Politechnika Częstochowska
Wydział Zarządzania

Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie
Research Reviews of Czestochowa University of Technology. Management

Nr 53 (2024), s. 104-120, ISSN: 2083-1560
DOI: 10.17512/znpcz.2024.1.09, https://znz.pcz.pl/

Nadesłanie artykułu: 05.01.2024; Poprawa artykułu: 25.01.2024;
Akceptacja: 26.01.2024; Publikacja: 31.03.2024.

BEZPIECZEŃSTWO INFORMACJI W ERZE PRACY ZDALNEJ A ROLA MODELU ISO 27001:2017

Anna Rychły-Lipińska[1*], Wiesław Kamiński[2]

[1, 2] Uniwersytet Pomorski w Słupsku, Instytut Zarządzania, Polska

Streszczenie: Bezpieczeństwo informacji w pracy zdalnej to kluczowy obszar wymagający uwagi i działań pracodawców. W artykule dokonano analizy elementów tego zagadnienia, koncentrując się na wyzwaniach związanych z pracą zdalną i roli normy ISO 27001:2017 w zarządzaniu bezpieczeństwem informacyjnym. W publikacji zwrócono uwagę na wzrost znaczenia pracy zdalnej, co skłania do refleksji nad bezpieczeństwem danych. Jako wsparcie w zarządzaniu bezpieczeństwem informacji w organizacji wskazano normę ISO 27001:2017. Metody badawcze wykorzystane w artykule to przegląd literatury i metoda delficka. Przegląd literatury obejmował analizę bezpieczeństwa informacji w pracy zdalnej, atrybutów bezpieczeństwa, normy ISO 27001:2017 oraz zarządzania bezpieczeństwem informacji. Dzięki zastosowaniu metody delfickiej wykorzystano opinie ekspertów, w tym audytorów ISO 27001:2017 i inspektorów bezpieczeństwa informacji z MŚP. Artykuł rozpoczęto omówieniem istoty bezpieczeństwa informacji, podkreślając jego znaczenie dla ochrony danych. Następnie dokonano analizy atrybutów bezpieczeństwa informacji, takich jak poufność, integralność i dostępność danych, w kontekście pracy zdalnej. W artykule przedstawione zostały również wyzwania, przed jakimi stoją pracodawcy, dotyczące bezpieczeństwa informacji przy pracy zdalnej. W dalszej części artykułu omówiono model systemowego zarządzania bezpieczeństwem informacyjnym – ISO 27001:2017, prezentując autorską check listę wspierającą ocenę efektywności systemów zarządzania bezpieczeństwem informacji.

Słowa kluczowe: atrybuty bezpieczeństwa informacji, bezpieczeństwo informacji, ISO 27001:2017, praca zdalna, systemowe zarządzanie bezpieczeństwem informacyjnym

Kod klasyfikacji JEL: L86, D23, D29

[1] Anna Rychły-Lipińska, dr, ul. Kozietulskiego 6-7, 76-200 Słupsk, Polska, anna.rychly-lipinska@upsl.edu.pl, https://orcid.org/0000-0001-9467-6682
[2] Wiesław Kamiński, mgr, ul. Kozietulskiego 6-7, 76-200 Słupsk, Polska, wieslaw.kaminski@upsl.edu.pl, https://orcid.org/0000-0002-0285-7062
* Autor korespondencyjny: Anna Rychły-Lipińska, anna.rychly-lipinska@upsl.edu.pl

DOI: 10.17512/znpcz.2024.1.09

Wprowadzenie

Przed wybuchem pandemii COVID-19 w zastosowaniu formy pracy zdalnej upatrywano przede wszystkim wiele korzyści. Zastosowanie technologii komputerowej miało obniżać koszty zatrudnienia, dając możliwości rozwoju przedsiębiorstwom, jednocześnie oferując pracownikom większą swobodę i autonomię oraz doświadczenie zawodowe.

Obecnie coraz częściej dostrzega się, że za pracą zdalną muszą iść pewne zmiany związane z przepisami oraz z zastosowaniem odpowiedniego zarządzania bezpieczeństwem informacji. Bezpieczeństwo informacji jest istotne zarówno dla podmiotów sektora prywatnego, jak i jednostek sektora publicznego. W efekcie coraz większego wykorzystania Internetu w życiu zawodowym informacje są narażone na coraz to większą skalę, a także różnorodność zagrożeń. Niezbędna jest więc implementacja odpowiednich środków bezpieczeństwa w celu ochrony informacji przed celowym lub nieumyślnym jej zmodyfikowaniem, zniszczeniem, przechwyceniem czy ujawnieniem (Myśko & Młodzik, 2014).

Niniejsza publikacja podzielona została na trzy części. W części pierwszej opisano ideę bezpieczeństwa informacji, która stanowi jeden z fundamentów działalności organizacji. W części drugiej zaprezentowany został problem pracy zdalnej – jako wyzwanie dla pracodawców, a w kolejnej przedstawione zostały założenia systemu ISO 27001 wraz z autorską listą pytań możliwą do wykorzystania przy sprawdzaniu systemu zarządzania bezpieczeństwem informacji. W artykule zwrócono uwagę na zmiany w przepisach związane z pracą zdalną, jakie zaszły 7 kwietnia 2023 r., oraz poddano zastanowieniu tezę, że implementacja normy ISO 27001 stanowi istotne wsparcie dla zapewnienia skutecznego bezpieczeństwa informacji w środowisku pracy zdalnej. Publikacja jest niejako zachętą do wykorzystania narzędzia, jakim jest norma ISO 27001 w zapewnieniu bezpieczeństwa informacji w danej organizacji, umożliwiając identyfikację, ocenę oraz kontrolę ryzyka związanego z przechowywaniem i przetwarzaniem danych, co jest kluczowe dla ochrony informacji w erze technologii komunikacyjnych.

Opisując model systemowego zarządzania bezpieczeństwem informacji w oparciu o normę ISO 27001:2017, autorzy wskazują na to, że może on być dobrą wytyczną dla organizacji w zakresie budowy, wdrożenia i doskonalenia systemu zarządzania bezpieczeństwem informacji. Może on stanowić ważne narzędzie, pozwalające organizacjom na skuteczne zarządzanie ryzykiem związanym z bezpieczeństwem informacji, w tym także w kontekście pracy zdalnej.

Metodyka badań

Artykuł skupia się na kluczowym aspekcie pracy zdalnej, jakim jest bezpieczeństwo informacji, i analizuje rolę normy ISO 27001:2017 w zarządzaniu bezpieczeństwem informacyjnym.

Celem głównym artykułu jest zbadanie kluczowego obszaru bezpieczeństwa informacji w kontekście pracy zdalnej oraz analiza roli normy ISO 27001:2017 w skutecznym zarządzaniu bezpieczeństwem informacyjnym. Celem dodatkowym

jest wskazanie praktycznego narzędzia, wspierającego ocenę efektywności systemów zarządzania bezpieczeństwem informacji.

Metody badawcze obejmują przegląd literatury konceptualnej w zakresie: bezpieczeństwa informacji w pracy zdalnej, atrybutów bezpieczeństwa, normy ISO 27001:2017, zarządzania bezpieczeństwem informacji oraz metodę delficką wykorzystującą opinie ekspertów w tym audytorów zewnętrznych ISO 27001:2017 i inspektorów bezpieczeństwa informacji z małych i średnich przedsiębiorstw.

Istota bezpieczeństwa informacji

W znaczeniu potocznym pojęcie bezpieczeństwa związane jest z osiąganiem stanu spokoju, stanu braku zagrożenia. Wraz z rozwojem technologii teleinformatycznych pojawił się problem zapewnienia bezpieczeństwa systemów teleinformatycznych oraz środowisk, w których są zastosowane, tak by przetwarzaną w nich informację i świadczone przez nie usługi można było uważać za bezpieczne. W tym przypadku bezpieczeństwo jest rozumiane jako niczym niezakłócone funkcjonowanie tych systemów podczas realizacji wyznaczonych dla nich zadań, wykonywanych dla dobra danej instytucji (Białas, 2017). Według Kosińskiego (2000) bezpieczeństwo informacji rozumiane jest jako pewność ochrony dostępu do informacji zgromadzonej i pewność ochrony informacji przesyłanej.

Pod pojęciem informacji „należy rozumieć przekaz wiadomości o dowolnym charakterze i strukturze nośnika, który wzbogaca naszą wiedzę" (Kowalska-Napora, 2010). Informacja to także towar, i to często o znaczeniu strategicznym (dla państwa, firmy, konkretnej osoby) (Liderman, 2012).

Informacja jest jednym z najcenniejszych zasobów organizacji. Z punktu widzenia biznesowego to właśnie informacje posiadają określoną wartość dla organizacji. W związku z tym, w celu zapewnienia ich bezpieczeństwa, powinny być chronione, co może mieć znaczenie dla zapewnienia rentowności, zachowania płynności finansowej i zgodności działalności z przepisami prawa oraz utrzymania reputacji przez organizację (Myśko & Młodzik, 2014).

Zapewnienie bezpieczeństwa informacji to pewien rodzaj praktyki, który obejmuje wdrażanie polityk i procedur mających na celu ochronę informacji i pomagających zapobiegać utracie lub kradzieży danych (Rudra, 2022).

Werner i Szczepaniuk (2016) definiują bezpieczeństwo informacyjne organizacji jako stan, w którym:

- Elementy tworzące system bezpieczeństwa cechuje zdolność do ochrony przed obecnymi i przyszłymi zakłóceniami (zagrożeniami) funkcjonowania lub utraty określonych wartości; czyli system jest odporny na wszelkiego typu zagrożenia, tj. wewnętrzne, zewnętrzne, przypadkowe, celowe.
- Bezpieczeństwo informacji jest osiągnięte i utrzymywane na założonym poziomie poufności, integralności i dostępności.
- Zapewniona jest autentyczność i rozliczalność podmiotów związana z autoryzacją użytkowników korzystających z określonych informacji i usług.

– Zarówno pracownicy organizacji, jak i odbiorcy informacji i usług (obywatele, przedsiębiorcy, pracownicy zatrudnieni w innych organizacjach) mają świadomość i są podatni na zagrożenia bezpieczeństwa informacyjnego.
– Aktorzy zagrożeń (także napastnicy wewnętrzni) mają małe możliwości wykorzystania systemów teleinformatycznych do generowania zagrożeń przez wykorzystanie słabości, podatności i luk w systemie zabezpieczeń.

Należy mieć na uwadze, że bezpieczeństwo informacji to nie tylko wymóg działalności biznesowej, który usprawnia organizację poprzez korzyści wynikające ze stosowania opracowanych zasad przetwarzania informacji, ale również jest to obowiązek wynikający z przepisów prawa. Niespełnienie wymagań prawnych skutkować może poważnymi konsekwencjami w postaci administracyjnych kar finansowych, a nawet zakończeniem działalności (Kasprzak, 2022).

Do najważniejszych wymagań prawnych w zakresie ochrony określonej kategorii informacji należy zaliczyć (Kasprzak, 2022):

– ochronę danych osobowych (klientów, kontrahentów, pracowników, współpracowników);
– ochronę tajemnicy przedsiębiorstwa (technologie, strategie, know-how);
– ochronę informacji finansowej i podatkowej (finanse, rachunki, faktury, płace);
– ochronę informacji niejawnych (tajemnicę państwową);
– tajemnicę zawodową (lekarską, adwokacką, bankową).

Bezpieczeństwo informacyjne jest pojęciem bardzo szerokim. Obejmuje bowiem ochronę informacji niezależnie od jej formy, np. informacji cyfrowych, dokumentów papierowych, komunikatów wypowiedzianych w rozmowie. Niezależnie jednak od formy bezpieczeństwo informacji powinno spełniać tzw. atrybuty bezpieczeństwa (Werner & Szczepaniuk, 2016).

W literaturze przedmiotu zostały określone trzy główne atrybuty bezpieczeństwa informacji i systemów informacyjnych (gov.pl, 2023):

– Poufność, czyli zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych. Utrata poufności oznacza nieuprawnione ujawnienie informacji.
– Integralność, oznaczającą ochronę przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji. Utrata integralności oznacza nieuprawnioną modyfikację lub zniszczenie informacji.
– Dostępność, czyli zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji. Utrata dostępności oznacza zaburzenie dostępu lub możliwości wykorzystania informacji lub systemu informacyjnego.

Werner i Szczepaniuk (2016) rozszerzają te trzy podstawowe atrybuty (poufność, integralność, dostępność) o kolejne, takie jak: rozliczalność, niezawodność, autentyczność (Tabela 1). Jak opisują Werner i Szczepaniuk (2016), pierwsze trzy z przywołanych atrybutów – tj. poufność, integralność, dostępność – odnoszone są do informacji w każdej postaci. Natomiast rozliczalność, niezawodność i autentyczność dotyczą ochrony informacji w systemach teleinformatycznych, czyli informacji cyfrowej.

Tabela 1. Atrybuty bezpieczeństwa informacji

Atrybut	Charakterystyka
Poufność	dostęp do informacji musi być ograniczony tylko do kręgu użytkowników autoryzowanych
Integralność	informacja musi być zachowana w swej oryginalnej postaci, za wyjątkiem sytuacji, gdy jest aktualizowana lub usuwana przez osoby do tego uprawnione
Dostępność	dostęp dla uprawnionych użytkowników w odpowiednim czasie;
Rozliczalność	możliwość identyfikacji użytkowników informacji oraz systemu teleinformatycznego
Niezawodność	właściwość oznaczająca spójne zamierzone zachowania i skutki
Autentyczność	oznacza możliwość jednoznacznego stwierdzenia tożsamości podmiotu przesyłającego dane

Źródło: (Werner & Szczepaniuk, 2016)

Bezpieczeństwo informacji jest kluczowe dla współczesnych organizacji, które w coraz większym stopniu polegają na technologii cyfrowej. Obejmuje ono zapewnienie poufności, integralności i dostępności danych, chroniąc przed nieuprawnionym dostępem, modyfikacją i utratą informacji. Dla firm informacja stanowi cenny zasób, wpływając bezpośrednio na ich rentowność, płynność finansową i reputację. Atrybuty bezpieczeństwa informacji – poufność, integralność i dostępność – są kluczowe dla skutecznego zarządzania ryzykiem oraz utrzymania stabilności operacyjnej organizacji. W obliczu możliwości korzystania z pracy zdalnej implementacja skutecznych strategii bezpieczeństwa informacji staje się niezbędna dla ochrony danych przed zaawansowanymi zagrożeniami.

Praca zdalna jako wyzwanie dla pracodawcy

Praca na odległość w regulacjach prawa polskiego ma raczej krótką historię. Jej pierwsze zorganizowane przejawy datuje się na rok 2007, kiedy to dodano do *Kodeksu pracy* rozdział dotyczący telepracy. Jednak mimo istnienia takiej możliwości wzrost zainteresowania zdalnym modelem wykonywania obowiązków nastąpił dużo później, a jego szczyt datuje się dopiero na lata 2020-2022, kiedy po raz pierwszy ustawodawca użył pojęcia pracy zdalnej. Nagły wzrost zainteresowania ową formą zatrudnienia wiązał się z koniecznością dostosowania warunków pracy do sytuacji epidemiologicznej na świecie, a także ze wzrostem technologicznym i powszechnym wdrażaniem nowoczesnych technologii do systemów pracy (Bernacka, 2023).

Pojęcie pracy zdalnej zaistniało w polskim prawie pracy w marcu 2020 roku. Przez lata mówiło się o tzw. pracy na odległość, której podstawową formę stanowiła tzw. telepraca (Sidor-Rządkowska, 2022).

Epidemia COVID-19 spowodowała upowszechnienie się pracy zdalnej, która jeszcze w 2020 roku występowała w trzech odsłonach prawnych (Deloitte, 2023):

– praca w formie telepracy;
– praca zdalna na podstawie przepisów tzw. tarczy antykryzysowej;
– praca zdalna poza powyższymi reżimami.

Od 7 kwietnia 2023 r. zostały wprowadzone do *Kodeksu pracy* zapisy dotyczące pracy zdalnej. Określają one, że praca zdalna może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (MRPiPS, 2024; Białogrecka & Smalara, 2023).

Wprowadzenie pracy zdalnej to wyzwanie dla pracodawców z punktu widzenia zarządzania bezpieczeństwem informacji. Są oni bowiem zobligowani do wdrożenia odrębnych procedur dotyczących bezpieczeństwa informacji, także tych niebędących danymi osobowymi (Łaguna, 2023).

W literaturze przedmiotu można się spotkać z opisanymi szansami oraz zagrożeniami związanymi z wykonywaną pracą zdalną rozpatrywaną zarówno z punktu widzenia pracownika, jak i pracodawcy. Autorzy publikacji skupili się wyłącznie na incydentach związanych z brakiem zachowania bezpieczeństwa informacji w pracy zdalnej rozpatrywanym od strony pracodawcy. Tego typu zagrożenia przedstawione zostały m.in. przez Bernacką (2023), Kurnytę (2023), Niwińskiego & Rzyckiego (2023), a są to m.in.:

– Ataki phishingowe na pracowników pracujących zdalnie. Pracownicy mogą otrzymywać fałszywe e-maile wyglądające na oficjalne wiadomości z miejsca pracy, proszące o potwierdzenie poufnych danych lub logowanie się na fałszywe strony internetowe. W rezultacie dane logowania do systemów firmy mogą zostać skradzione, co prowadzi do wycieku informacji.
– Nieaktualne oprogramowanie i brak zabezpieczeń. Jeżeli pracownicy zdalni nie aktualizują regularnie swojego oprogramowania ani nie stosują odpowiednich zabezpieczeń, to otwiera to drzwi do ataków złośliwego oprogramowania lub innego rodzaju cyberataków, które mogą narazić systemy firmy na ryzyko.
– Nieuprawnione korzystanie z sieci Wi-Fi. Jeżeli pracownicy korzystają z publicznych sieci Wi-Fi lub innych niezabezpieczonych połączeń internetowych podczas pracy zdalnej, to naraża to firmę na ryzyko przechwycenia danych przez osoby trzecie.
– Utrata urządzeń przenośnych z poufnymi danymi. Jeżeli pracownik pracujący zdalnie zagubi urządzenie zawierające poufne dane firmowe, to brak odpowiednich zabezpieczeń, takich jak szyfrowanie danych, może prowadzić do wycieku informacji.
– Brak świadomości pracowników o politykach bezpieczeństwa. Jeżeli pracownicy nie są świadomi polityk bezpieczeństwa informacji w firmie lub nie przestrzegają ich, np. poprzez udostępnianie poufnych danych osobom nieuprawnionym lub używanie prywatnych kont do przesyłania danych firmowych, to narażają firmę na ryzyko.
– Atak na systemy zdalne. Złośliwe oprogramowanie jest wprowadzane do systemu zdalnego pracownika, co skutkuje zablokowaniem dostępu do danych i żądaniem okupu w zamian za odblokowanie systemu.

Te incydenty wyraźnie pokazują, jak nieprzestrzeganie zasad bezpieczeństwa informacji w pracy zdalnej może prowadzić do różnych problemów i narazić firmę na poważne ryzyko utraty danych lub ataków cybernetycznych. Wdrożenie odpowiednich procedur i polityk bezpieczeństwa oraz zwiększenie świadomości pracowników są kluczowe dla zapewnienia bezpieczeństwa informacji w środowisku pracy zdalnej.

Dlatego też decyzją o charakterze strategicznym jest przyjęcie przez organizację systemu zarządzania bezpieczeństwem informacji. Na ustanowienie i wdrożenie systemu zarządzania bezpieczeństwem informacji mają wpływ potrzeby i cele organizacji, wymagania bezpieczeństwa, procesy funkcjonujące w organizacji oraz wielkość i struktura organizacyjna. W tym kontekście wprowadzenie w organizacji pracy zdalnej z całą pewnością ma wpływ na potrzeby i wymagania bezpieczeństwa dotyczące procesów w organizacji, bowiem zmienia się struktura przepływu informacji. Do przetwarzania informacji nie dochodzi już tylko w siedzibie pracodawcy czy w miejscach zorganizowanych przez pracodawcę. Przy pracy zdalnej cenne informacje dla pracodawcy mogą być także przetwarzane w domu pracownika lub w innym uzgodnionym miejscu pracy zdalnej. Dlatego też wprowadzenie pracy zdalnej stanowi wyzwanie dla pracodawców z punktu widzenia zarządzania bezpieczeństwem informacji (Łaguna, 2023).

System zarządzania bezpieczeństwem informacji (SZBI) to nic innego jak strategia działania, której celem jest zapewnianie właściwej ochrony informacji. Strategia ta ma zapewnić ciągłe doskonalenie działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności. Innymi słowy, system bezpieczeństwa informacji ma chronić w taki sposób przed zagrożeniami, żeby zapewnić organizacji (Kasprzak, 2022):

- ciągłość prowadzenia działalności,
- zminimalizowanie strat,
- maksymalizowanie zwrotu nakładów na inwestycje i działania o charakterze biznesowym.

SZBI zgodny z normą ISO/IEC 27001 uznawany jest za rozwiązanie zapewniające zachowanie poufności, integralności i dostępności informacji, których ochrona jest obecnie naturalnym wymogiem naszych czasów (Kasprzak, 2022).

Model systemowego zarządzania bezpieczeństwem informacyjnym – ISO 27001:2017

Norma ISO 27001 (lub ISO/IEC 27001) to międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji (SZBI). Norma ta określa wymagania dla ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Ponadto zawiera wytyczne dotyczące szacowania i postępowania z ryzykiem związanym z bezpieczeństwem informacji (Resilia, 2022).

Zgodnie z ISO/IEC 27000 system zarządzania bezpieczeństwem informacji (SZBI) to „zbiór polityk, procedur, wytycznych oraz aktywności wykorzystywanych przez organizację w celu ochronnych swoich zasobów informacyjnych" (PN-EN ISO/IEC 27000:2020-07).

DOI: 10.17512/znpcz.2024.1.09

Według autorów norma ISO 27001 wspiera organizacje w spełnianiu regulacji i przepisów dotyczących bezpieczeństwa informacji w pracy zdalnej na kilka sposobów poprzez:

- Ramowy standard zgodności – norma ISO 27001 stanowi ramy do stworzenia systemu zarządzania bezpieczeństwem informacji. Implementacja tego standardu umożliwia organizacji ustanowienie spójnych i zgodnych z przepisami procedur i polityk bezpieczeństwa informacji.
- Uwzględnienie wymogów prawnych – przy wdrażaniu ISO 27001 organizacje muszą wziąć pod uwagę obowiązujące przepisy dotyczące bezpieczeństwa informacji, co obejmuje również aspekty związane z pracą zdalną. Standard pomaga uwzględnić te wymogi w systemie zarządzania bezpieczeństwem informacji.
- Identyfikację i zarządzanie ryzykiem zgodności – ISO 27001 nakłada obowiązek na organizację, aby identyfikować i zarządzać ryzykiem związanym z niewykonaniem przepisów i regulacji. Obejmuje to również ryzyko związane z bezpieczeństwem informacji w pracy zdalnej.
- Ciągłe doskonalenie systemu – wdrożenie ISO 27001 wymaga ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Organizacje muszą monitorować zmieniające się przepisy i regulacje dotyczące pracy zdalnej oraz aktualizować swoje procedury, aby pozostać zgodnym z wymogami prawnymi.
- Zwiększone zaufanie ze strony regulatorów – posiadanie certyfikatu zgodności z normą ISO 27001 może zwiększyć zaufanie organów regulacyjnych i instytucji nadzorczych, pokazując, że organizacja podejmuje odpowiednie kroki w kierunku zabezpieczenia informacji, także w kontekście pracy zdalnej.

Dzięki tym aspektom norma ISO 27001 stanowi nie tylko strukturę do zarządzania bezpieczeństwem informacji w pracy zdalnej, ale również umożliwia organizacjom spełnianie obowiązujących regulacji i przepisów związanych z ochroną danych w tym specyficznym kontekście.

Norma ISO 27001 definiuje standardowe wymagania i wytyczne dotyczące zarządzania bezpieczeństwem informacji w organizacjach. Norma zawiera *Załącznik A*, który jest prawdopodobnie najbardziej znanym załącznikiem ze wszystkich norm ISO. Załącznik ten jest wręcz podstawowym narzędziem do zarządzania zagrożeniami bezpieczeństwa informacji (Stinet, 2023). Zawiera 114 punktów i związanych z nimi celów kontroli, które mogą być wdrożone w celu ochrony informacji w organizacji. Te cele kontroli są uważane za ogólne cele w obszarze bezpieczeństwa informacji.

Warto zaznaczyć, że *Załącznik A* nie jest obowiązkowy, ale jest wykorzystywany jako wskazówka do opracowania własnych standardów kontroli i procedur bezpieczeństwa, które są odpowiednie dla danej organizacji i jej kontekstu. Wdrażanie konkretnych standardów kontroli zależy od oceny ryzyka i potrzeb organizacji.

Organizacje nieposiadające wdrożonego systemu zarządzania bezpieczeństwem informacji ISO 27001 mają możliwość korzystania z *Załącznika A* jako wręcz przewodnika w opracowaniu lub udoskonaleniu swojego obecnego systemu bezpieczeństwa informacji. *Załącznik A* do normy ISO 27001 może być traktowany jako

tzw. check lista zbioru kontrolnych punktów wspierających organizacje w zarządzaniu bezpieczeństwem informacji.

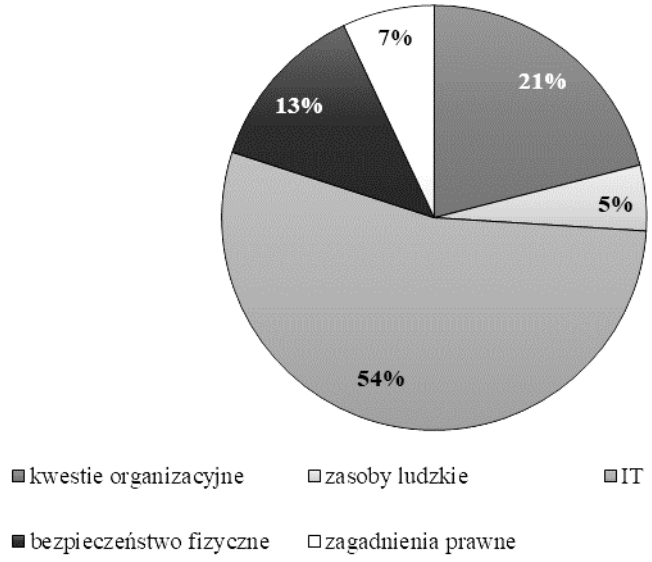
Z *Załącznika A* można korzystać na dwa sposoby (Stinet, 2023):

- projektując strategię bezpieczeństwa firmy – poprzez wybór tych punktów kontroli, które mają zastosowanie do konkretnej organizacji.
- oceniając gotowość organizacji do procesu zarządzania bezpieczeństwem informacji – jako ocena już wdrożonej strategii bezpieczeństwa i jako baza do doskonalenia posiadanego systemu.

Wspomniana lista 114 punktów kontroli ISO 27001 znajduje się w 14 domenach opisanych w *Załączniku A*. Wbrew pozorom nie wszystkie są zorientowane na IT. Poniżej przedstawione zostało zestawienie (wraz z odpowiednimi punktami *Załącznika A*), które pokazuje, na czym skupiają się punkty kontroli. Są to sekcje dotyczące:

- kwestii organizacyjnych (te kwestie zawierają się w punktach *Załącznika A*: A.5, A.6, A.8, A.15);
- zasobów ludzkich (A.7);
- IT (A.9, A.10, A.12, A.13, A.14, A.16, A.17);
- bezpieczeństwa fizycznego (A.11);
- zagadnień prawnych (A.18).

Procentowy podział zagadnień w poszczególnych sekcjach *Załącznika A* do normy ISO 27001 przedstawiono na Rysunku 1.



Rysunek 1. Procentowy podział zagadnień w poszczególnych sekcjach *Załącznika A* do normy ISO 27001

Źródło: Opracowanie własne na podstawie (Stinet, 2023)

DOI: 10.17512/znpcz.2024.1.09

Analizując dane przedstawione na Rysunku 1, można zauważyć, że ponad 50% punktów stanowią punkty kontroli związane z posiadaną infrastrukturą IT, kwestie organizacyjne stanowią 21%, bezpieczeństwo fizyczne – 13%, zagadnienia prawne – 7%, zasoby ludzkie – 5%.

W Tabeli 2 zaprezentowano rozszerzenia 14 domen ISO 27001 w podziale na zidentyfikowane wyżej sekcje.

Tabela 2. Domeny *Załącznika A* do normy ISO 27001 wraz z opisem

Punkt	Nazwa	Opis
DOMENY ZWIĄZANE Z IT		
A.9	Kontrola dostępu	mechanizmy kontroli zarządzania prawami dostępu użytkowników, systemów i aplikacji oraz zarządzania obowiązkami użytkowników
A.10	Kryptografia	kontrole związane z szyfrowaniem i zarządzaniem kluczami
A.12	Bezpieczeństwo operacyjne	wiele kontroli związanych z zarządzaniem produkcją IT: zarządzanie zmianą, zarządzanie wydajnością, złośliwe oprogramowanie, tworzenie kopii zapasowych, logowanie, monitorowanie, instalacja, podatności itp.
A.13	Bezpieczeństwo komunikacji	kontrole związane z bezpieczeństwem sieci, segregacją, usługami sieciowymi, przesyłaniem informacji, przesyłaniem wiadomości itp.
A.14	Pozyskiwanie, rozwój i utrzymanie systemu	mechanizmy kontrolne określające wymagania bezpieczeństwa oraz bezpieczeństwo w procesach rozwoju i wsparcia
A.16	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	mechanizmy kontroli zgłaszania zdarzeń i słabych punktów, określanie odpowiedzialności, procedury reagowania i gromadzenie dowodów
A.17	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	mechanizmy kontrolne wymagające planowania ciągłości działania, procedur, weryfikacji i przeglądu oraz redundancji IT
DOMENY ZWIĄZANE Z KWESTIAMI ORGANIZACYJNYMI		
A.5	Polityki bezpieczeństwa informacji	kontrole sposobów, w jaki polityki są pisane i przeglądane
A.6	Organizacja bezpieczeństwa informacji	kontrola przydzielania obowiązków; obejmuje również sterowanie urządzeniami mobilnymi i telepracą
A.8	Zarządzanie aktywami	kontrole związane z inwentaryzacją aktywów i dopuszczalnym wykorzystaniem; również do klasyfikacji informacji i obsługi mediów
A.15	Relacje z dostawcami	kontrole dotyczące tego, co należy uwzględnić w umowach i jak monitorować dostawców

Punkt	Nazwa	Opis
DOMENY ZWIĄZANE Z KWESTIAMI ZAGADNIEŃ PRAWNYCH		
A.18	Zgodność	kontrole wymagające identyfikacji obowiązujących przepisów i regulacji, ochrony własności intelektualnej, ochrony danych osobowych oraz przeglądów bezpieczeństwa informacji
DOMENY ZWIĄZANE Z KWESTIĄ ZASOBÓW LUDZKICH		
A.7	Bezpieczeństwo zasobów ludzkich	kontrole przed zatrudnieniem, w trakcie i po zatrudnieniu
DOMENY ZWIĄZANE Z KWESTIAMI BEZPIECZEŃSTWA FIZYCZNEGO		
A.11	Bezpieczeństwo fizyczne i środowiskowe	kontrole określające bezpieczne obszary, kontrole wejścia, ochrona przed zagrożeniami, bezpieczeństwo sprzętu, bezpieczna utylizacja, polityka czystego biurka i czystego ekranu itp.

Źródło: Opracowanie własne na podstawie (Stinet, 2023)

W domenach przedstawionych w Tabeli 2 zawiera się 114 punktów kontroli bezpieczeństwa, które należy wdrożyć, by zapewnić bezpieczeństwo informacji i zorganizować je w system w każdej organizacji.

Biorąc pod uwagę opinie audytorów zewnętrznych ISO 27001, podejście do bezpieczeństwa informacji w pracy zdalnej przed i po wdrożeniu normy ISO 27001 może ulec znaczącym zmianom.

Przed wdrożeniem normy ISO 27001 przez organizację, w kontekście bezpieczeństwa informacji pracy zdalnej, można zauważyć często występujące następujące aspekty:

- Brak spójnych standardów. Przed wdrożeniem normy ISO 27001 firmy mogą operować bez klarownych standardów bezpieczeństwa informacji dla pracy zdalnej. Często w organizacji brakuje spójnych procedur i polityk tego bezpieczeństwa.
- Reaktywne podejście. Bez normy ISO 27001 podejście do bezpieczeństwa informacji w pracy zdalnej może być bardziej reaktywne niż proaktywne. Firmy mogą reagować na incydenty, zamiast zapobiegać im.
- Niedostateczna świadomość zagrożeń. Przed wdrożeniem normy świadomość pracowników na temat zagrożeń bezpieczeństwa informacji w pracy zdalnej często jest wręcz znikoma, co może prowadzić do większej podatności na ataki.

Po wdrożeniu normy ISO 27001 zauważalne pozytywne aspekty to:

- Zdefiniowane standardy i procedury. Po wdrożeniu normy ISO 27001 firma posiada spójne standardy, procedury i wytyczne dotyczące bezpieczeństwa informacji w pracy zdalnej, co zapewnia strukturalne podejście do zarządzania ryzykiem.
- Proaktywne podejście. Norma ISO 27001 promuje podejście proaktywne do bezpieczeństwa informacji. Organizacje stają się bardziej zdolne do przewidywania potencjalnych zagrożeń i podejmowania środków zapobiegawczych.

– Zwiększona świadomość. Wdrożenie normy ISO 27001 prowadzi do zwiększenia świadomości pracowników na temat zagrożeń i procedur bezpieczeństwa informacji w pracy zdalnej poprzez szkolenia i edukację.
– Monitorowanie i doskonalenie. Norma ISO 27001 wymaga monitorowania i doskonalenia systemów bezpieczeństwa informacji. Po wdrożeniu organizacje prowadzą regularne rewizje i aktualizacje, by dostosować się do zmieniających się zagrożeń.

W rezultacie wdrożenie normy ISO 27001 w pracy zdalnej prowadzi do bardziej ustrukturyzowanego, proaktywnego i świadomego podejścia do bezpieczeństwa informacji, co z kolei zmniejsza ryzyko i zwiększa efektywność działań w tym zakresie.

Autorzy opracowali tzw. autorską listę pytań, możliwą do wykorzystania przy sprawdzaniu systemu zarządzania bezpieczeństwem informacji. Ze względu na fakt, że punktów kontrolnych jest 114, w Tabeli 3 przedstawiono jedynie wybrane punkty, do których zostały opracowane pytania. Wybrane zostały pytania z każdego zakresu:
– kwestii organizacyjnych, które przedstawione zostały przez pytania: A.5.1.1, A.6.1.2;
– zasobów ludzkich – A.7.1.2;
– IT – A.9.2.5;
– bezpieczeństwa fizycznego – A.11.2.7, A.12.6.2;
– zagadnień prawnych – A.18.2.3.

Tabela 3. Lista zawierająca pytania sprawdzające funkcjonującego w organizacji systemu zarządzania bezpieczeństwem informacji – wybrane punkty

Punkt z *Załącznika A* do normy ISO 27001	**Zakres**	**Pytanie sprawdzające**	**Odpowiedź**	**Uwagi/możliwe dodatkowe pytania/prośby**
Punkt A.5.1.1 dotyczy polityki bezpieczeństwa informacji, której celem jest zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.				
A.5.1.1	Polityka bezpieczeństwa informacji	Czy w organizacji został opracowany zbiór polityk bezpieczeństwa informacji?	□TAK	Prośba o przedstawienie.
			□NIE	
		Czy zbiór polityk bezpieczeństwa informacji został zatwierdzony przez kierownictwo?	□TAK □NIE	
		Czy zbiór polityk bezpieczeństwa informacji został zakomunikowany wszystkim pracownikom w organizacji?	□TAK	W jaki sposób? Czy jest systematycznie przypominany? Czy pracownicy mają do niego dostęp?
			□NIE	

Punkt z *Załącznika A* do normy ISO 27001	**Zakres**	**Pytanie sprawdzające**	**Odpowiedź**	**Uwagi/możliwe dodatkowe pytania/prośby**
		Czy zbiór polityk bezpieczeństwa informacji został zakomunikowany właściwym stronom zewnętrznym?	□TAK	W jaki sposób? Czy jest systematycznie przypominany?
			□NIE	
Punkt A.6.2.2 dotyczy organizacji bezpieczeństwa informacji w organizacji wewnętrznej oraz urządzeń mobilnych i telepracy. Celem jest ustanowienie struktury zarządzania bezpieczeństwem informacji w organizacji, a także zapewnienie bezpieczeństwa telepracy i stosowania urządzeń mobilnych.				
A.6.2.2	Telepraca	Czy została opracowana i wdrożona polityka oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy?	□TAK	Proszę wskazać zabezpieczenia. Czy pracownicy korzystający z telepracy są świadomi obowiązków oraz odpowiedzialności związanej z zapewnieniem bezpieczeństwa informacji?
			□NIE	
Punkt A.7.1.2 związany jest z bezpieczeństwem zasobów ludzkich, którego celem jest uzyskanie świadomości przez pracowników i kontrahentów swoich odpowiedzialności oraz obowiązków dotyczących bezpieczeństwa informacji.				
A.7.1.2	Warunki zatrudnienia	Czy umowy z pracownikami określają odpowiedzialność stron w obszarze bezpieczeństwa informacji?	□TAK □NIE	
		Czy umowy z kontrahentami określają odpowiedzialność stron w obszarze bezpieczeństwa informacji?	□TAK □NIE	
Punkt A.9.2.5 dotyczy kontroli dostępu, celem jest odpowiednie zarządzanie dostępem użytkowników do systemów i usług IT.				
A.9.2.5	Przegląd praw dostępu użytkowników	Czy właściciele aktywów IT dokonują przeglądów prawa dostępu użytkowników w regularnych odstępach czasu?	□TAK	Kiedy odbył się ostatni przegląd?
			□NIE	

DOI: 10.17512/znpcz.2024.1.09

Punkt z *Załącznika A* do normy ISO 27001	**Zakres**	**Pytanie sprawdzające**	**Odpowiedź**	**Uwagi/możliwe dodatkowe pytania/prośby**
Punkt A.11.2.7 dotyczy bezpieczeństwa fizycznego i środowiskowego organizacji. Celem jest zapobieganie utracie, uszkodzeniu, kradzieży aktywów organizacji lub zakłócenia w jej działalności.				
A.11.2.7	Bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia	Czy sprzęt jest sprawdzany, przed zbyciem lub przekazywaniem do ponownego użycia, pod kątem usunięcia wszystkich danych wrażliwych, licencjonowanych programów?	□TAK	Przez kogo sprzęt jest sprawdzany?
			□NIE	
Punkt A.12.6.2 dotyczy bezpiecznej eksploatacji środków przetwarzania informacji.				
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Czy w organizacji funkcjonują zasady instalowania oprogramowania przez użytkowników?	□TAK	Czy pracownicy są świadomi tych zasad?
			□NIE	
Punkt A.18.2.3 dotyczy zapewnienia zgodności z wymaganiami prawnymi i umownymi. Celem jest zapewnienie zgodności z politykami organizacji oraz stosowanie zasad bezpieczeństwa informacji.				
A.18.2.3	Sprawdzanie zgodności technicznej	Czy w organizacji regularnie przeglądane są systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa organizacji i standardami obowiązującymi w organizacji?	□TAK	Kiedy odbył się ostatni przegląd? Jak często dokonuje się przeglądów?
			□NIE	

Źródło: Opracowanie własne na podstawie *Załącznika A* do normy EN ISO/IEC 27001:2017

Stosowanie tzw. check listy, której wybrana część została przedstawiona w Tabeli 3, może być pomocna w procesie nie tylko implementacji standardu ISO 27001, ale również może stanowić wsparcie dla organizacji, umożliwiając m.in.:

- identyfikację kluczowych punktów w organizacji, które wymagają modyfikacji czy udoskonalenia podczas tworzenia, czy monitorowania systemu zarządzania bezpieczeństwem informacji;
- zapewnienie kompleksowego podejścia do obszarów związanych z bezpieczeństwem informacji, co zapobiega pominięciu istotnych kwestii;
- pomoc w monitorowaniu postępów w procesie wdrażania i ocenie stopnia zgodności z założeniami normy ISO 27001, jeżeli organizacja posiada wdrożony system lub zamierza go wdrożyć w przyszłości;

– ujednolicenie działań, tzn. ujednolicenie procedur i praktyk związanych z bezpieczeństwem informacji, co jest kluczowe dla spójnego wdrażania standardów w całej firmie;
– wsparcie dla procesu audytu, pomagając w sprawdzeniu zgodności i ocenie wydajności systemu zarządzania bezpieczeństwem informacji.

Ostatecznie wykorzystanie pełnej check listy opracowanej na podstawie *Załącznika A* do normy ISO 27001 stanowi praktyczne narzędzie, które ułatwia organizacjom proces implementacji standardu oraz zapewnia skuteczne zarządzanie bezpieczeństwem informacji.

Podsumowanie

Wdrażanie formy pracy zdalnej spowodowane pandemią COVID-19 uchroniło wiele przedsiębiorstw przed bankructwem, a zatrudnionych w nich pracowników przed bezrobociem. Uruchomiło tym samym proces analizy zysków i strat spowodowanych możliwością implementacji tej formy pracy w okresie po jej zakończeniu. Przed wybuchem pandemii COVID-19 w zastosowaniu formy pracy zdalnej upatrywano wiele korzyści. Zastosowanie technologii komputerowej miało obniżać koszty zatrudnienia, dając możliwości rozwoju przedsiębiorstwom, jednocześnie oferując pracownikom większą swobodę i autonomię oraz doświadczenie zawodowe (Zaręba, 2021). Obecnie coraz częściej dostrzega się, że za pracą zdalną muszą iść pewne zmiany związane z przepisami oraz z zastosowaniem odpowiedniego zarządzania bezpieczeństwem informacji.

Artykuł podkreśla kluczową rolę implementacji normy ISO 27001 w zapewnieniu skutecznego bezpieczeństwa informacji w środowisku pracy zdalnej. Główna teza artykułu opiera się na przekonaniu, że wdrażanie tej normy stanowi istotne wsparcie dla organizacji w identyfikacji, ocenie i kontroli ryzyka związanego z przechowywaniem i przetwarzaniem danych w erze zdalnych technologii komunikacyjnych.

Implementacja normy ISO 27001 staje się kluczowym punktem odniesienia dla organizacji, dając strukturalne ramy do skutecznego zarządzania bezpieczeństwem informacji w kontekście pracy zdalnej. Standard ten umożliwia określenie procedur, polityk i kontrolnych punktów, które są niezbędne dla ochrony danych, zarówno w sieciach firmowych, jak i w warunkach pracy zdalnej.

Korzyści z wprowadzenia rozwiązania opisanego w artykule nie ograniczają się jedynie do minimalizacji ryzyka. Implementacja normy ISO 27001 lub wykorzystanie tzw. check listy stanowi również krok w kierunku ustanowienia strukturalnych ram do efektywnego zarządzania bezpieczeństwem informacji, nie tylko w sieciach firmowych, ale także w warunkach pracy zdalnej. To rozwiązanie nie tylko chroni integralność, poufność i dostępność informacji, ale także przyczynia się do zwiększenia efektywności operacyjnej organizacji, utrzymania rentowności oraz zgodności z przepisami prawa. W ten sposób wprowadzenie opisanego w artykule rozwiązania stanowi niezbędny krok ku zabezpieczeniu i optymalizacji działań organizacji w nowej rzeczywistości zdalnej pracy.

Autorzy zamierzają kontynuować badania w tym kierunku, a w szczególności porównywać i analizować konkretne przypadki, jak również zastosowane praktyki związane z bezpieczeństwem informacji w pracy zdalnej pomiędzy organizacjami z różnych branż. Może to stanowić pomoc w identyfikacji specyficznych wyzwań i promowaniu najlepszych praktyk dostosowanych do konkretnych sektorów.

Literatura

Bernacka, J. (2023). Home office z perspektywy postpandemicznej – szanse i zagrożenia. Analiza pracy zdalnej w ujęciu prawnym i społecznym. *Rocznik Administracji Publicznej*, *9*, 107-134. DOI: 10.4467/24497800RAP.23.007.18303

Białas, A. (2017). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Wydawnictwo WNT.

Białogrecka, B., & Smalara, R. (2023). Praca zdalna jako nowa forma zatrudnienia w Polsce. W: M. Gasz, A. Polita (Red.), *Problemy gospodarki i rynku pracy* (s. 16-29). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu. DOI: 10.15611/2023.69.5.02

Deloitte. (2023). *Praca zdalna – regulacje prawne i podatkowe. Jak wygląda praca zdalna dziś, a jak przed pandemią?* Newsletter Strefa Pracodawcy. https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/newsletter-strefa-pracodawcy-podatki-i-prawo/praca-zdalna-a-regulacje-prawne-i-podatkowe-obecnie-i-w-przyszlosci.html (dostęp: 20.01.2024).

gov.pl. (2023). *Narodowe Standardy Cyberbezpieczeństwa*. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber (dostęp: 16.10.2023).

Kasprzak, A. (2022). *System zarządzania bezpieczeństwem informacji*. https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji (dostęp: 20.10.2023).

Kosiński, J. (2000). *Komunikacja w zarządzaniu*. Agencja Wydawnicza Placet.

Kowalska-Napora, E. (2010). Jakość informacji i jej wpływ na innowacje działań organizacji. W: T. Sikora (Red.), *Zarządzanie jakością, doskonalenie organizacji* (s. 104-117). T. II. Wydawnictwo Naukowe PTTŻ.

Kurnyta, A. (2023), Istota pracy zdalnej ze strony pracownika i pracodawcy. W: M. Gasz, A. Polita (Red.), *Problemy gospodarki i rynku pracy* (s. 30-39). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu. DOI: 10.15611/2023.69.5.03

Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Wydawnictwo Naukowe PWN.

Łaguna, Ł. (2023). *Praca zdalna. Oto sześć zasad, które zapewnią bezpieczeństwo firmowych informacji*. https://businessinsider.com.pl/prawo/opinie/praca-zdalna-co-zrobic-aby-zapewnic-bezpieczenstwo-firmowych-informacji/5rcr69k (dostęp: 02.10.2023).

MRPiPS. (2024). *Praca zdalna*. Ministerstwo Rodziny, Pracy i Polityki Społecznej. https://www.gov.pl/web/rodzina/praca-zdalna (dostęp: 20.01.2024).

Myśko, A., & Młodzik, E. (2014). Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych. *Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833. Finanse, Rynki Finansowe, Ubezpieczenia*, *72*, 107-119.

Niwiński, D., & Rzycki, A. (2023), *Zagrożenia pracy zdalnej oraz jak się przed nimi zabezpieczyć?* https://gdpr.pl/zagrozenia-pracy-zdalnej-oraz-jak-sie-przed-nimi-zabezpieczyc (dostęp: 23.01.2024).

PN-EN ISO/IEC 27000:2020-07. *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia*. Polski Komitet Normalizacyjny.

Resilia. (2022). *Co to jest norma ISO 27001 i dlaczego jest tak ważna dla organizacji?* https://resilia.pl/blog/iso-27001-czym-jest-jakie-daje-korzysci/ (dostęp: 12.11.2023).

Rudra, A. (2022). *Czym jest bezpieczeństwo informacji?* PowerDMARC. https://powerdmarc.com/pl/what-is-information-security/ (dostęp: 12.10.2023).

Sidor-Rządkowska, M. (2022). Praca zdalna i hybrydowa jako wyzwanie dla zarządzania zasobami ludzkimi w polskiej służbie cywilnej. *Studia Iuridica*, *92*, 304-317. DOI: 10.31338/2544-3135.si.2022-92.18

Stinet. (2023). *ISO 27001 – Załącznik A – dlaczego warto się z nim zapoznać?* https://stinet.pl/iso-27001-zalacznik-a-dlaczego-warto-sie-z-nim-zapoznac%E2%80%A8/ (dostęp: 04.11.2023).

Werner, J., & Szczepaniuk, E. (2016). Bezpieczeństwo informacyjne organizacji. *Zeszyty Naukowe AON*, *4*(105), 167-187.

Zaręba, I. (2021). Implementacja pracy zdalnej – identyfikacja głównych obszarów badawczych. *Przegląd Organizacji*, *10*(981), 19-26. DOI: 10.33141/po.2021.10.03

Wkład autorów: Anna Rychły-Lipińska – 50%; Wiesław Kamiński – 50%.

Konflikt interesów: Brak konfliktu interesów.

Źródła finansowania: Brak finansowania.

INFORMATION SECURITY IN THE ERA OF REMOTE WORKING AND THE ROLE OF THE ISO 27001:2017 MODEL

Abstract: Information security in remote working is a key area requiring attention and action by employers. The article analyses elements of this issue, focusing on the challenges related to remote working and the role of ISO 27001:2017 in information security management. The publication draws attention to the increasing importance of remote working, which prompts reflection on data security. The ISO 27001:2017 standard was used to support information security management in an organisation. The research methods used in the article are a literature review and the Delphi method. The literature review included an analysis of information security in remote working, security attributes, the ISO 27001:2017 standard and information security management. Through the use of the Delphi method, the opinions of experts, including ISO 27001:2017 auditors and information security inspectors from SMEs, were used. The article began with a discussion of the essence of information security, highlighting its importance for data protection. Then information security attributes such as confidentiality, integrity and data availability were analysed in the context of remote working. The article also presents the challenges employers face regarding information security when working remotely. The rest of the article discusses the information security management system model - ISO 27001:2017, presenting the author's checklist to support the assessment of the effectiveness of information security management systems.

Keywords: information security attributes, information security, ISO 27001:2017, remote working, systemic management of information security