzegać. Ich celem jest zdefiniowanie poziomu ochrony, aby zapewnić, że dane organizacyjne i sieci są bezpieczne.

Przedsiębiorstwa, w tym także przedsiębiorstwa z branży TSL, mogą jednak nie być w stanie pozwolić sobie na wdrożenie złożonych i często kosztownych, ale skutecznych procedur bezpieczeństwa, co powoduje, że będą one bardziej narażone na cyberataki, a w konsekwencji będą miały mniej kontroli wewnątrzorganizacyjnej. Przedsiębiorstwa branży TSL od kilku już lat stają się coraz częstszym celem cyberataków. Jednym z najgłośniejszych takich incydentów był atak wirusa Petya przeprowadzony w 2017 roku, który uderzył w duńską firmę transportową Maersk – największego na świecie operatora morskiego transportu kontenerowego. Systemy informatyczne firmy przez kilka dni były sparaliżowane za sprawą złośliwego oprogramowania typu ransomware, blokującego systemy firmy, a jednocześnie pojawił się komunikat o żądaniu okupu. W tym czasie operator musiał wyłączyć część swoich systemów zarządzania flotą i przyjmowania nowych zleceń. Na szczęście nie doszło do kradzieży danych. Mimo to atak sparaliżował działanie firmy, spowodował znaczne straty finansowe (kwartalny zysk operatora spadł o 300 mln dolarów) oraz spowodował znaczne zakłócenia w globalnym łańcuchu dostaw. To i kilka innych podobnych wydarzeń związanych z naruszeniem cyberbezpieczeństwa w dużych przedsiębiorstwach zajmujących się transportem, spedycją i logistyką sprawiły, że w 2019 roku firmy Thales i Verint umieściły branżę TSL na czwartym

⁵ W. Stallings, *Cryptography...op. cit*; S.G. Govender, E. Kritzinger, M. Loock, *A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture*, 1226. Cham: Springer; 2020.

miejscu zestawienia najczęściej atakowanych przez cyberprzestępców sektorów⁶. Duża część tych ataków przeprowadzana jest na firmy działające w Europie Środkowo-Wschodniej, w tym w Polsce. Jest to przede wszystkim spowodowane faktem, że przedsiębiorstwa z sektora TSL w ciągu ostatnich lat przeszły szybką transformację cyfrową. Zarządzanie flotą czy ładunkami, optymalizacja tras przejazdu i obsługa zamówień coraz częściej odbywają się przy użyciu systemów informatycznych. Stało się to standardem branżowym, zwłaszcza w przypadku dużych operatorów transportowych, z gęstą siecią powiązań na rynku. Natomiast nie nadąża za tym odpowiedni poziom cyberzabezpieczeń w zakresie posiadanych technologii. W zależności od firmy, może się on znacząco różnić. Problemem może być także fakt, że sektor TSL charakteryzuje się bardzo rozbudowaną siecią powiązań w łańcuchu dostaw, co powoduje, że cyberatak wymierzony w jednego z operatorów automatycznie paraliżuje działanie współpracujących z nim dostawców i partnerów. Głównymi powodami, dla których sektor TSL jest podatny na cyberataki, jest cały wachlarz cech charakterystycznych dla tego sektora: występowanie luk w systemach zabezpieczeń, brak jednolitych standardów ochrony przed cyberatakami, a przede wszystkim posiadanie wielu interesujących, cennych danych na temat ładunków. Tego rodzaju informacje są atrakcyjne dla cyberprzestępców, którzy chcą wykorzystać pozyskane w ten sposób dane np. do działalności przemytniczej lub terrorystycznej. A także w celu destabilizacji bądź zerwania łańcuchów dostaw bądź do wygenerowania znaczących strat finansowych w konkretnych przedsiębiorstwach (Mraković 2019)⁷.

Rodzina międzynarodowych norm standaryzująca zarządzanie bezpieczeństwem informacji ISO/IEC 27000

Powszechnie w literaturze brak jest akceptowanego pojęcia informacji, można uznać, że jest to „termin złożony, interdyscyplinarny, definiowany odmiennie w różnych naukach, niemający jednoznacznej, powszechnej definicji”⁸. Biorąc pod uwagę podejście cybernetyki i zarazem teorii informacji, informacja jest definiowana jako „zbiór faktów, zdarzeń cech itp. określonych obiektów (rzeczy, procesów systemów) zawarty w wiadomości (komunikacie), tak

⁶ <https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who> (dostęp 27.04.2023).

⁷ I. Mraković, R. Vojinović, Maritime Cyber Security Analysis – How to Reduce Threats?, “Transactions on Maritime Science”, 2019 08 (01), s. 132-139, <https://doi.org/10.7225/toms.v08.n01.013> (dostęp 27.04.2023).

⁸ C. Banasiński (red.), Cyberbezpieczeństwo zarys wykładu, Wolters Kluwer, Warszawa 2018, s. 21.

ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne”⁹. Zgodnie z Polską Normą PN-ISO/IEC 2382-1:1996, „informacja to wiedza dotycząca obiektów takich jak fakty, zdarzenia, przedmioty, procesy lub idee zawierające koncepcje, która w określonym kontekście ma określone znaczenie”. Zgodnie z normą od informacji należy odróżnić termin dane, które są definiowane jako „reprezentacja informacji mająca interpretację, właściwą do komunikowania się, interpretacji lub przetwarzania”.

Brytyjska jednostka normalizacyjna (ang. *British Standards Institution*, BSI) w 1995 r. jako pierwsza opublikowała normy zawierające wytyczne związane z organizacją procesu zarządzania bezpieczeństwem IT (BS 7799-1). Cztery lata później została wydana Komplementarna norma, określająca wymagania, BS 7799-2:1999.

W obydwu normach została opisana procedura ustanowienia wewnątrz organizacji tzw. systemu zarządzania bezpieczeństwem informacji (SZBI), ang. *Information Security Management System* (ISMS) (rysunek 1).



Rysunek 1. Istota Systemu Zarządzania Bezpieczeństwem Informacji

Źródło: J. Antczak¹⁰.

⁹ P. Sienkiewicz, *10 wykładów*, AON, Warszawa 2005, s. 62.

¹⁰ J. Antczak, *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*, ASzWoj, Warszawa 2021, s. 35.

Międzynarodowy Komitet Standaryzacyjny na podstawie o BS 7799 opracował własne normy międzynarodowe, które opisują wytyczne oraz wymagania dla systemów zarządzania bezpieczeństwem informacji. Norma ISO/IEC 27000 (tabela 1), obejmuje przegląd systemów zarządzania bezpieczeństwem informacji, terminy oraz definicje powszechnie stosowane w rodzinie norm SZBI. Norma ISO/IEC 27002 zawiera wytyczne dla budowy ISMS, natomiast ISO/IEC 27001 definiuje wymagania niezbędne do uzyskania certyfikatu wydawanego przez niezależne jednostki certyfikujące jako obiektywnego dowodu na spełnienie tego międzynarodowego standardu.

ISO/IEC 27001 to najbardziej znana na świecie norma dotycząca systemów zarządzania bezpieczeństwem informacji (ISMS) i ich wymagań. Dodatkowe najlepsze praktyki w zakresie ochrony informacji i cyberodporności są objęte przez kilkanaście norm z rodziny ISO/IEC 27000 (tabela 1). Razem umożliwiają one organizacjom wszystkich sektorów i rozmiarów zarządzanie bezpieczeństwem aktywów takich jak informacje finansowe, własność intelektualna, dane pracowników i informacje powierzone przez strony trzecie.

Tabela 1. Wybrane normy z serii ISO/ IEC 27000 Technika informatyczna. Techniki bezpieczeństwa (Information technology – Security techniques)

Normy zawierające wymagania	Normy opisujące ogólne wytyczne	Normy zawierające wytyczne dla poszczególnych sektorów
ISO/ IEC 27001 Informatyka - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania	ISO/IEC 27002 Praktyczne zasady zabezpieczania informacji (wykaz zabezpieczeń)	ISO/IEC 27011 Technologia informacyjna - Techniki bezpieczeństwa - Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji oparty na ISO / IEC 27002 dla organizacji telekomunikacyjnych
ISO/ IEC 27006 Technika informatyczna - Techniki bezpieczeństwa - Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji	ISO/ IEC 27003 Przewodnik implementacji ISO/ IEC 27004 Monitorowanie, pomiary, analiza i ocena ISO/ IEC 27005 Zarządzanie ryzykiem w bezpieczeństwie informacji (norma zawiera m.in. katalog zagrożeń,	ISO/IEC 27015 Technologia informacyjna - Techniki bezpieczeństwa - Wytyczne dotyczące zarządzania bezpieczeństwem informacji w usługach finansowych

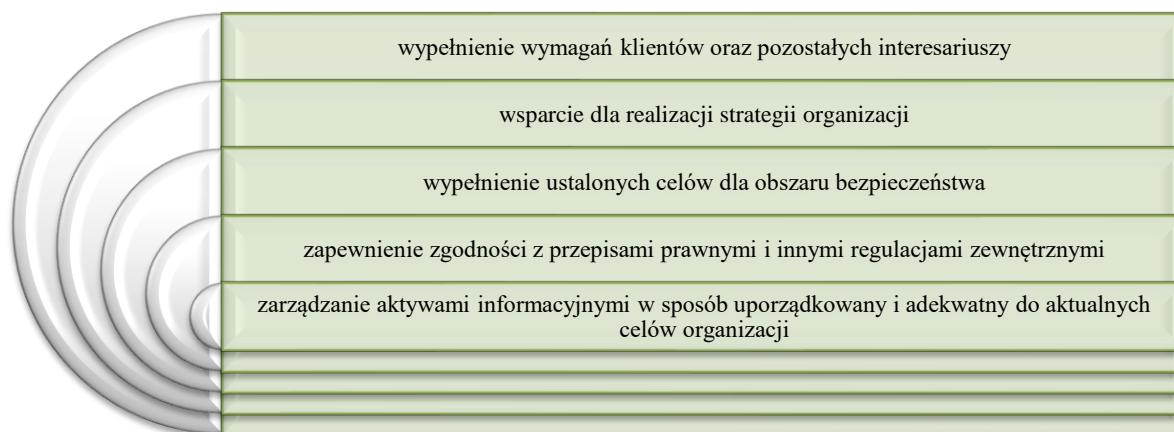
	<p>które należy wziąć pod uwagę przy analizie ryzyka)</p> <p>ISO/IEC 27007</p> <p>Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Wytyczne dotyczące audytu systemów zarządzania bezpieczeństwem informacji</p> <p>ISO/IEC 27013</p> <p>Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dotyczące zintegrowanego wdrażania ISO / IEC 27001 i ISO / IEC 20000-1</p> <p>ISO/IEC 27014</p> <p>Technologia informacyjna - Techniki bezpieczeństwa - Zarządzanie bezpieczeństwem informacji</p>	<p>ISO/IEC 27017</p> <p>Technologia informacyjna - Techniki bezpieczeństwa - Kodeks postępowania dotyczący kontroli bezpieczeństwa informacji w oparciu o ISO / IEC 27002 dla usług w chmurze</p> <p>ISO/IEC 27019</p> <p>Technologia informacyjna - Techniki bezpieczeństwa - Mechanizmy kontroli bezpieczeństwa informacji w przemyśle energetycznym</p> <p>ISO/IEC 27799</p> <p>Informatyka w ochronie <i>zdrowia</i> - Zarządzanie bezpieczeństwem informacji w zdrowiu z wykorzystaniem normy ISO / IEC 27002</p>
<p>Normy zintegrowane z rodziną norm ISO/IEC 27000:</p> <p>ISO/IEC 29134</p> <p>Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dotyczące oceny skutków dla prywatności</p> <p>ISO/IEC 27032</p> <p>Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dotyczące cyberbezpieczeństwa</p>		

Źródło: J. Antczak¹¹.

¹¹ J. Antczak, *Zarządzanie...op.*, cit., s. 37.

Liderzy tacy jak Microsoft, Apple, Google, Intel i IBM, stosują normę ISO/IEC 27001. Dzięki rosnącej globalnej popularności i obecności w tysiącach obiektów na całym świecie, norma ISO/IEC 27001 stała się de facto standardem dla systemów zarządzania bezpieczeństwem informacji. Aby chronić swoje krytyczne zasoby danych przed cyfrowymi zagrożeniami i podatnościami, organizacje muszą przyjąć postawę cyberodporną. Cyberodporność musi być integralną częścią nie tylko systemów technicznych, ale także zespołów, kultury organizacyjnej i codziennych operacji. Według raportu World Economic Forum (WEF) Global Security Outlook 2023, 91% respondentów stwierdziło, że ich zdaniem daleko idące i katastrofalne zdarzenie cybernetyczne jest "co najmniej nieco prawdopodobne w ciągu najbliższych dwóch lat". Firmy na całym świecie zareagowały na presję, wdrażając ISO/IEC 27001, najbardziej znaną na świecie normę dotyczącą systemów zarządzania bezpieczeństwem informacji (ISMS). Jest to udokumentowany zestaw polityk, procedur, procesów i systemów, które zarządzają ryzykiem utraty danych w wyniku cyberataków, włamań, wycieków danych lub kradzieży.

Norma ISO/IEC 27000 zawiera przegląd systemów zarządzania bezpieczeństwem informacji oraz terminy i definicje powszechnie stosowane w rodzinie standardów Information Security Management System (ISMS). Rysunek 2 ilustruje główne korzyści z wdrożenia normy ISO/IEC 27000.



Rysunek 2. korzyści z wdrożenia normy ISO/IEC 27000

Źródło: opracowanie własne na podstawie PN-EN ISO/IEC 27000:2020-07

Do fundamentalnych zasad, na których oparte jest wdrożenie normy ISO/IEC 27000 w jednostce organizacyjnej niezależnie od jej wielkości oraz branży w jakiej działa należą (PN-EN ISO/IEC 27000:2020-07):

- Potrzeba budowania świadomości w zakresie potrzeb dotyczących bezpieczeństwa informacji,
- zapewnienie odpowiedniego zaangażowania kierownictwa, które powinno wykazywać przywództwo w odniesieniu do aspektów bezpieczeństwa informacji oraz uwzględnienie oczekiwań interesariuszy,
- przypisanie ról i odpowiedzialności za zapewnienie bezpieczeństwa informacji,
- dobór zabezpieczeń w odniesieniu do zidentyfikowanych poziomów ryzyka,
- uznanie bezpieczeństwa jako istotnego elementu zarządzania całej organizacji w tym jej systemami i sieciami,
- wdrożenie mechanizmów zapobiegania i wykrywania incydentów bezpieczeństwa.

Norma ISO/IEC 27002 *Praktyczne zasady zabezpieczania informacji (wykaz zabezpieczeń)* zawiera wytyczne dla budowy ISMS, natomiast ISO/IEC 27001 *Informatyka - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania niezbędne do zbudowania tego systemu.*

Norma ISO/IEC 27001 określa wymagania i zarazem zasady inicjowania, wdrażania, utrzymania i poprawy zarządzania bezpieczeństwem informacji w organizacji. Zawiera także najlepsze praktyki celów stosowania zabezpieczeń w obszarach zarządzania bezpieczeństwem informacji. Zakres normy ISO/IEC 27001 dotyczy wsparcia w ulepszaniu mechanizmów cyberbezpieczeństwa przy jednoczesnym wskazaniu powiązań pomiędzy cyberbezpieczeństwem a innymi płaszczyznami: bezpieczeństwo informacji, systemów, sieci oraz infrastruktury krytycznej, które mają wpływ na bezpieczeństwo IT. Z zakresu wyłączono płaszczyzny: ochrony cybernetycznej i cyberprzestępstwa.

W październiku 2022 r. opublikowano kolejną wersję normy ISO/IEC 27001 będącą odpowiedzią na globalne wyzwania związane z bezpieczeństwem informacji szczególnie przetwarzanych w systemach teleinformatycznych. Opracowane na arenie międzynarodowej wymagania skoncentrowane są na przyniesieniu korzyści organizacjom, poprzez wskazanie

zabezpieczeń wszystkich form informacji, dla zapewnienia ich integralności, poufności i dostępności. Okres przejściowy na wdrożenie nowego wydania normy ISO27001 wynosi 36 m-cy. Ta popularna norma jest odpowiedzią na potrzeby wszystkich organizacji, które chcą chronić swoje aktywa informacyjne przed coraz częstszymi i wyrafinowanymi cyberatakami. Jej popularność wynika z faktu, że nie tylko duże organizacje, ale coraz częściej małe firmy są celem hackerów. Badanie przeprowadzone przez PwC na zlecenie brytyjskiego Departamentu Biznesu, Innowacji i Umiejętności wykazało, że małe firmy doświadczają obecnie poziomów incydentów wcześniej obserwowanych jedynie w większych organizacjach, a 87% małych organizacji zgłosiło naruszenie bezpieczeństwa w ciągu 2022 roku¹².

Kolejnym czynnikiem jest stale rosnący poziom wykorzystywania nowych technologii tak w życiu prywatnym jak i zawodowym. Aktywni użytkownicy telefonów komórkowych, portali społecznościowych, smartfonów i laptopów powinni dbać o utrzymanie poziomu bezpieczeństwa przetwarzanych tam informacji. Reasumując, nowe wydanie normy ISO 27001 to szereg ulepszeń w zakresie propozycji zabezpieczeń opisanych w załączniku A, co gwarantuje, że dokument ten pozostaje aktualny i adekwatny do bieżących wyzwań i zagrożeń. Nie bez znaczenia jest także fakt, że standard ten jest zgodny ze strukturą wysokiego poziomu stosowaną we wszystkich standardach systemów zarządzania, co znacznie ułatwia integrację z innymi systemami zarządzania. Tak, jak wskazano nowe wydanie normy to przede wszystkim odpowiedź na skalę zagrożeń z grupy cyberataków. Obecnie bowiem sferą walki informacyjnej jest cyberprzestrzeń, ponieważ *ex definitione* służy do przekazywania, przetwarzania i przechowywania informacji. Cyberprzestrzeń to globalna przestrzeń elektromagnetyczna dostępna za pośrednictwem technologii elektronicznej, użytkowana przez odpowiednią modulację energii elektromagnetycznej. Istotą cyberprzestrzeni jest posługiwanie się informacją w postaci zdigitalizowanej¹³.

Cyberbezpieczeństwo i cyberprzestrzeń są ściśle ze sobą powiązane i zarazem nieodłącznie związane z rewolucją ostatnich lat jaką jest dostęp do informacji, będący skutkiem rewolucji informatycznej.

Najczęściej cyberbezpieczeństwo definiuje się z punktu widzenia zapobiegania uszkodzeniom, ochronie oraz w perspektywie przywracania zdolności do poprawnego

¹² www.iso.org (dostęp 18.04.2023).

¹³ T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016, s. 172.

funkcjonowania komputerów, systemów łączności elektronicznej czy też usług komunikacji odbywających się w cyberprzestrzeni. Cyberbezpieczeństwo to również ochrona informacji zawartych w przestrzeni komunikacji elektronicznej, w celu zapewnienia poufności z jednoczesnym uwierzytelnieniem osób do tego upoważnionych¹⁴. Istota zapewnienia bezpieczeństwa informacji przede wszystkim w cyberprzestrzeni została oddana w nowym układzie zabezpieczeń w Załączniku A do normy ISO 27001. Zabezpieczenia te zostały podzielone na 4 grupy tematyczne, tj.:

- zabezpieczenia organizacyjne,
- zabezpieczenia związane z zasobami ludzkimi,
- zabezpieczenia fizyczne,
- zabezpieczenia technologiczne.

W grupie zabezpieczenia organizacyjne zidentyfikowano łącznie 37 zabezpieczeń, w tym 34 zabezpieczenia istniały we wcześniejszym wydaniu normy, a 3 są nowe. Wśród nowych zabezpieczeń należy wymienić: postępowanie z informacjami w celu uzyskania informacji o zagrożeniach, bezpieczeństwo informacji w usłudze chmury, gotowość teleinformatyczną do zapewnienia ciągłości działania organizacji. W zakresie zabezpieczeń związanych z zasobami ludzkimi pozostawiono 8 dotychczasowych zabezpieczeń i nie wprowadzono żadnych nowych wymagań. Podobnie jest w obszarze zabezpieczeń fizycznych, gdzie łącznie jest 14 zabezpieczeń, 13 istniejących i dodano jedno nowe polegające na monitorowaniu bezpieczeństwa fizycznego. Największe zmiany odnotowano w grupie zabezpieczeń technologicznych. Znajduje się tam łącznie 34 zabezpieczenia, w tym 27 istniejących i 7 nowych. W drodze wypracowanego konsensu dodano następujące zabezpieczenia:

- zarządzanie konfiguracją,
- usuwanie informacji,
- maskowanie danych,
- zapobieganie wyciekom danych,

¹⁴ M. C. Dunn, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, London 2008, s. 19-23.

- działania monitorujące,
- filtrowanie sieci,
- bezpieczne programowanie.

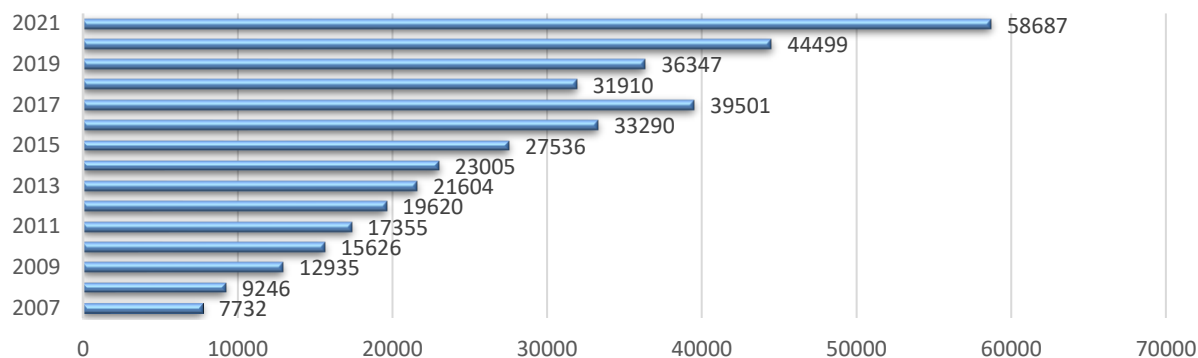
Zmianie nie uległo podejście do Systemu Zarządzania Bezpieczeństwem Informacji jako sformalizowanego podejścia do zarządzania bezpieczeństwem informacji. ISMS obejmuje polityki, procedury, wytyczne oraz towarzyszące im aktywa i działania, którymi organizacja kolektywnie zarządza w celu ochrony swoich informacji. Źródłem zaś wymagań w zakresie stopnia zapewnienia bezpieczeństwa informacji przetwarzanych w danej organizacji są wymagania zidentyfikowane przez wszystkie strony zainteresowane. Obejmować mogą one wymagania prawne i regulacyjne także zobowiązania wynikające z umów. Kadra kierownicza wyższego szczebla powinna być bezpośrednio zaangażowana w planowanie ISMS. Zaangażowanie kadry kierowniczej wyższego szczebla na wczesnym etapie jest niezbędne przy formułowaniu zakresu, jak również do pozyskania dodatkowego kluczowego zaangażowania (a co za tym idzie środków) do wykorzystania w następnych krokach przy wdrażaniu, utrzymaniu i doskonaleniu ISMS. Postęp dotyczący implementacji powinien być regularnie raportowany, z uwzględnieniem terminów realizacji ustalonych dla tej implementacji. W tej fazie należy przedstawić i wybrać cele mierzalne i okołobiznesowe. Cele te, podobnie jak cała reszta ISMS, zawsze powinny się koncentrować na ciągłym doskonaleniu, iteracja po iteracji (ISO/IEC 27001 s. 36 – 37)¹⁵. System Zarządzania Bezpieczeństwem Informacji, podobnie jak inne współczesne systemy zarządzania, bazuje na decyzjach wynikających z procesu zarządzania ryzykiem. Z praktyki audytorskiej wynika, że prawidłowo przeprowadzony proces szacowania ryzykiem determinuje adekwatność doboru zabezpieczeń. Z kolei właściwie dobrane zabezpieczenia wpływają na stopień zapewnienia bezpieczeństwa informacji w całej organizacji.

Certyfikowany System Zarządzania Bezpieczeństwem Informacji w ujęciu globalnym

Analizy rzeczywistej sytuacji na rynku certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji, dokonano na podstawie raportów publikowanych przez International Organization

¹⁵ ISO/ IEC 27001: 2022 Informatyka - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania (Information security management systems. Requirements), s. 36 – 37.

for Standardization. Rysunek 3 ilustruje liczbą wydanych certyfikatów systemu ISO/IEC 27001 w ujęciu globalnym w latach 2007 – 2021.



Rysunek 3. Liczba wydanych certyfikatów systemu ISO/IEC 27001 w ujęciu globalnym w latach 2007 – 2021

Źródło: opracowanie własne na podstawie: <https://www.iso.org> (dostęp 26.04.2023).

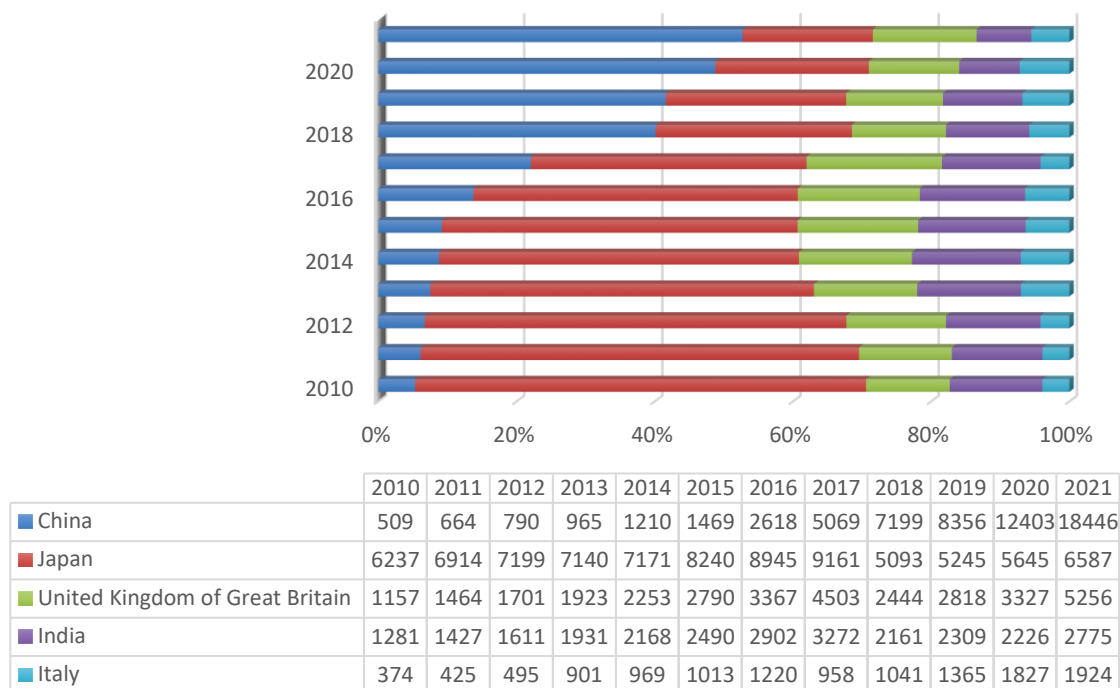
Liczba wydanych certyfikatów norma ISO/ IEC 27001 na przestrzeni 15 lat wzrosła ponad siedmiokrotnie, co może świadczyć o:

- wzrastającej świadomości zarządzających w obszarze bezpieczeństwa informacją,
- zwiększeniu ryzyka związanego z zapewnieniem bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych,
- częstszych cyberatakach i pojawieniu się nowych, wyrafinowanych sposobów wykradania danych,
- poprawie bezpieczeństwa własnych informacji organizacji jak i tych powierzonych przez partnerów biznesowych,
- podniesienie wartości organizacji
- budowa przewagi konkurencyjnej na rynku.

Biorąc pod analizę 2021 r. można zauważyć intensywny wzrost rynku certyfikacji ISO 27001 w skali globalnej o 32% w porównaniu r/r. Dla porównania w 2020 r. wzrost tego rynku w skali globalnej wynosił 22% w porównaniu do 2019 roku. Wydaje się, że wzrost ten spowodowany jest gwałtownym nasileniem przetwarzania informacji w systemach

teleinformatycznych w wyniku pandemii COVID-19 a tym samym koniecznością budowania swojej odporności na cyberzagrożenia przez nowe organizacje.

Rysunki 4 – 5 ilustrują w ujęciu globalnym pierwszą piątkę w 2021 r. krajów i branż z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001.



Rysunek 4. TOP 5 państw z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001

Źródło: opracowanie własne na podstawie: <https://www.iso.org> (dostęp 26.04.2023).

Dokonując analizy danych zaprezentowanych na rysunku 4 można zauważyć, że w ujęciu globalnym na przestrzeni dwunastu lat najwięcej certyfikatów wystawianych jest w Japonii, gdzie w 2021 r. ich liczba kształtowała się na poziomie 6587 i był to wzrost o 17% w porównaniu r/r. Biorąc pod uwagę 12 analizowanych lat to liczba wydanych certyfikatów w Japonii wzrosła o 6 % porównując 2021 r. z 2010 r.

Od 2018 r. najwięcej wydanych certyfikatów analizując poszczególne lata wydano w Chinach, gdzie w 2021 r. ich liczba kształtowała się na poziomie 18448 i był to wzrost o 49% w porównaniu r/r. Biorąc pod uwagę 12 analizowanych lat to liczba wydanych certyfikatów wzrosła ponad trzydziestokrotnie.

Na trzecim miejscu uplasowała się Wielka Brytania, gdzie w 2021 r. liczba wydanych certyfikatów kształtowała się na poziomie 5256 i był to wzrost o 58% w porównaniu r/r. Biorąc pod uwagę 12 analizowanych lat to liczba wydanych certyfikatów wzrosła ponad trzykrotnie.

Na czwartym miejscu uplasowały się Indie, gdzie w 2021 r. liczba wydanych certyfikatów kształtowała się na poziomie 2775 i był to wzrost o 25% w porównaniu r/r. Biorąc pod uwagę 12 analizowanych lat to liczba wydanych certyfikatów wzrosła o 117%.

Na piątym miejscu uplasowały się Włochy, gdzie w 2021 r. liczba wydanych certyfikatów kształtowała się na poziomie 1924 i był to wzrost o 5% w porównaniu r/r. Biorąc pod uwagę 12 analizowanych lat to liczba wydanych certyfikatów wzrosła ponad czterokrotnie.



Rysunek 5. TOP 5 branż z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001

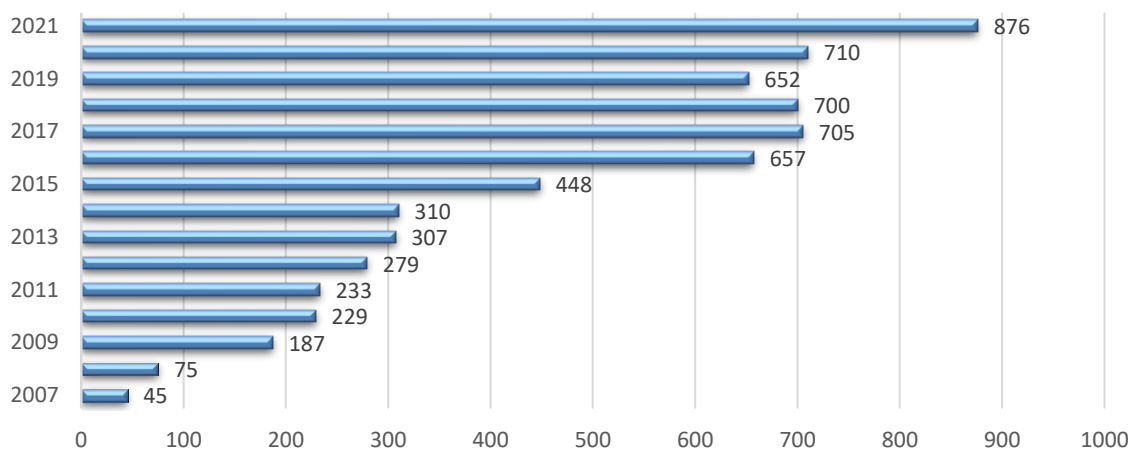
Źródło: opracowanie własne na podstawie: <https://www.iso.org> (dostęp 26.04.2023).

Biorąc pod uwagę branżę to na pierwszym miejscu są technologie informacyjne z liczbą certyfikatów w 2021 r. 10644 i był to wzrost o 5% w porównaniu r/r, w porównaniu do 2010 r. był to ponad dwukrotny wzrost.

Na przestrzeni 12 badanych lat największy wzrost (ponad trzydziestokrotny) wydanych certyfikatów odnotowała branża: Transport, magazynowanie i komunikacja. W 2021 r. porównując r/r był to wzrost ponad dziesięciokrotny. Gdzie w porównaniu r/r w 2020 r. odnotowano spadek o 37%.

Certyfikacja Systemu Zarządzania Bezpieczeństwem Informacji w Polsce

Rysunek 6 zilustrowano liczbą wydanych certyfikatów systemu ISO/IEC 27001 w Polsce w latach 2007 – 2021.



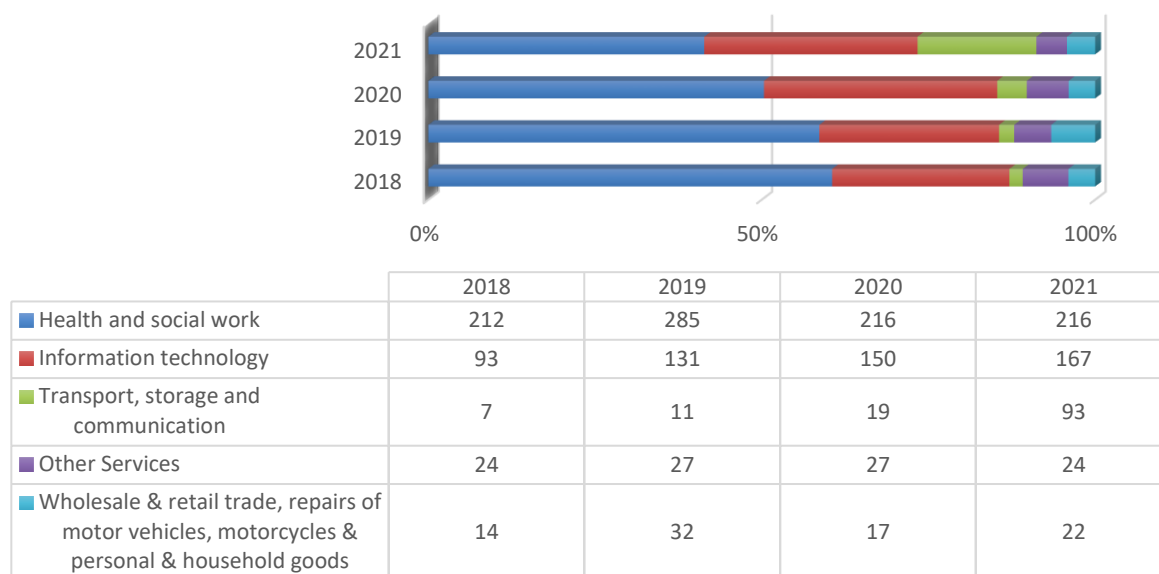
Rysunek 6. Liczba wydanych certyfikatów systemu ISO/IEC 27001 w Polsce w latach 2007 – 2021

2021 876

Źródło: opracowanie własne na podstawie: <https://www.iso.org> (dostęp 26.04.2023).

Dokonując analizy liczby wydanych certyfikatów w Polsce na przestrzeni 15 lat, nastąpił ponad osiemnastokrotny wzrost. Największy wzrost (półtorakrotny) odnotowano w 2009 roku. Spadki były w latach 2018 i 2019 odpowiednio 1% i 7%. W 2021 r. porównując do roku poprzedniego odnotowano wzrost o 166 certyfikaty tj. o 23%. W 2020 r. Polska plasowała się na 13 miejscu w rankingu globalnym wydanych certyfikatów.

Na rysunku 7 zilustrowano top 5 branż z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001 w Polsce.



Rysunek 7. TOP 5 branż z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001 w Polsce

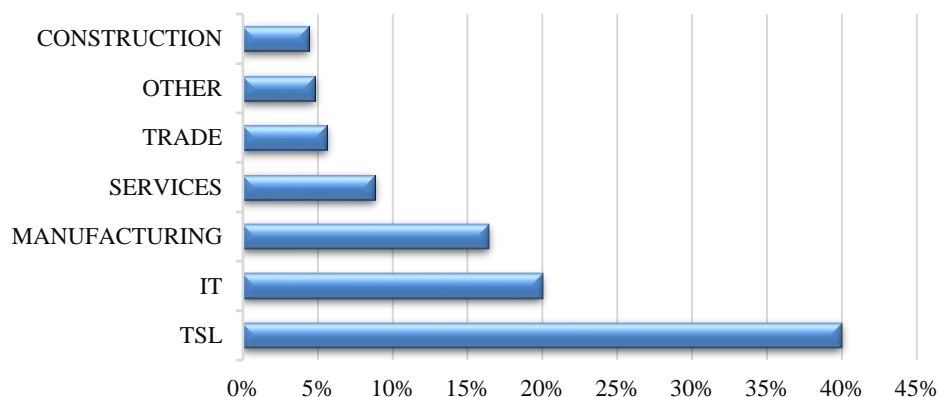
Źródło: opracowanie własne na podstawie: <https://www.iso.org> (dostęp 26.04.2023).

W Polsce branża, w której najwięcej wydano certyfikatów w analizowanym okresie to zdrowie i opieka społeczna, gdzie w 2020 i 2021 r. wydano 216 certyfikatów. Na drugim miejscu plasuje się branża technologie informacyjne, gdzie w 2021 r. wydano 167 certyfikatów tj. wzrost o 11% w porównaniu do roku poprzedniego. Na trzecim miejscu uplasowała się branża transport, gospodarka magazynowa, łącznie, gdzie w 2021 r. wydano 93 certyfikaty i był to ponad trzykrotny wzrost w porównaniu r/r.

Badania własne na przykładzie przedsiębiorstw działających w Polsce

Badanie przeprowadzono na próbie 250 przedsiębiorstw działających na terytorium Rzeczypospolitej Polskiej (rysunek 8). Największą próbą badawczą stanowiły przedsiębiorstwa z branży TSL (40%). Badania zostały zrealizowane na przestrzeni dwóch lat (listopad 2020 r. – listopad 2022 r.). Badanie sondażowe metodą ankietową autorstwa jednej z Auterek niniejszego opracowania artykułu z wykorzystaniem wywiadu telefonicznego przeprowadziło na zlecenie Instytutem Badawczym IPC Sp. z o.o. z siedzibą we Wrocławiu. Badanie zostało zrealizowane metodą wywiadów telefonicznych wśród osób odpowiedzialnych za cyberbezpieczeństwo w firmach. Osobami, które udzieliły odpowiedzi w 50% byli to pracownicy działu IT, 19%

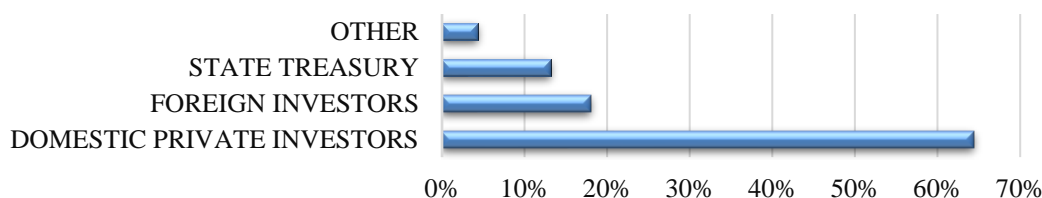
stanowili pracownicy działu logistyki, administracji i finansów, 18% kierownicy oraz 10% właściciele. Celem badań była analiza budowy systemu cyberbezpieczeństwa w przedsiębiorstwach. W niniejszym artykule przedstawiono fragment badań dotyczący stosowania norm ISO.



Rysunek 8. Rodzaj branż badanych przedsiębiorstw

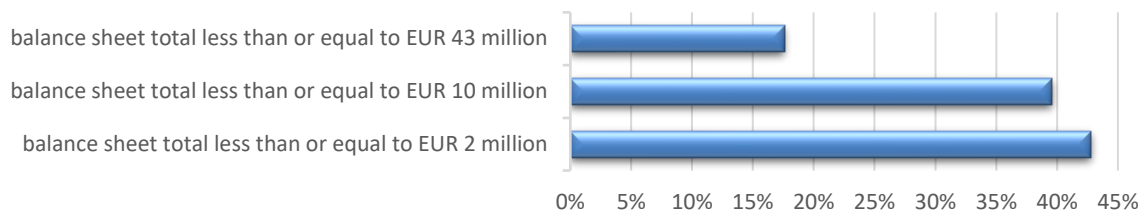
Źródło: opracowanie własne na podstawie badań ankietowych.

Dokonując charakterystyki badanych przedsiębiorstw biorąc pod uwagę akcjonariat (rysunek 9) 64% stanowili krajowi inwestorzy prywatni, 18% zagraniczni a 13% Skarb Państwa. Analizując badane przedsiębiorstwa pod względem wartości sumy bilansowej (rysunek 10) 43% stanowiły firmy, gdzie suma bilansowa była mniejsza lub równa 2 mln EUR, 40% - 10 mln EUR i 18% - 43 mln Euro. Firmy w których zatrudnienie kształtuje się na poziomie powyżej 250 osób stanowiły 35%, 26% - mniej niż 250 osób, 22% - mniej niż 50 pracowników a 18% - mniej niż 10 (rysunek 11).



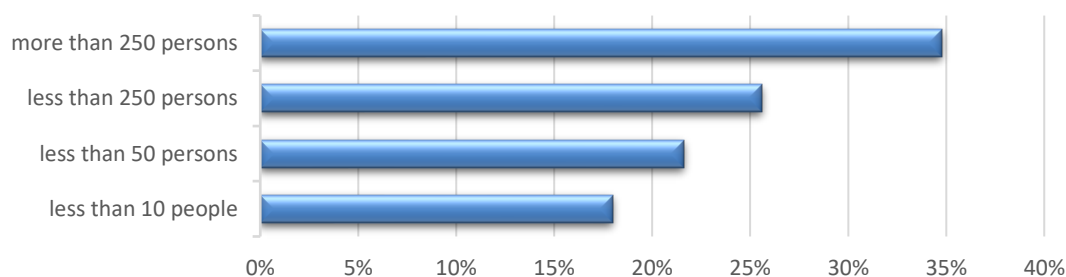
Rysunek 9. Akcjonariat badanych przedsiębiorstw

Źródło: opracowanie własne na podstawie badań ankietowych.



Rysunek 10. Wielkość sumy bilansowej badanych przedsiębiorstw

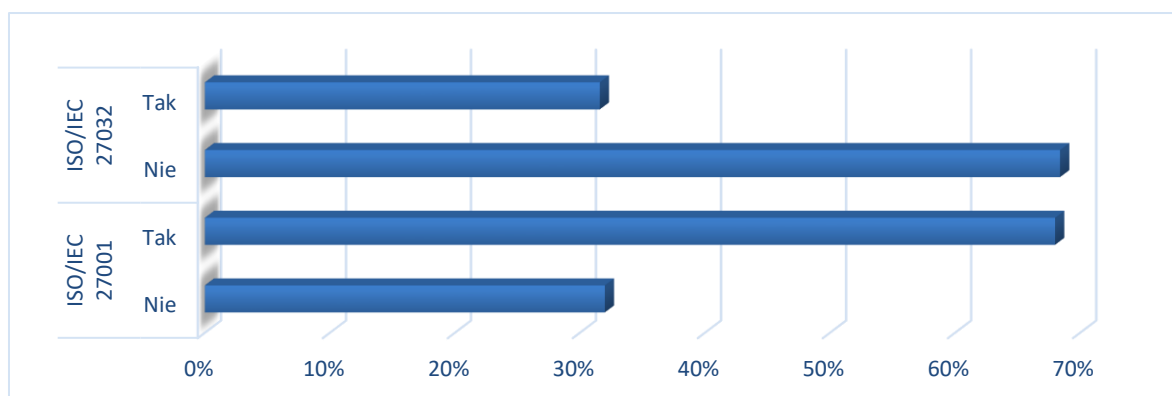
Źródło: opracowanie własne na podstawie badań ankietowych.



Rysunek 11. Wielkość zatrudnienia przedsiębiorstw

Źródło: opracowanie własne na podstawie badań ankietowych.

Ankietowani zadeklarowali w 68 %, że jest wprowadzona norma ISO/IEC 27001 oraz 32% norma ISO/IEC 27032 (rysunek 12).



Rysunek 12. ISO/IEC 27001 oraz ISO/IEC 27032

Źródło: opracowanie własne na podstawie badań ankietowych.

Biorąc pod uwagę samą branżę TSL to 73 % respondentów zadeklarowało, że jest wprowadzona norma ISO/IEC 27001 oraz 64% norma ISO/IEC 27032 adekwatnie w branży IT 74 % i 18% a w pozostałych branżach 60% i 6%

Ankietowani w szczególności w przedsiębiorstwach z branży TSL zadeklarowali również, że wprowadzone w ich przedsiębiorstwach są normy:

ISO 9001 Systemy zarządzania jakością – Wymagania, określająca wymagania, które powinien spełniać system zarządzania jakością w organizacji;

ISO 14001 Systemy zarządzania środowiskowego;

ISO 45001 Systemy zarządzania bezpieczeństwem i higieną pracy;

ISO 28000 Systemy zarządzania bezpieczeństwem w łańcuchu dostaw.

Podsumowanie

Dynamika zmian zachodzących w otoczeniu gospodarczym powoduje, że coraz więcej podmiotów gospodarczych podejmuje świadome działania w zakresie zarządzania bezpieczeństwem informacji. Kumulacja takich wydarzeń, jak pandemia COVID-19, inwazja Rosji na Ukrainę, wzrost inflacji na świecie spowodowała, że informacje przetwarzane w systemach informatycznych stały cennymi aktywami. To natomiast doprowadziło do gwałtownego wzrostu wyrafinowanych ataków hackerskich, prób wyłudzenia informacji i danych osobowych. Skala zmian zarówno po stronie prawnej, organizacyjnej jak i technologicznej była przyczynkiem do opublikowania w 2022 roku nowego wydania międzynarodowej normy zawierającej wymagania dla systemu zarządzania bezpieczeństwem informacji.

Przedstawiona w niniejszym artykule analiza wybranych zagadnień związanych z rosnącym znaczeniem zapewnienia bezpieczeństwa przetwarzanych przez organizację aktywów informacyjnych potwierdza istotny wzrost zainteresowania wśród kadry zarządzającej wdrożeniem i utrzymaniem międzynarodowych standardów w obszarze bezpieczeństwa. Najpopularniejszą formą obiektywnego potwierdzenia spełnienia wymagań bezpieczeństwa informacji jest spełnienie wymagań norm z rodziny ISO 27000. Analiza oczekiwań interesariuszy w tym zakresie, wyniki procesu zarządzania ryzykiem bezpieczeństwa informacji, klasyfikacja informacji, reagowanie na incydenty naruszenia bezpieczeństwa czy

też zapewnienie ciągłości działania to czynniki, które decydują o budowaniu odporności organizacji na współczesne zagrożenia. Potwierdzeniem tego trendu jest stale rosnąca na świecie liczba certyfikowanych organizacji na zgodność z wymaganiami ISO 27001. Tak, jak wskazano w niniejszym artykule w 2021 roku nastąpił wzrost wydanych certyfikatów ponad siedmiokrotnie porównując do 2006 roku.

W ujęciu globalnym w pierwszej piątce krajów z największą liczbą wydanych certyfikatów systemu ISO/IEC 27001 w 2021 r. znalazły się:

- Chiny – 18 448 (wzrost o 49% w porównaniu r/r);
- Japonia – 6 587 (wzrost o 17% w porównaniu r/r);
- Wielka Brytania – 5 256 (wzrost o 58% w porównaniu r/r);
- Indie – 2 775 (wzrost o 25% w porównaniu r/r);
- Włochy – 1 924 (wzrost o 5% w porównaniu r/r);

Biorąc pod uwagę branże w których wydano najwięcej certyfikatów w 2021 r. pierwszej piątce znalazły się:

- technologia informacyjna – 10 644 (wzrost o 5% w porównaniu r/r);
- transport, przechowywanie i komunikacja – 6 909 (ponad dziesięciokrotny wzrost w porównaniu r/r);
- inne usługi – 1 693 (wzrost o 25% w porównaniu r/r);
- pośrednictwo finansowe, nieruchomości, wynajem – 645 (wzrost o 14% w porównaniu r/r);
- usługi inżynierskie – 630 (wzrost o 58% w porównaniu r/r);

Biorąc pod uwagę sytuację w Polsce, to zauważalna jest pozytywna tendencja. Na przestrzeni 15 lat, nastąpił ponad osiemnastokrotny wzrost wydanych certyfikatów normy ISO/IEC 27001. Analizując branżę to najwięcej certyfikatów w 2021 r. wydano w:

- zdrowie i opieka społeczna – 216 (taka sama wartość jak w 2020 r.);
- technologie informacyjne – 167 (wzrost o 11% w porównaniu r/r);

-
- transport, gospodarka magazynowa i łączność – 93 (ponad trzykrotny wzrost w porównaniu r/r).

W analizowanych przedsiębiorstwach ankietowani wskazali w szczególności trzy obszary zarządzania organizacją w których stosowane są normy ISO tj.: bezpieczeństwo informacją, jakością i środowiskiem. W branży TSL wskazano również normy ISO w zakresie systemu zarządzania bezpieczeństwem i higieną pracy oraz zarządzania bezpieczeństwem w łańcuchu dostaw.

Warto zauważyć, że branżą, w której odnotowano największy wzrost zarówno w ujęciu globalny jak i w Polsce jest branża logistyczna co może świadczyć o wzrastającej świadomości kadry zarządzającej, że normy ISO zapewniają organizacjom pomoc w zapewnieniu najlepszych możliwych ram i zapewnieniu ich cyberbezpieczeństwa.

Streszczenie:

W zaprezentowanej pracy podjęto problem zarządzania bezpieczeństwem informacji we współczesnych organizacjach gospodarczych z perspektywy standardów definiowanych przez normy ISO, a także strategii i działań jakie podejmują przedsiębiorstwa w celu zapobiegania i minimalizowania niebezpieczeństw związanych z cyberatakami. Przedstawiono badania literaturowe dotyczące działalności przedsiębiorstw w obszarze zarządzania cyberbezpieczeństwem i uzupełniono je badaniami ankietowymi zrealizowanymi w przedsiębiorstwach działających w Polsce.

Słowa kluczowe:

Zarządzanie, bezpieczeństwo, informacja

Keywords:

Management, security, information

Bibliografia:

1. Aleksandrowicz T. R. *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016.
2. Antczak J., *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*, ASzWoj, Warszawa 2021.
3. Banasiński C. (red.) *Cyberbezpieczeństwo zarys wykładu*, Wolters Kluwer, Warszawa 2018.
4. Bell, S. *Cybersecurity is not just a 'big business' issue*. Gov. Dir. 2017, 69.
5. Dhillon G. *Managing information system security*. Macmillan International Higher Education; 1997.
6. Dunn M. C. *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, London 2008.
7. European Union Agency for Cybersecurity (ENISA). Standardization in support of the Cybersecurity Certification; 2019, za: <https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i>, (November 2022).
8. Ghafir I., Saleem J., Hammoudeh M, Faour H, Prenosil V., Jaf S., Jabbar S, Baker T., *Security threats to critical infrastructure: the human factor*. The Journal of Supercomputing 2018;74(10):4986–5002.
9. Ghelani D. *Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review*, “American Journal of Science, Engineering and Technology”, Vol. 3, No. 6, 2022.
10. Govender S.G, Kritzinger E, Loock M . *A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture*, 1226. Cham: Springer; 2020.
11. <https://www.iso.org>.
12. <https://www.iso.org/contents/news/2023/02/how-to-build-cyber-resilience.html> (14.04.2022).
13. <https://www.iso.org/isoiec-27001-information-security.html> (14.04.2023).
14. <https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who>.
15. ISO/ IEC 27000:2016 *Technika informatyczna. Techniki bezpieczeństwa* (Information technology – Security technique).
16. ISO/ IEC 27001:2022 *Informatyka - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania* (Information security management systems. Requirements).
17. Jalagat R., *The impact of change and change management in achieving corporate goals and objectives: Organizational perspective*. ”International Journal of Science and Research” 2016;5(11):1233–9 .
18. Mraković, I., Vojinović, R. *Maritime Cyber Security Analysis – How to Reduce Threats?*, “Transactions on Maritime Science”, 2019 08 (01). <https://doi.org/10.7225/toms.v08.n01.013>

-
19. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* 2021, 1, 119–139.
 20. Rojszczak M. (2018), Cyberbezpieczeństwo z perspektywy przedsiębiorcy, [w:] Banasiński C., Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer Polska, Warszawa.
 21. Sienkiewicz P., *10 wykładów*, AON, Warszawa 2005
 22. Stallings, W. *Cryptography and Network Security*, 4th ed.; Pearson Education India: Delhi, India, 2006.
 23. Stoneburner, G.; Goguen, A.; Feringa, *Risk management guide for information technology systems*. Nist Spec. Publ. 2002.
 24. Tekleselas W. H. *Emerging Cyber Security Threats in Organization*, “International Journal of Information and Communication Sciences”. Vol. 5, No. 2, 2020.