INNOWACYJNA GMINA

Audyt bezpieczeństwa informacyjnego

pod redakcją
Mirosława Hajdera

Rzeszów 2018

Mirosław Hajder, Lucyna Hajder

INNOWACYJNA GMINA

Audyt bezpieczeństwa informacyjnego

Redakcja naukowa serii: Mirosław Hajder

Rzeszów, 2018

Recenzja naukowa:
Prof. dr hab. Sergii Kryvyi,
Prof. dr hab. Heorhii Loutskii

Redakcja naukowa serii:
Mirosław Hajder

Autorzy:
Mirosław Hajder – Katedra Elektroniki i Telekomunikacji, Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie
Lucyna Hajder – Wydział Inżynierii Metali i Informatyki Przemysłowej, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

Redakcja i korekta:
Agnieszka Hajder

Projekt okładki i stron tytułowych:
Andrii Sydorak, Przemysław Nycz, Lucyna Hajder

Skład, łamanie i przygotowanie do druku:
Piotr Hajder, Mariusz Nycz

Pomysł monografii:
Mirosław Hajder, Janusz Kolbusz, Mariusz Nycz

ISBN 978-83-64286-65-0

Wydawca:
Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie
35-225 Rzeszów, ul. Sucharskiego 2
www.wsiz.rzeszow.pl
e-mail: wsiz@wsiz.rzeszow.pl
Księgarnia internetowa: www.ksiegarnia.wsiz.pl

WYŻSZA SZKOŁA
INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

SPIS TREŚCI

Wstęp

Doświadczeni nauczyciele akademiccy mówią w żartach, że praca na uczelni byłaby fantastyczna, gdyby nie zajęcia. Niestety, podobne odczucia towarzyszą użytkownikom Internetu. Usługi oferowane przez sieć już od wielu lat są częścią naszej codzienności, bez której trudno sobie wyobrazić nasze sprawne funkcjonowanie. Jednak Internet, podobnie jak praca dydaktyczna ma swoją drugą, ciemniejszą stronę. Brak ograniczeń w komunikowaniu się, będący największą zaletą Internetu stał się jednocześnie jego przekleństwem. Informacja, która trafia do sieci staje się w niej nieśmiertelna, żyje własnym życiem, bez względu na to, czy jest ona prawdziwa czy też nie.

Ogólnodostępność i nieśmiertelność informacji stały się powodem wielu nieszczęść. Walka z osobami wykorzystującymi Internet do anonimowego szerzenia fałszywych opinii krzywdzących inne osoby jest trudna, lecz nie niemożliwa. Jedną z najskuteczniejszych metod walki z tą patologią jest wdrażanie rygorystycznych zasad przetwarzania danych osobowych tak, aby nie trafiały one do osób niepowołanych, a także ograniczenie dopuszczalności umieszczania w przestrzeni publicznej informacji o innych, bez ich zgody. Doskonałym przykładem takich działań jest wdrożenie w Polsce *Rozporządzenia 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*. Dokument ten, potocznie nazywany RODO, precyzyjnie określa zasady postępowania z naszymi danymi i wizerunkiem przez podmioty je przetwarzające.

Powyższy akt normatywny jest nie pierwszym i zapewne nieostatnim dokumentem poświęconym bezpieczeństwu gromadzonej, magazynowanej, przetwarzanej, przesyłanej i udostępnianej informacji. Do chwili obecnej, pomimo wycofania przez Polski Komitet Normalizacyjny stosowana jest norma *PN-ISO/IEC 15408 Technika informatyczna -- Techniki zabezpieczeń -- Kryteria oceny zabezpieczeń informatycznych*. Składa się ona z trzech części zatytułowanych: *Wprowadzenie i model ogólny*, *Komponenty funkcjonalne zabezpieczeń* oraz *Wymagania uzasadnienia zaufania do zabezpieczeń.* Obecnie, najszerzej wykorzystywaną serią standardów poświęconych bezpieczeństwu informacji jest złożona z kilkudziesięciu niezależnych dokumentów norma ISO/IEC 27000.

Niestety, w wyniku wieloletnich zaniedbań w obszarze bezpieczeństwa informacji, wdrożenie RODO, podobnie jak wcześniej norm ISO, okazało się wielkim wyzwaniem dla polskich przedsiębiorstw i samorządów. Dlatego, zespół redakcyjny *Innowacyjnej Gminy* zdecydował się poświęcić kolejne wydanie monografii tematom bezpieczeństwa informacyjnego. Szczególnym obszarem zainteresowania autorów będzie nie techniczne, a prawno-organizacyjne zapewnienie bezpieczeństwa.

Nasza monografia nie jest opisem którejkolwiek z ustaw, norm czy rozporządzeń – w tym temacie napisanych zostało już wiele doskonałych publikacji [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]. Autorzy postawili przed sobą ambitne zadanie pomocy osobom odpowiedzialnym w przedsiębiorstwie za bezpieczeństwo informacyjne w kreowaniu stosownej polityki. Dlatego, w jej obu tomach skoncentrowano się na przedstawieniu najważniejszych kroków, które powinien podjąć odpowiedzialny personel, w celu zapewnienia bezpieczeństwa swoich zasobów informacyjnych. Nie ulega wątpliwości, że działaniem przysparzającym najwięcej kłopotów jest opracowanie i wdrożenie Polityki bezpieczeństwa informacyjnego – zestawu instrukcji i regulaminów określających postępowanie z zasobami informacyjnymi przedsiębiorstwa. Aby rozwiązania zaprezentowane w monografii oparte były na solidnych podstawach, zdecydowano się opisać politykę zgodną z normą ISO/IEC 27001. Każdy z rozdziałów został poświęcony wybranemu problemowi bezpieczeństwa, jawnie występującemu w normie. Rozpoczynają się one od analizy występującego problemu bezpieczeństwa, kończą zaś prezentacją rozbudowanego dokumentu (polityki, regulaminu, instrukcji), uwzględniającego większość wymagań bezpieczeństwa.

Zadaniem administratora bezpieczeństwa informacyjnego (lub inspektora ochrony danych) będzie dostosowanie wzoru polityki lub regulaminu do własnych, specyficznych potrzeb. Aby odróżnić analizę od przykładów, te ostatnie wyróżniono inną czcionką i numeracją. Przedstawione dokumenty były zweryfikowane przez kilkudziesięciu użytkowników instytucjonalnych. Dzięki ich pomocy zostały one dostosowane do aktualnych realiów ochrony.

Chociaż w prezentowanej książce dominują tematy związane z polityką bezpieczeństwa informacyjnego, rozpoczyna ją jednak rozdział będący opisem procedury audytu, będącej podstawą najważniejszych działań w obszarze bezpieczeństwa informacyjnego. Audyt może być ukierunkowany na wiele różnych uregulowań bezpieczeństwa systemów informacyjnych. Procedury przytoczone w książce mają uniwersalny charakter i nie dotyczą bezpośrednio żadnego z aktów normatywnych definiujących sposób audytowania – zaprezentowany został autorski scenariusz prowadzenia audytu.

Podobnie jak wcześniejsze wydania Innowacyjnej Gminy, również niniejszy tom oferowany jest czytelnikom nieodpłatnie. Jednocześnie informujemy, że wszystkie dotychczasowe tomy naszej monografii cyklicznej są zdeponowane na ogólnodostępnych portalach z publikacjami naukowymi (Research Gate, Google Scholar), a także w bibliotece internetowej wydawnictwa Wyższej Szkoły Informatyki i Zarządzania z siedzibą w Rzeszowie.

Autorzy

Rozdział 1

Podstawy prowadzenia audytu bezpieczeństwa informacyjnego

1.1. Pojęcia bazowe bezpieczeństwa informacyjnego

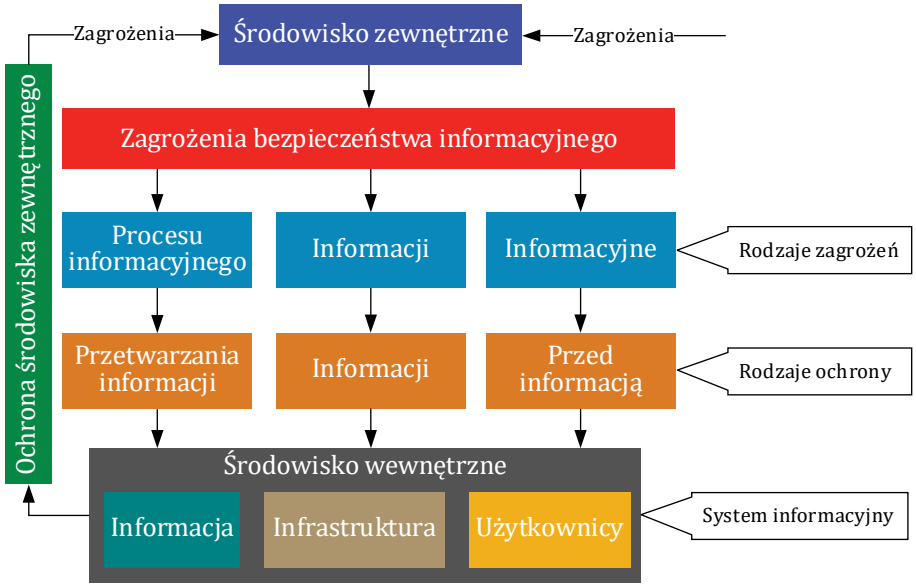
Definicje terminu *bezpieczeństwo informacyjne* (BI) zmieniały się wraz z upływem czasu. Zazwyczaj mają one charakter formalny i są opracowywane przez organizacje standaryzujące. Zgodnie z jedną z wcześniejszych definicji *bezpieczeństwo informacyjne, to niewrażliwość informacji oraz utrzymującej ją infrastruktury na przypadkowe lub zamierzone działania o charakterze naturalnym bądź wymuszonym, które mogą przynieść nieakceptowalny uszczerbek podmiotom relacji informacyjnych, w szczególności właścicielom i użytkownikom informacji lub utrzymującej je infrastrukturze*. Jawne pojawienie się infrastruktury i użytkowników trzecich w określeniu BI nastąpiło stosunkowo późno. Głównym elementem wcześniejszych definicji była troska o zapewnienie bezpieczeństwa zasobów informacyjnych. Przełomem w tym względzie było ujawnienie nowej klasy robaków internetowych atakujących instalacje przemysłowe, a rezydujących w sterownikach PLC [15], [16]. Takie wirusy jak Stuxnet, Flame, Duqu, Gauss i in. były w istocie ukierunkowane na niszczenie infrastruktury sieciowej, czy szerzej przemysłowej.

Poniżej przedstawiamy jeszcze trzy alternatywne definicje BI. Według pierwszej z nich, popularnej w literaturze rosyjskojęzycznej, bezpieczeństwo informacyjne to *stan systemu, przy którym jest on zdolny przeciwdziałać destabilizującemu wpływowi czynników wewnętrznych i zewnętrznych, funkcjonowanie bezpiecznego SI nie stwarza zagrożeń dla niego samego oraz środowiska zewnętrznego*. Podobną w zawartości definicję propaguje Amerykański Narodowy Instytut Standardów (ANSI). Zgodnie z nią BI to *stan ochrony życiowo ważnych interesów społeczeństwa i państwa w środowisku informacyjnym, od zagrożeń wewnętrznych i zewnętrznych*.

Obie powyższe definicje BI są na tyle ogólne, że można wyróżnić w nich następujące elementy składowe: bezpieczeństwo informacji, infrastruktury oraz środowiska zewnętrznego. Zapewnianie *bezpieczeństwa informacji* ma na celu ochronę informacji przetwarzanej w systemie przed zagrożeniami wewnętrznymi i zewnętrznymi. *Bezpieczeństwo infrastruktury* zapewnia ochronę programowych i sprzętowych elementów systemu informacyjnego (SI) przed zagrożeniami wewnętrznymi i zewnętrznymi. Z kolei *bezpieczeństwo środowiska zewnętrznego* ma zagwarantować ochronę osób i podmiotów trzecich przed zagrożeniami informacyjnymi rozpatrywanego systemu. Zgodnie ze współczesną interpretacją, zagrożenia bezpieczeństwa dotyczą: procesu informacyjnego (związane z procesem gromadzenia, przetwarzania i magazynowania informacji), samej informacji (dotyczące ataków

na gromadzoną, przetwarzaną i magazynowaną informację) oraz zagrożenia przez informację (wiążące się z posiadaniem i wykorzystaniem informacji).

Alternatywną klasyfikację zagrożeń bezpieczeństwa informacyjnego przedstawiono graficznie na rys. 1.1.



Rys. 1.1. Klasyfikacja zagrożeń bezpieczeństwa informacyjnego

Zagrożenia środowiska zewnętrznego względem SI zazwyczaj pochodzą z niego samego. Mogą pochodzić również z systemu informacyjnego i dlatego jego system bezpieczeństwa zostaje wyposażony w ochronę środowiska zewnętrznego. Środowisko wewnętrzne tworzy system informacyjny, którego zasobami są: gromadzona, przetwarzania i udostępniane informacja; infrastruktura programowo-sprzętowa oraz użytkownicy. Podstawowym zadaniem podsystemu bezpieczeństwa SI jest jego ochrona przed szkodliwym wpływem na jego zasoby, jak również ochrona środowiska zewnętrznego przed szkodliwym działaniem ze strony jego samego. Zagrożenia charakterystyczne dla systemów informacyjnych najczęściej dzielimy na: *zagrożenia procesu informacyjnego* tj. działań związanych z tworzeniem i przetwarzaniem informacji; *zagrożenia informacji* pojawiające się na etapie jej magazynowania oraz *zagrożenia informacyjne* będące skutkiem niepoprawnego udostępniania informacji [17], [18], [19]. Powyższe zagrożenia implikują wykorzystywane rodzaje ochrony. Ochrona *przetwarzania informacji* dotyczy samego procesu informacyjnego, w którym poufne mogą być nie tylko dane, ale również sposób ich obróbki. Ochrona informacji wiąże się z potrzebą zachowania jej poufności. Chociaż w informatyce do tego celu oprócz kryptografii stosuje się również rozgraniczanie dostępu i steganografię, to właśnie metody kryptograficzne są głównym sposobem ochrony [20], [21]. Rozgraniczanie dostępu, będące standardową usługą

systemu operacyjnego powszechnie uważa się za mało skuteczne, a jego neutralizację za względnie prostą [22], [23], [24]. Z kolei steganografia jest raczej techniką niszową, przeznaczoną do zabezpieczenia wąskiego zakresu typów przesyłanych informacji, a jej przydatność do ochrony w skali masowej – znikoma [25], [26], [27].

Z bezpieczeństwem informacyjnym wiąże się kilka podstawowych terminów, których brzmienie przytoczymy poniżej. Zgodnie z [28] dla wybranych dokonamy szerszej analizy na bazie literatury i doświadczeń autorów.

System informacyjny (SI) według Normy to aplikacje, usługi, aktywa technik informacyjnych lub inne komponenty przetwarzające informacje. Systemy informacyjne stanowią dzisiaj nieodłączny element dowolnej struktury zarządzającej przedsiębiorstwem. Nie ma jednolitej definicji SI, który w ogólnym przypadku jest *zbiorem zasobów technicznych, programowych, organizacyjnego i osobowych, których zadaniem jest zagwarantowanie użytkownikom SI dostępu do informacji*. Zgodnie z inną, popularną definicją, system informacyjny to *zbiór danych zawartych w bazach oraz technologii informatycznych i środków technicznych zapewniających jej przetwarzanie*. Inna często wykorzystywana definicja zakłada, że system informacyjny to *kompleks, obejmujący sprzęt obliczeniowy i komunikacyjny, oprogramowanie, narzędzia lingwistyczne oraz zasoby informacyjne, a także systemowy zapewniający wsparcie dla dynamicznego modelu fragmentu świata rzeczywistego, w celu zaspokojenia potrzeb informacyjnych użytkowników*. Zgodnie ze standardem ISO/IEC 2382-1, system informacyjny, to *narzędzie przetwarzania informacji, działające wspólnie z zasobami organizacyjnymi, takimi jak ludzie, środki techniczne oraz finansowe, które dostarczają i dystrybuują informacje*.

Systemy informacyjne mogą się bardzo różnić pod względem swoich funkcjonalności, architektury oraz metod i sposobów realizacji, w zależności od planowanego zastosowania. Jednakże, można wyróżnić, co najmniej dwie właściwości, wspólne dla wszystkich SI:

a. Każdy system informatyczny jest przeznaczony do zbierania, przechowywania i przetwarzania informacji. Dlatego, bazą dowolnego SI jest środowisko przetwarzania, przechowywania i dostępu do danych. Środowisko to, musi zapewnić niezawodność i wydajność dostępu oraz niezbędne obszary zastosowania systemu informacyjnego. Zauważmy, że w klasycznych komputerowych systemach informacyjnych istnienie takiego środowiska jest nieobowiązkowe;

b. Systemy informacyjne są zorientowane na użytkownika, którym może być przykładowo: urzędnik bankowy, pracownik magazynu, księgowy lub urzędnik administracji przedsiębiorstwa. Zazwyczaj, osoby takie nie mają dostatecznej wiedzy z obszaru informatyki, która jest dla nich wyłącznie narzędziem pracy zawodowej. Dlatego, każdy system informacyjny musi zostać wyposażony w prosty, wygodny, łatwo przyswajalny interfejs komunikacyjny, udostępniający użytkownikowi wszystkie funkcje niezbędne do jego

wykorzystania. Jednocześnie, interfejs ten nie powinien dawać mu możliwości wykonywania jakichkolwiek działań, które mogłyby zaszkodzić SI.

Konkretne zadania, które powinny być rozwiązywane przez system informatyczny, zależą od konkretnego obszaru aplikacyjnego, dla którego SI jest przeznaczony. Obszary zastosowania technologii informacyjnych są zróżnicowane. Począwszy od bankowości, przez ubezpieczenia, medycynę, transport, edukację, administrację publiczną, produkcję oprogramowania itd. Obecnie, trudno znaleźć obszar aktywności człowieka, w którym można byłoby obejść się bez systemów informacyjnych. Z drugiej jednak strony, zadania rozwiązywane przez konkretny system informacyjny mogą bardzo różnić się pomiędzy sobą. Przykładowo, trudno jest znaleźć wspólne cechy rozwiązań tworzonych przez bankowe systemy informacyjne, systemy medyczne lub logistyczne.

Wszystkie rozważane powyżej systemy łączy jeden zasadniczy fakt: kierownictwo firm odczuwa potrzebę posiadania rzetelnej informacji na temat wszelkich aspektów działalności firmy oraz jej otoczenia. Informacje te wykorzystywane są w procesie podejmowania decyzji. Od tego zależy jakość zarządzania firmą, możliwość efektywnego planowania jej działalności, przetrwanie w warunkach ostrej walki konkurencyjnej. Przy tym krytycznie ważną jest przejrzystość i prostota prezentacji informacji, szybkość otrzymania nowych rodzajów wiedzy, możliwość analizy aktualnych i historycznych danych.

Zgodnie z Normą *Audyt* to systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt wykonywany jest przez eksperta z dziedziny ochrony informacji, posiadającego prawo prowadzenia działań w obszarze bezpieczeństwa środków programowo-technicznych i metod ochrony informacji. Szczegółowe opisy różnych typów audytu zawarto w dalszej części monografii.

Uwierzytelnienie (autentyfikacja) to pewność, że deklarowana charakterystyka podmiotu jest poprawna. W praktyce autentyfikacja ma nieco szersze znaczenie. *Po pierwsze*, to sprawdzenie przynależności do podmiotu dostępu przedstawionego przez niego identyfikatora. *Po drugie*, to sprawdzenie identyfikacji podmiotu (sprawdzenie autentyczności jego tożsamości), urządzenia bądź innego komponentu systemu, wykonywane zazwyczaj w celu podjęcia decyzji o zezwoleniu na dostęp do zasobów systemu. *Po trzecie*, sprawdzanie integralności przechowywanych lub przekazywanych danych w celu wykrycia ich niedozwolonej modyfikacji. *Po czwarte*, ustanowienie lub potwierdzenie uwierzytelniania osób, środków programowych lub technicznych, elementów baz danych bądź przekazywanych wiadomości.

Tożsamość możemy potwierdzić na podstawie: **a.** Posiadanej przez nas wiedzy (hasła, kodu PIN itp.); **b.** Naszego stanu posiadania (karta, fizyczny klucz itp.), **c.** Naszych nieprzenaszalnych cech osobowych (linie papilarne, rysunek tęczówki oka); **d.** Naszych cech behawioralnych (sposobu pisania na klawiaturze, składania podpisu odręcznego na touchpadzie itp.).

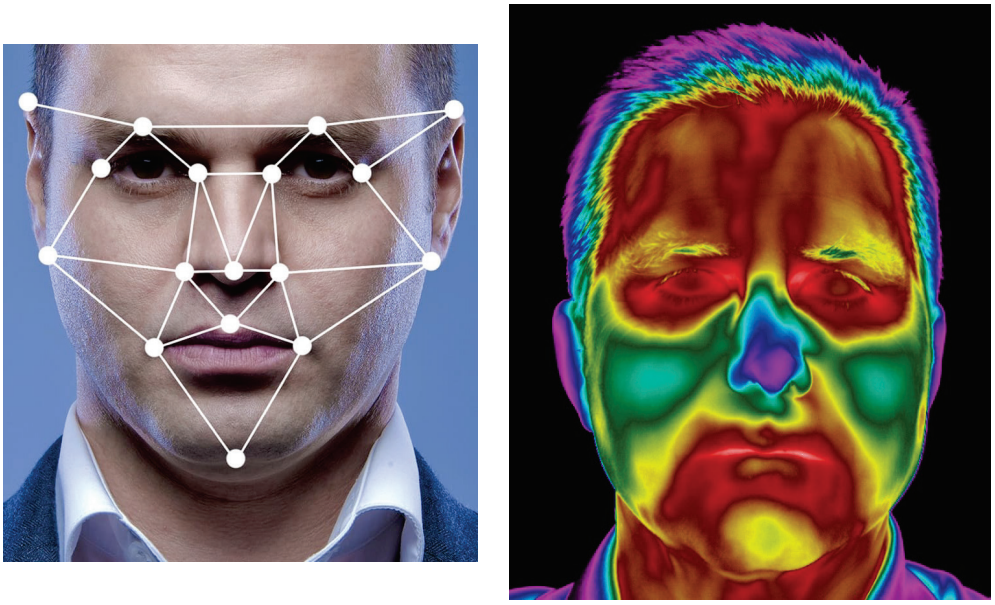
Jeżeli do uwierzytelnienia stosujemy tylko jeden z wymienionych sposobów, nazywamy go jednoskładnikowym, jeżeli kilka – wieloskładnikowym. Systemy wieloskładnikowe bardziej obciążają użytkownika (eksploatacja systemu informacyjnego staje się mniej przyjazna), gwarantując przy tym wyższy poziom bezpieczeństwa. Ten rodzaj identyfikacji można podzielić na dwie kategorie: **a.** Identyfikacja użytkownika osobowego, oparta na bezpośrednim lub pośrednim (za pomocą środków komunikacji) kontakcie z nim samym. Zazwyczaj bazuje na zastosowaniu technik biometrycznych (linie papilarne, biometria naczyniowa, analiza behawioralna) bądź weryfikacji stanu wiedzy osoby uwierzytelnianej (podanie kodu PIN, hasła itp.). Nie ulega wątpliwości, że połączenie obu ww. sposobów uwierzytelniania jest celowe i zapewnia bardzo wysoki poziom bezpieczeństwa; **b.** Identyfikacja użytkownika nieożywionego (programu, interfejsu, urządzenia), która najczęściej opiera się na zastosowaniu metod kryptograficznych.

Szerszej uwagi wymagają metody biometryczne uwierzytelniania opisane m. in. w [29], [30], [31], [32]. Dzięki nieprzenaszalności unikalnych cech biologicznych uwierzytelnianego podmiotu metody biologiczne należy uważać za najskuteczniejsze z dostępnych. Ponadto, sposób ich realizacji jest zazwyczaj trywialnie prosty, co dodatkowo zwiększa ich atrakcyjność. Jedną z metod biometrycznych, pozornie identyczną ze sposobem wykorzystywanym codziennie przez człowieka, jest uwierzytelniane na podstawie obrazu twarzy. Identyfikując znaną nam wcześniej osobę zwracamy uwagę na szczegóły związane z kształtem i usytuowaniem jej ust, oczu, brwi, nosa czy podbródka. Cały proces rozpoznawania zachodzi w płacie skroniowym mózgu i ma charakter działania podświadomego. Mimo pewnych podobieństw, metody wykorzystywane w identyfikacji komputerowej różnią się w sferze realizacyjnej od tych stosowanych przez człowieka. Obecnie, najszerzej stosuje się dwie metody, z których pierwsza opiera się na określaniu wartości współczynników matematycznych określanych na postawie kształtu twarzy. Druga natomiast wykorzystuje termogram twarzy. Pierwsza z metod funkcjonuje w oparciu o program komputerowy analizujący obraz z kamery nakierowanej na twarz interesującej nas osoby.

Program wydziela na twarzy niezależne obiekty (brwi, oczy, nos, usta), określa ich charakterystyki i wzajemne rozmieszczenie, następnie oblicza wartości relacji matematycznych wyliczanych na podstawie rozmiaru kształtu i rozmieszczenia obiektów twarzy. Ich wartości jednoznacznie określają konkretną twarz. Ponieważ identyfikacja osoby może odbywać się w naturalnym środowisku, analizowany obiekt może poruszać się i znajdować się pod różnym kątem i różnej odległości w stosunku do śledzącej go kamery. Dlatego większość profesjonalnych systemów identyfikacji na bazie obrazu z kilku kamer buduje trójwymiarowy obraz ludzkiej twarzy. Pomimo konieczności wykorzystania kilku kamer, systemy takie są tanie i proste w instalacji i eksploatacji, co spowodowało ich szerokie zastosowanie. Podstawową wadą tych rozwiązań jest umiarkowana dokładność, która może zostać poprawiona przez zastosowanie większej ilości kamer. Zauważmy również, że przez cały czas identyfikacji badana osoba może celowo zmieniać wyraz twarzy (różniący się od tego zapisanego w bazach), odwracać głowę

od kamer lub ukrywać twarz w kominiarce, ewentualnie pod kapturem. Nie bez znaczenia pozostaje również makijaż, np. zmiana kształtu brwi przez kobietę może spowodować, że nie zostanie ona rozpoznana przez system identyfikacji. Również identyfikacja bliźniaków, szczególnie jednojajowych może być niemożliwa z wiadomych powodów. Przykład odległości mierzonych w procesie identyfikacji twarzy został pokazany na rys. 1.1.a. W rzeczywistych pomiarach określenie wszystkich pokazanych odległości może okazać się niemożliwe.

a. b.



Rys. 1.2. Identyfikacja osoby na podstawie jej twarzy: a. Przykład odległości mierzonych na twarzy identyfikowanej osoby [33]; b. Termogram twarzy [34]

Alternatywna technologia identyfikacji osoby na podstawie twarzy korzysta z termogramu. Twarz człowieka jest miejscem, gdzie przepływ krwi w tętnicach jest szczególnie intensywny. Ponieważ krew niesie ze sobą ciepło, wykorzystując kamerę termowizyjną można zarejestrować rozkład temperatur na twarzy identyfikowanej osoby. Rozmieszczenie tętnic jest różne nawet u bliźniaków jednojajowych, co sprawia, że skuteczność metody jest wysoka. Niestety, znaczny koszt kamery termowizyjnej ogranicza zastosowanie tej metody do systemów profesjonalnych. Przykład termogramu pokazano na rys. 1.1.b.

Szerokie rozpowszechnienie uzyskały metody oparte na analizie ludzkiego oka, w szczególności siatkówki i tęczówki. Metody bazujące na określeniu rysunku tworzonego przez naczynia krwionośne rozlokowane na dnie oka są stosowane stosunkowo długo. Podobnie wcześnie zastosowanie znalazły rozwiązania oparte na pochłanianiu i odbijaniu światła przez samą siatkówkę. Elementarna znajomość fizjologii i anatomii podpowiada, że sfałszowanie obu obrazów jest praktycznie niemożliwe. Dlatego metody uważane są za jedne z najskuteczniejszych. Jednak

starsze metody, oparte o analizę siatkówki oka posiadają szereg wad, które ograniczają zakres ich wykorzystania. Po pierwsze, chociaż skanowanie odbywa się z zastosowaniem promieniowania niewidzialnego, mogą towarzyszyć mu nieprzyjemne odczucia mające podłoże psychiczne, potęgowane koniecznością patrzenia w ściśle określony punkt. Po drugie, analiza wyniku skanowania jest czasochłonna – może trwać kilkadziesiąt sekund – co powoduje oczywisty dyskomfort. Po trzecie, w przypadku chorób wzroku obraz siatkówki ulega zmianie i identyfikacja osób cierpiących na takie dolegliwości może być utrudniona lub wręcz niemożliwa. Opisane wyżej metody znalazły ograniczone zastosowanie w obronności.

Znacznie lepsze wyniki można uzyskać korzystając z rysunku rozmieszczonego na *tęczówce* oka. W oparciu o specjalistyczne oprogramowanie kamera wykonuje zdjęcie twarzy identyfikowanej osoby, którego program wyróżnia tęczówkę, na podstawie której wykonywana jest identyfikacja. Metoda jest skuteczna dla niedowidzących, nie wywołuje dyskomfortu u osób poddawanych badaniu, jest tania i dokładna w działaniu.

Inne znajdujące umiarkowane zastosowanie metody identyfikacji opierają się na analizie *kształtu dłoni*. Pierwsza z nich, za pomocą kamery i zestawu diod LED buduje trójwymiarowy obraz, który następnie jest następnie porównywany z danymi referencyjnymi. Niezawodność metody jest względnie wysoka, a jej wadą jest wrażliwa na uszkodzenia mechaniczne konstrukcja skanera. Wielu autorów podkreśla, że czas życia urządzenia jest nieakceptowalnie krótki [18], [32]. Druga z metod bada termogram dłoni i jest identyczna do opisanej wcześniej analizy twarzy identyfikowanej osoby.

Najszerzej wdrożoną i wykorzystywaną metodą identyfikacji biometrycznej jest analiza *odcisków palca*. Na rynku dostępne są cztery typy urządzeń skanujących. Pierwsza z metod korzysta ze *skanerów optycznych*, których działanie jest bardzo podobne do zasad pracy tradycyjnych skanerów. Zaletą takich rozwiązań jest niska cena całej instalacji, wady to: zależność pomiaru od stanu skóry i czystości samego skanera. Skutkiem powyższych uwarunkowań jest niska dokładność identyfikacji, w efekcie metoda nie jest zalecana do wykorzystania. Druga z metod oparta jest na zastosowaniu *skanerów elektrycznych*. Użytkownik dotyka palcem płyty złożonej z kilkuset tysięcy krzemowych okładzin kondensatorów, zapewniających skanowanie z dokładności powyżej 600 dpi. Ponieważ potencjał pola elektrycznego wewnątrz kondensatora zależy od odległości między płytkami, jego mapa powtarza brodawkowaty wzór palca. Pole elektryczne jest mierzone, a wyniki są przekształcane w ośmiobitowy obraz rastrowy. Zalety tej technologii: wysoka dokładność wyniku; niewrażliwość na zanieczyszczenia; wysoka miniaturyzacja. Najważniejsze wady to: wysoki koszt wynikający ze skomplikowania technologicznego, wrażliwość na parametry otoczenia, w tym wibracje i wstrząsy; niemożność pracy w obecności silnego promieniowania elektromagnetycznego.

Trzecia technologia identyfikacji odcisków palców wykorzystuje materiał polimerowy wrażliwy na różnicę pola elektrycznego pomiędzy grzbietami i zagłębieniami skóry. Zasada działania takich urządzeń podobna jest do skanerów elektrycznych. Charakteryzuje je jednak szereg zalet. Po pierwsze, koszt wytworzenia czujnika polimerowego jest setki razy niższy od krzemowego. Po drugie, skaner jest wytrzymały mechanicznie, ma niewielkie rozmiary i może być umieszczony praktycznie w każdym urządzeniu elektronicznym. Czwarty, ostatni typ skanerów odcisków palca, bazuje na efekcie absorbcji fal podczerwonych m. in. przez hemoglobinę będącą jednym z podstawowych składników krwi.

Uwierzytelnianie może mieć charakter lokalny lub zdalny. Uwierzytelnianie *lokalne* jest prostsze w realizacji nie wymaga bowiem komunikowania o wyniku zdalnego odbiorcy. Rozwiązania, w których uwierzytelnianie byłoby w całości realizowane zdalnie należą do rzadkości. Zazwyczaj odbiorcy przesyłany jest wyłącznie wynik operacji autentykacji.

Autentyczność według Normy to właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje.

Dostępność to właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu. Zdaniem wielu autorów jest ona najważniejszą właściwością opisującą dowolny system informacyjny. Z punktu widzenia teorii systemów, dostępność to charakterystyka jakości funkcjonowania macierzy określająca udział czasu efektywnego funkcjonowania w ogólnym czasie jej działania. Jest ona opisywana współczynnikiem K_d dostępności $K_d = t_p/(t_p + t_o)$, gdzie t_p – czas efektywnej pracy systemu, t_o – czas odtworzenia jego funkcji po awarii. Dostępność opisuje grupa parametrów, które określają częstotliwość pojawiania się oraz długości przestojów w instalacji. Wybrane z nich przedstawiamy poniżej.

Średni czas do awarii *MTBF* (ang. *Mean Time Between Failures*) to czas, który upływa pomiędzy dwoma kolejnymi awariami urządzenia, najczęściej pomiędzy wyprodukowaniem, a pierwszą awarią. Jest on określany analitycznie na podstawie charakterystyk elementów składowych urządzenia. Dla większości współczesnych złożonych systemów informacyjnych czas *MTBF* posiada wartość w zakresie od kilku do kilkudziesięciu tysięcy godzin, a w szczególnych przypadkach (systemy wojskowe) nawet kilkuset tysięcy. Nie oznacza to jednak, że system nie ulegnie awarii po kilkudziesięciu godzinach pracy.

Pewnego komentarza wymagają wartości tego parametru w systemach złożonych z wielu komponentów wykorzystujących przetwarzanie równoległe lub nadmiarowość. W systemach ze zrównoleglaniem procesu obliczeniowego do otrzymania wyniku wszystkie fragmenty systemu prowadzące proces obliczeniowy muszą być sprawne, a niesprawność chociażby jednego z komponentów czyni uzyskanie poprawnego wyniku niemożliwym. Dlatego, średni czas do awarii $MTBF_S$ systemu tej klasy określa się na podstawie czasu $MTBF_K$ komponentów, za pomocą wzoru:

$$MTBF_S = MTBF_K / n , \tag{1}$$

gdzie: n – liczba identycznych komponentów systemu. Oznacza to, że klaster obliczeniowy złożony z 1000 jednostek, z których każda posiada czas $MTBF_K$ równy jeden milion godzin, będzie charakteryzować się czasem $MTBF_S$ równym 1000 godzin, tj. nieco ponad 40 dni. Powyższe zależności opisują również systemy wieloprocesorowe.

Jeżeli w analizowanym systemie stosowane jest nadmiarowanie (redundancja), proces obliczeniowy jest prowadzony jednocześnie i niezależnie na każdej z wytypowanych jednostek obliczeniowych, a wynik może zostać odczytany z dowolnego z alternatywnych urządzeń. Wtedy wyrażenie (1) należy przekształcić do następującej postaci:

$$MTBF_S = n \cdot MTBF_K . \tag{2}$$

Pomimo tego, iż zaprezentowana definicja *MTBF* posiada charakter teoretyczny, w dużym przybliżeniu określa awaryjność systemu w warunkach idealnej eksploatacji. Początkowo, znaczenia tego parametru określane są na podstawie modeli matematycznych. Następnie, w miarę pojawiania się uszkodzeń wartość teoretyczna parametru jest modyfikowana. Kiedy czas eksploatacji danego modelu systemu jest wystarczająco długi, szacowana jest rzeczywista praktyczna wartość *MTBF*, która zawsze jest mniejsza od wartości teoretycznej.

Wyżej wymienione parametry charakteryzowały dostępność systemu informacyjnego z punktu widzenia przestojów w pracy. Zakładano przy tym, że awaria niekoniecznie musi powodować utratę przetwarzanych danych. Na przykład, uszkodzenie dowolnego z komponentów obliczeniowych nie powoduje jeszcze utraty danych, a wyłącznie ich niedostępność. Z uwagi na newralgiczny charakter danych przetwarzanych we współczesnych systemach informatycznych w znakomitej większości są one archiwizowane. Dlatego w przypadku utraty danych przechowywanych bezpośrednio w pamięci masowej systemu, zawsze istnieje możliwość ich odtworzenia z kopii zapasowej. Również z tego powodu coraz większe znaczenie przywiązuje się także do stanu niedostępności danych. Parametrem określającym ilość czasu, przez jaką system działa, zanim dozna awarii prowadzącej do niedostępności danych jest średni czas do niedostępności danych *MTTDI* (ang. *Mean Time to Data Inaccessibility*).

Uszkodzenia komponentów sprzętowych systemów, w większości przypadków, mogą być usunięte w procesie naprawy, którego podstawowym zadaniem jest przywrócenie ich pełnej wydajności i funkcjonalności. Podatność systemu do naprawy określana jest za pomocą dwóch parametrów: średniego czasu do naprawy oraz średniego czasu wyodrębnienia. Średni czas do naprawy *MTTR* (ang. *Mean Time to Repair*) to czas niezbędny na usunięcie powstałego uszkodzenia i przywrócenia nominalnych parametrów systemu. Dla współczesnych systemów obliczeniowych znajduje się on w granicach: od kilku minut do kilkudziesięciu godzin. Z kolei średni czas wyodrębnienia uszkodzenia *MTTI* (ang. *Mean Time To Isolate*) jest czasem niezbędnym do identyfikacji przyczyny uszkodzenia. Czas wyodrębnienia uszkodzenia jest fragmentem czasu naprawy, tj. czas *MTTI* zawiera się w *MTTR*. Współczesne systemy sprzętowe wyposażane są w narzędzia diagnostyki (m. in. w tzw. procesory

techniczne) pozwalające lokalizować uszkodzenia w bardzo krótkim czasie. Dlatego, przy analizie dostępności systemu, parametr *MTTI* można pomijać.

Miarą dostępności A systemu jest stosunek czasu poprawnej pracy systemu do jego czasu funkcjonowania pomiędzy kolejnymi awariami, co można przedstawić za pomocą wzoru $A = MTBF/(MTBF + MTTR)$. Parametrem odwrotnym do dostępności jest niedostępność systemu, określana jako stosunek czasu jego faktycznej niedostępności *MTTR* do czasu, dla którego określany jest parametr (*MTBF+MTTR*), co przedstawia wzór:

$$U = 1 - A = \frac{MTTR}{MTBF + MTTR}.$$

Znając wartości średniego czasu międzyawaryjnego *MTBF* oraz średniego czasu do naprawy *MTTR*, możemy określić również średnią liczbę F_A uszkodzeń w czasie t. Jest ona opisywana wzorem:

$$F_A = \frac{t}{MTBF + MTTR} \approx \frac{t}{MTBF}.$$

W systemach obliczeniowych spełniona jest nierówność *MTBF>>MTTR*. Wartość średniego czasu do naprawy przy określaniu F_A nie jest zazwyczaj uwzględniana.

Analiza dostępności w systemach informacyjnych jest zadaniem znacznie bardziej złożonym, niż wynikałoby to z powyższych rozważań. W celu udowodnienia tej tezy rozważmy urządzenia dyskowe (macierze), w których wykorzystuje się rozwarstwianie i dublowanie [35], [36]. W systemach takich utrata pojedynczego bloku danych nie powoduje jeszcze utraty jakichkolwiek informacji. W celu ich analizy wykorzystuje się średni czas do utraty danych MTTDL *(ang.* Mean Time to Data Loss). Określa on średni czasu, jaki system działa poprawnie, nim wystąpi awaria skutkująca utratą danych. Jeśli do realizacji odczytu (zapisu) wszystkie komponenty macierzy muszą być sprawne, wartość *MTTDL* jest równa wartości *MTBF* najbardziej zawodnego komponentu. Oczywistym zaleceniem dla projektantów jest maksymalizacja wartości *MTTDL* macierzy, dla niezmiennych wartości czasu *MTBF* komponentów, tworzących system. Prostym rozwiązaniem tego problemu jest zastosowanie opisywanego dalej zwielokrotniania dysków. W systemie z dublowaniem (dwa dyski przechowują tę samą informację) do utraty danych dojdzie wyłącznie w tym przypadku, kiedy uszkodzeniu ulegną jednocześnie oba dyski. Zauważmy, że taka awaria jest znacznie mniej prawdopodobna niż uszkodzenie pojedynczego dysku. W takich systemach, wysoka wartość *MTTDL* zespołu napędów dyskowych nie oznacza jednak ciągłej dostępności informacji. Awaria kontrolera, wspólnego dla wszystkich dysków, spowoduje niedostępność informacji pomimo pełnej sprawności pozostałych komponentów macierzy.

Integralność to według Normy właściwość polegająca na zapewnieniu dokładności i kompletności. Z treści definicji wynika, że informacja udostępniania wszystkim użytkownikom powinna być identyczna i niezmienna w trakcie jakiejkolwiek operacji wykonywanej nad nią.

Poufność według Normy to właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom. Często wykorzystywanym terminem jest *informacja poufna*, którą określamy informację zawierającą treści będące tajemnicą państwową, korporacyjną, handlową, lekarską, adwokacką itp. Dokładną analizę każdego z rodzajów poufności można znaleźć w literaturze [37], [18], [20], tutaj jednak ograniczymy się do krótkiej analizy tajemnicy handlowej.

Tajemnica handlowa zapewnia tryb poufności informacji, który umożliwia jej posiadaczowi w istniejących lub prawdopodobnych warunkach zwiększyć swoje przychody, uniknąć nieuzasadnionych wydatków, zachować pozycję na rynku towarów lub usług bądź uzyskać inną korzyść biznesową. Informacją będącą tajemnicą handlową może być również *tajemnica produkcji* będącą zbiorem informacji o charakterze technologicznym, technicznym, organizacyjnym, ekonomicznym itp. najczęściej powstałych w rezultacie badań naukowo-technicznych. Są nimi również informacje o sposobie prowadzenia działalności biznesowej, do których osoby trzecie nie posiadają swobodnego dostępu. Decyzja o tym co stanowi tajemnicę handlową podejmują osoby prowadzące działalność gospodarczą, uwzględniając przy tym wykaz informacji, które tajemnicą nie mogą być. W standardach światowych systemów prawnych do takich należą m. in. informacje:

1. Zawarte w dokumentach założycielskich osoby prawnej, potwierdzające fakt dokonywania wpisów o osobach prawnych oraz prywatnych przedsiębiorcach będących osobami fizycznymi do rejestrów państwowych;
2. Zawarte w dokumentach zezwalających na wykonywanie działalności gospodarczej;
3. O mieniu przedsiębiorstw publicznych i samorządowych, instytucji publicznej oraz korzystaniu przez nie ze środków publicznych;
4. Dotyczące zanieczyszczenia środowiska, stanie ochrony przeciwpożarowej, warunków sanitarno-epidemiologicznych oraz ochrony przed promieniowaniem radioaktywnym, bezpieczeństwa żywności i innych czynników, które zapewniają bezpieczne funkcjonowanie obiektów produkcyjnych, bezpieczeństwo każdego obywatela i bezpieczeństwo ludności w ogóle;
5. Liczebności i składzie osobowym oraz zawodowym pracowników, o systemie ich wynagradzania, warunkach pracy, w tym o ochronie pracy: o wypadkowości w miejscu pracy i zachorowalności na choroby zawodowej oraz o dostępności wolnych miejsc pracy w jednostkach publicznych i samorządowych;
6. O długu pracodawców w zakresie wypłaty wynagrodzeń i innych świadczeń społecznych;
7. O łamaniu prawa danego kraju i faktach pociągnięcia do odpowiedzialności za popełnienie tych naruszeń;
8. O przetargach na prywatyzację obiektów będących wcześniej mieniem publicznym lub komunalnym, a także o przetargach na dostawę towarów lub wykonanie usług finansowanych z pieniędzy publicznych;

9. O wielkości i strukturze dochodów organizacji non-profit, o rozmiarze i komponentach ich majątku, o kosztach, liczebności i wynagrodzeniu pracowników, a także o wykorzystaniu wolontariatu (lub innych form nieodpłatnej pracy) w działalności organizacji;
10. O liście osób, mających prawo reprezentować osobę prawną bez pełnomocnictwa.

Zakres powyższych informacji może różnić się pomiędzy różnymi krajami. Lokalne prawo określa również kary za nieujawnienie lub ograniczenie dostępu do powyższych danych. Dysponent informacji ma w swej dyspozycji wiele środków ochrony poufności informacji, której jest właścicielem. W szczególności, może on wykorzystywać:

1. Systematyczne definiowanie listy informacji określanej jako poufna;
2. Ograniczanie dostępu do informacji stanowiącej tajemnicę poprzez zdefiniowanie zasad korzystania z niej oraz metod kontroli nad ich przestrzeganiem;
3. Ewidencjonowanie osób posiadających dostęp do informacji poufnych oraz osób, które taki dostęp uzyskały;
4. Wnoszenie do umów o pracę dla pracowników oraz umów cywilnoprawnych dla kontrahentów zapisów regulujących postępowanie z informacją poufną;
5. Nanoszenie na materialne nośniki informacji poufnej napisów informujących o charakterze informacji wraz ze wskazaniem właściciela takiej informacji (w przypadku osób prawnych podanie pełnej nazwy i miejsca prowadzenia działalności, dla przedsiębiorców indywidualnych – nazwisko i imię przedsiębiorcy oraz miejsce prowadzenia działalności gospodarczej).

Pojęcie *poufność* może mieć również inne odcienie znaczenia. Z punktu widzenia interesujących nas prac audytorskich, *poufność* to zasada, zgodnie z którą audytorzy i organizacje audytorskie są zobowiązane do zapewnienia bezpieczeństwa dokumentów otrzymanych lub sporządzanych przez nich w trakcie inspekcji. Dokumenty lub ich kopie nie mogą być przekazywane w całości lub częściowo jakimkolwiek osobom trzecim. Również ustne ujawnianie zawartych w nich informacji bez zgody audytowanego podmiotu jest niedopuszczalne. Przestrzeganie zasady poufności jest niezbędne zarówno w trakcie prac audytorskich, jak i po ich zakończeniu, bez jakichkolwiek limitów czasowych.

Zdarzenie związane z bezpieczeństwem informacji to zgodnie z Normą stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji. *Incydent związany z bezpieczeństwem informacji* to pojedyncze, niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Terminem *zarządzanie incydentami związanymi z bezpieczeństwem informacji* określamy procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji.

Zgodnie z Normą pod pojęciem *kontrola dostępu* rozumiemy środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa. Kontrola jest jednym z najczęściej stosowanych mechanizmów ochronnych. Pojawia się ona w wielu różnych postaciach, również jej skuteczność jest różna.

Atak to próba zniszczenia, ujawnienia, zmiany, uniemożliwienia dostępu, kradzieży lub uzyskania nieautoryzowanego dostępu albo nieautoryzowanego użycia aktywów. *Zabezpieczeniem* nazywamy środek modyfikujący ryzyko. *Cel stosowania zabezpieczenia* to deklaracja opisująca co ma być rezultatem wdrożenia zabezpieczenia.

Pojęcie *najwyższe kierownictwo* opisuje osobę lub grupę osób, które określają kierunek i sterują organizacją na najwyższym poziomie. Kierownictwo ma prawo do delegowania władzy i zapewnienia zasobów w ramach organizacji.

1.2. Definicja audytu bezpieczeństwa informacyjnego

Audyt bezpieczeństwa informacyjnego (BI) przedsiębiorstwa polega na fachowym badaniu podstawowych aspektów bezpieczeństwa i ich weryfikacji na zgodność z określonymi prawnie lub zwyczajowo wymogami. W niektórych przypadkach, pod pojęciem *audytu* rozumie się sprawdzanie bezpieczeństwa poszczególnych komponentów infrastruktury informatycznej (segmentów sieci, wybranych serwerów, baz danych, stron internetowych itp.) oraz skuteczności działania elementów ochronnych (firewalli, systemów wykrywania włamań i in.).

Wyczerpującą definicję audytu podało Stowarzyszenie Audytu i Zarządzania Systemami Informacyjnymi (ang. *The Information Systems Audit and Control Association ISACA*) [38]. Zgodnie z nią, audyt bezpieczeństwa informacyjnego to procedura gromadzenia i analizy informacji pozwalających stwierdzić czy: **a.** Zapewniane jest bezpieczeństwo zasobów organizacji włączając w to dane; **b.** Zagwarantowane są niezbędne parametry spójności i dostępności danych; **c.** Czy cele organizacji w zakresie efektywności technologii informacyjnych zostały osiągnięte?

W niniejszym rozdziale założono, że audyt bezpieczeństwa informacyjnego jest kompleksowym i wyczerpującym badaniem wszystkich technicznych i organizacyjnych aspektów bezpieczeństwa. Dokonywany jest on w całym obszarze działalności gospodarczej przedsiębiorstwa, z uwzględnieniem obowiązujących zasad bezpieczeństwa, obiektywnych potrzeb firmy, a także wymagań stawianych przez podmioty trzecie (przykładowo: organy państwa, kontrahentów biznesowych, osoby prywatne itp.).

W rozumieniu niniejszej monografii celami audytu są:

1. Ustalenie poziomu bezpieczeństwa zasobów informacyjnych przedsiębiorstwa, określenie wad oraz kierunków dalszego rozwoju systemu ochrony informacji;

2. Weryfikacja przez organy nadzorcze przedsiębiorstwa (lub inne zainteresowane osoby bądź podmioty) uzyskania wyznaczonych celów w zakresie bezpieczeństwa informacyjnego, w szczególności spełnienia wymagań zdefiniowanych w polityce bezpieczeństwa przedsiębiorstwa;
3. Certyfikacja zgodności z przyjętymi normami i wymogami w dziedzinie technologii bezpieczeństwa (w szczególności z normami krajowymi i międzynarodowymi);
4. Kontrola efektywności zakupów inwestycyjnych, przeznaczonych na środki ochrony informacji i realizację działań w zakresie zapewnienia jej bezpieczeństwa.

Jednym z najważniejszych strategicznych zadań rozwiązywanych w procesie audytu bezpieczeństwa informacyjnego oraz uzyskiwania odpowiedniego certyfikatu jest określenie wiarygodności przedsiębiorstwa. Pozytywne wyniki audytu prezentują przedsiębiorstwo jako wiarygodnego i stabilnego partnera, zdolnego zapewnić kompleksową ochronę zasobów informacyjnych, co może być szczególnie ważne przy realizacji kontraktów, wymagających wymiany informacji poufnych, posiadających określoną wartość komercyjną.

Rozróżnia się dwa podstawowe rodzaje audytu: *wewnętrzny*, przeprowadzany wyłącznie siłami pracowników przedsiębiorstwa oraz *zewnętrzny*, dokonywany przez wyspecjalizowane podmioty zewnętrzne. W przypadku *audytu wewnętrznego*, grupę audytorów należy skompletować spośród specjalistów, którzy nie są twórcami lub administratorami analizowanych systemów informatycznych i narzędzi bezpieczeństwa oraz nie mieli wpływu na ich wdrożenie w przedsiębiorstwie. Wykorzystanie audytorów zewnętrznych zazwyczaj ma na celu:

1. Zwiększenie obiektywności, niezależności i profesjonalizmu prac;
2. Uzyskanie z niezależnego źródła opinii o stanie bezpieczeństwa i jego zgodności z międzynarodowymi aktami normatywnymi.

Audyt zewnętrzny jest prowadzony zgodnie ze sformalizowanymi wytycznymi przez firmy zewnętrzne, specjalizujące się w tematyce bezpieczeństwa. Przed wyborem konkretnej firmy audytorskiej należy zapoznać się z jej referencjami, w szczególności odnoszącymi się do przedsiębiorstw o podobnym profilu działalności.

Organizacja przeprowadzająca audyt zewnętrzny musi spełniać określone wymagania formalno-prawne. W szczególności, powinna ona:

1. Dysponować prawem do wydawania opinii o zgodności z określonymi wymogami normatywnymi;
2. Jej pracownicy powinni posiadać certyfikaty dostępu do informacji stanowiącej tajemnicę państwową (o ile takie informacje występują w badanym przedsiębiorstwie);
3. Dysponować odpowiednim oprogramowaniem i sprzętem komputerowym, gwarantującym wyczerpującą weryfikację wykorzystywanego w przedsiębiorstwie sprzętu i oprogramowania.

Podział audytów na wewnętrzny i zewnętrzny nie jest jedynym. Inny podział, opisany m. in. w [39] dzieli audyty z punktu widzenia zakresu wykonywanych działań na: audyt penetracyjny, audyt na zgodność ze standardami lub normami oraz audyt ekspercki. Każdy z nich może zostać zrealizowany jako audyt wewnętrzny lub zewnętrzny. Pełny zakres audytu obejmuje wszystkie trzy jego typy funkcjonalne. Rodzaje audytu pokazano na rys. 1.3.

Rys. 1.3. Rodzaje audytu bezpieczeństwa informacyjnego

Audyt penetracyjny jest prowadzony z punktu widzenia intruza posiadającego rozbudowaną wiedzę w obszarze technologii informacyjnych. Wykonując swoją pracę, audytor korzysta wyłącznie z ogólnodostępnych informacji i zasobów, na podstawie których przeprowadza on maksymalną możliwą liczbę różnych ataków.

Ponieważ audyt tego typu wykonywany jest za pomocą specjalistycznych narzędzi (programów, rzadziej zestawów programowo-sprzętowych) istnieje możliwość automatyzacji audytowania, a udział w nim pracowników jest sprowadzony do niezbędnego minimum. Niska (z punktu widzenia podmiotu) pracochłonność audytu penetracyjnego pozwala wykonywać go wielokrotnie, powtórne skanowanie systemu informacyjnego prowadzone jest zazwyczaj po: **a.** Usunięciu zagrożeń odnalezionych w czasie poprzedniej procedury audytu penetracyjnego. Uzyskujemy w ten sposób potwierdzenie skuteczności działań naprawczych; **b.** Wdrożeniu do systemu nowych komponentów programowo-sprzętowych mogących spowodować pojawienie się nowych luk; **c.** Upływie terminu planowego audytu bezpieczeństwa SI.

Asortyment przeprowadzanych testów jest dość szeroki, zazwyczaj obejmuje: wyszukiwanie luk w systemie ochrony; weryfikację odporności systemu na ataki różnych typów, na przykład DDoS; testy obciążeniowe, przeciążeniowe i wydajnościowe [40], [41] i in. Potrzeba dysponowania specjalistycznym komercyjnym oprogramowaniem pozwalającym automatycznie skanować system naraża Zleceniodawcę na dodatkowe, często niepotrzebne koszty i obciążenie systemu. Dlatego, zlecenie testów penetracyjnych można zlecić zewnętrznej firmie, która z uwagi na dużą dostępność tego typu usług może zaproponować atrakcyjną cenę. Alternatywnym rozwiązaniem jest zastosowanie jednego z szerokiej gamy produktów typu *open source*.

Zastosowanie testów penetracyjnych posiada również kilka istotnych wad. Pierwsza z nich to wysokie koszty specjalistycznego komercyjnego oprogramowania. Z kolei oprogramowanie typu *open source* może być źródłem dodatkowych zagrożeń. Po drugie, audyt penetracyjny pozwala wykrywać zagrożenia

jawnie zdefiniowane w narzędziu wykorzystywanym do jego realizacji. Wymaga to ciągłego śledzenia aktualności posiadanego oprogramowania – starsze wersje aplikacji mogą nie wyszukiwać nowych zagrożeń. Zdarzają się również fałszywe alarmy będące skutkiem niepoprawnej interpretacji przez program zdarzeń występujących w trakcie testowania. Sposób przeprowadzenia audytu penetracyjnego, jak dotąd nie został zdefiniowany w żadnym akcie normatywnym, trudno więc mówić o unifikacji działań audytorskich i porównywaniu ich wyników. Często stawianym zarzutem jest także potrzeba chwilowego wstrzymania (na czas audytu) pracy systemu informacyjnego. W praktyce zarzut ten nie ma istotnego znaczenia – każdy z komercyjnych programów skanujących zbiera dane w trakcie pracy audytowanego systemu. Powyższy zarzut bywa słuszny w przypadku zastosowanie niektórych programów skanujących typu *open source*.

Pomimo powyższych wad, audyt penetracyjny należy do najbardziej pożądanych rodzajów audytu. Jego wynikiem są informacje o lukach w systemie ochrony, wnoszonych zagrożeniach oraz o sposobach ich usunięcia. Więcej informacji na ten temat można znaleźć w literaturze [40], [42], [43].

Audyt *na zgodność ze standardami lub normami,* nazywany dalej *audytem zgodności*. Określa on, na ile bezpieczeństwo systemu informacyjnego odpowiada wymaganiom wybranego standardu lub normy. Należy zauważyć, że pojęcia standardu i normy nie są tożsame. *Standard* często jest podstawą normy, odwrotna relacja jest niemożliwa. Zazwyczaj jest to zestaw parametrów określających poziom jakości, bezpieczeństwa bądź zgodności z innymi wytworami techniki. Przykładowo, ilość gwiazdek przy opisie hotelu określa jego standard, tj. poziom jakości oferowanych przez niego usług. Z kolei *norma*, nazywana również dokumentem normatywnym jest przyjętym na zasadzie konsensusu aktem, opisującym zasady, wytyczne lub charakterystyki, dotyczące różnych rodzajów działalności bądź ich wyników. Zadaniem normy jest uzyskanie optymalnego stopnia uporządkowania w określonym obszarze działalności człowieka. Przykładowo, norma PN-ISO/IEC 27001 określa wymagania stawiane przed systemem zarządzania bezpieczeństwem informacji. Więcej informacji w tym temacie można znaleźć na portalu Polskiego Komitetu Normalizacyjnego [44]. Warto zaznaczyć, że w większości języków narodowych problem ten nie występuje: terminy: standard i norma są tożsame.

Sekwencja kroków audytu określona jest w dokumencie, na podstawie którego jest on wykonywany (standard, norma, rozporządzenie, zalecenie itp.). Dzięki temu wszystkie audyty mogą być prowadzone identycznie, a ich wyniki porównywalne. Sformalizowana jest również postać sprawozdania i sposobu jego przygotowania. Audyt zgodności bazuje na wiedzy i doświadczeniu audytorów i nie wymaga dodatkowego oprogramowania. Nie wymaga on zatrzymywania pracy weryfikowanego systemu ani dodatkowego oprogramowania. W Polsce to jeden z najczęściej wykonywanych audytów bezpieczeństwa informacyjnego. Wydawany certyfikat, najczęściej sygnowany przez międzynarodową organizację standaryzującą pozytywnie wpływa na wizerunek organizacji. Wymagania stawiane przez normy

i certyfikaty są przygotowywane przez międzynarodowy zespół specjalistów najwyższej klasy i odzwierciedlają one dobre praktyki w obszarze bezpieczeństwa informacji.

Niestety, *audyt zgodności* posiada również kilka wad, z których najważniejsze to: **a.** Konieczność angażowania w jego wykonanie pracowników podmiotu, również spoza Działu informatyki, od których wymaga się dogłębnej wiedzy o funkcjonowaniu audytowanego systemu informacyjnego; **b.** Procedura audytu jest czaso- i pracochłonna, co skutkuje pokaźnymi jej kosztami i powinna towarzyszyć wszelkim zmianom wnoszonym do systemu informacyjnego; **c.** Zmienia się również baza normatywna (normy, standardy, ustawy, rozporządzenia) będące podstawą przeprowadzenia audytu. Zmiana bazy może powodować potrzebę chociażby cząstkowego powtórzenia czynności audytorskich; **d.** Ograniczone możliwości samodzielnej realizacji – certyfikat może być wystawiany wyłącznie przez upoważnioną organizację; **e.** W dokumentach normatywnych, szczególnie w ustawach i rozporządzeniach zdecydowanie zbyt często pojawiają się sprzeczności i nieścisłości; **f.** Nie istnieje jeden powszechnie akceptowany dokument normatywny, koniecznym może okazać się więc wykonanie kilku różnych audytów.

Wynikiem audytu tego typu jest: **a.** Określenie zgodności analizowanego systemu informacyjnego z wybranym standardem lub normą; **b.** Oszacowanie zgodności systemu z wewnętrznymi wymaganiami podmiotu w obszarze bezpieczeństwa informacyjnego; **c.** Szczegółowa analiza dokumentów podmiotu, określających zasady zapewniania bezpieczeństwa informacji, w szczególności Polityki Bezpieczeństwa Informacyjnego oraz standardów i norm wykorzystywanych w tym celu; **d.** Przygotowanie zaleceń modernizacji systemu zarządzania bezpieczeństwem informacji zgodnego z zaleceniami standardu bądź normy, a jeżeli takowy nie istnieje, opis sposobu jego budowy.

Ostatnim rodzajem jest *audyt ekspercki* będący krytycznym porównaniem stanu bezpieczeństwa informacyjnego z opisem zawartym m. in. w wytycznych definiowanych przez zarząd podmiotu oraz bazujący na wieloletnim doświadczeniu w obszarze audytu, zarówno osobistym audytorów, jak również innych organizacji. Do najważniejszych zalet tego typu audytu należy odnieść: **a.** Nie wymaga on dodatkowych środków programowo-technicznych podczas realizacji; **b.** Audyt jest niezależny od funkcjonowania samego systemu, tj. ingerencja w jakiekolwiek jego zasoby nie jest wymagana;

Gromadzenie informacji niezbędnych do opracowania opinii odbywa się na bazie wywiadów z pracownikami podmiotu. Wywiady prowadzone są z zarówno z personelem technicznym, bezpośrednio zarządzającym bezpieczeństwem informacyjnym, jak również użytkownikami systemu informacyjnego. Ponieważ badanie opinii wszystkich użytkowników systemu jest trudne w realizacji, w pierwszej kolejności zaleca się przeprowadzenie wywiadów u osób krytycznie nastawionych do eksploatacji systemu informacyjnego. Wynikiem audytu jest zbiór rekomendacji dotyczących modernizacji systemu ochronnego. Więcej informacji dotyczących

każdego z wyszczególnionych rodzajów audytu zaprezentowano w dalszej części monografii.

Dalej omówiony zostanie przykład kompleksowego audytu bezpieczeństwa, który będzie obejmować wybrane elementy każdego z powyższych rodzajów działań kontrolnych. W praktyce może się zdarzyć, że zlecone prace obejmować będą wszystkie komponenty zdefiniowanych wyżej audytów. Jednak sytuacja taka nie występuje nagminnie. Najczęściej kompleksowy audyt obejmuje wyłącznie wybrane elementy bazowych prac audytorskich.

1.3. Formalno-prawne podstawy audytu

Podstawą przygotowania audytów są przedmiotowe normy i wymagania. Do najczęściej wykorzystywanych należą:

1. ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation. Jej odpowiednikiem jest Polska Norma PN- ISO/IEC 15408 Kryteria oceny zabezpieczeń informatycznych. Norma opisuje procedury pozwalające na zdefiniowanie zagrożeń oraz adresowanych do nich zabezpieczeń, a także przeprowadzenie formalnej weryfikacji ich faktycznego działania w systemie;
2. ISO/IEC 27002 (wcześniej ISO/IEC 17799: Code of Practice for Information Security Management, z polskim odpowiednikiem PN-ISO/IEC 17799:2007 Praktyczne zasady zarządzania bezpieczeństwem informacji. Norma definiuje zasady ustanowienia, określenia, eksploatacji oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji. Stanowi ona opisowe rozwinięcie normy ISO/IEC 27001;
3. COBIT: Control Objectives for Information and related Technology. Jest to zestaw otwartych dokumentów w obszarze zarządzania, IT, audytu oraz bezpieczeństwa informacyjnego.

Z uwagi na rygorystyczne wymagania dotyczące ochrony danych osobowych często wykonywany jest również audyt, którego wytyczne zawarte są w dokumentach:

1. 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 (ogólne rozporządzenie o ochronie danych);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000.

Zakres audytu dotyczącego obu powyższych aktów prawnych jest węższy niż dla wcześniejszych dokumentów. Stosuje się je w sytuacji, kiedy weryfikacji ma podlegać wyłącznie bezpieczeństwo danych osobowych.

1.4. Etapy realizacji audytu

Audyt to proces wieloetapowy. Rozpoczyna go zarząd przedsiębiorstwa, który precyzyjnie wyznacza jego cele. Etap ten nazywany jest **inicjacją audytu**. Cele

powinny być dostosowane do aktualnego rozwoju systemu informatycznego firmy, a także poziomu wykorzystywanych zabezpieczeń. Jeżeli audyt nie ma kompleksowego charakteru, to należy określić obszar, który będzie on obejmował. W szczególności konieczne jest przygotowanie: wykazu badanych zasobów i systemów informacyjnych; listy budynków, pomieszczeń i terenów, w których obrębie będzie się odbywać audyt; wykazu podstawowych zagrożeń, ochronę przed którymi należy poddać inspekcji; listę zabezpieczeń włączonych w proces badania (dotyczy to komponentów organizacyjnych, prawnych, urządzeń technicznych, sprzętu oraz oprogramowania).

Kolejnym, uważanym za najistotniejszy w całej procedurze etapem audytu jest *bezpośrednie zbieranie informacji i przeprowadzenie przez audytorów badań zasobów zleceniodawcy*. Etap ten powinien zawierać:

1. Analizę wykorzystywanej polityki bezpieczeństwa, a także innej dokumentacji organizacyjno-technicznej obowiązującej w firmie;
2. Przeprowadzenie spotkań, ankietowania, szczerych rozmów i wywiadów z pracownikami przedsiębiorstwa;
3. Weryfikację stanu bezpieczeństwa fizycznego infrastruktury informatycznej;
4. Badania techniczne sprzętowych i programowych komponentów systemów informatycznych.

Przed przystąpieniem do swoich obowiązków, audytorzy (w szczególności, jeżeli są oni pracownikami firmy zewnętrznej), powinni zapoznać się ze strukturą przedsiębiorstwa, jego funkcjami, zadaniami oraz głównymi procesami biznesowymi, a także z istniejącymi systemami informacyjnymi (ich składem, funkcjami, procedurami wykorzystania i ich rolą w przedsiębiorstwie).

Początkowo, audytorzy podejmują decyzje o tym, jak szczegółowo będą badane poszczególne elementy systemu informacyjnego oraz składniki ochrony informacji. Konieczne jest wcześniejsze skoordynowanie prac audytorskich z normalnym funkcjonowaniem infrastruktury informacyjnej, w szczególności, jeżeli audyt wymaga ograniczenia dostępu użytkowników (takie procedury, w miarę możliwości, powinny odbywać się poza godzinami pracy lub w okresach najmniejszego obciążenia systemu informacyjnego).

Analiza jakościowa funkcjonującej w przedsiębiorstwie polityki bezpieczeństwa jest punktem wyjścia do przeprowadzenia audytu. Jednym z pierwszych jej kroków jest ustalenie, w jakim stopniu aktualna polityka bezpieczeństwa odpowiada obiektywnym potrzebom danego przedsiębiorstwa, czy podejmowane działania pozwalają zapewnić odpowiedni poziom bezpieczeństwa informacji, w trakcie jej przetwarzania, przechowywania i przesyłania. To z kolei może wymagać przeprowadzenia dodatkowej oceny istotności głównych zasobów informacyjnych firmy, ich wrażliwości, jak również ryzyka oraz istniejących zagrożeń.

Analiza polityki powinna obejmować ocenę takich parametrów jak:

1. Kompletność rozpatrywania zagadnień bezpieczeństwa, a także poprawność wzajemnych relacji pomiędzy politykami różnych poziomów;

2. Zrozumiałość tekstu polityki dla osób, które nie są zawodowo związane z informatyką, a także precyzyjność sformułowań i niemożność ich niejednoznacznej interpretacji;
3. Aktualność wszystkich postanowień i wymagań polityki, terminowość uwzględnienia zmian zachodzących w systemach i procesach biznesowych.

Po sprawdzeniu podstawowych założeń polityki bezpieczeństwa, w trakcie audytu, mogą być badane obowiązujące klasyfikacje zasobów informacyjnych według stopnia ich krytyczności i prywatności, a także inne dokumenty, które odnoszą się do bezpieczeństwa informacji. Dotyczy to m. in.:

1. Dokumentów organizacyjnych poszczególnych działów przedsiębiorstwa (decyzje o ich utworzeniu, opisy stanowisk pracy, regulaminy pracy, zakresy obowiązków pracowników itp.);
2. Instrukcji, przepisów i procedur odnoszących się do poszczególnych procesów biznesowych;
3. Dokumentacji kadrowej, zobowiązań o nieujawnianiu informacji danych pracowników, zaświadczeń o ukończeniu szkoleń, certyfikatów zawodowych, potwierdzeń o zaznajomieniu się z obowiązującymi przepisami;
4. Dokumentacji technicznej, instrukcji użytkownika używanego sprzętu i oprogramowania (zapór ogniowych, routerów, przełączników, zasilaczy awaryjnych, systemów operacyjnych, programów antywirusowych, aplikacji zarządzania przedsiębiorstwem itp.).

W procesie kompletowania informacji, podstawowym celem pracy rewidentów jest zbadanie rzeczywistych działań podejmowanych w celu ochrony aktywów informacyjnych przedsiębiorstwa, takich jak:

1. Organizacja procesu szkolenia użytkowników w zakresie zasad bezpiecznego korzystania z systemów informatycznych;
2. Organizacja pracy administratorów systemów informacyjnych, telekomunikacyjnych i systemów ochrony informacji (prawidłowość wykorzystania oprogramowania, sprzętu oraz narzędzi administracyjnych, terminowość tworzenia i usuwania kont użytkowników, a także ich prawa dostępu, terminowość wymiany haseł i zapewnienie ich zgodności z wymaganiami bezpieczeństwa, wykonywanie kopii zapasowych danych, opracowanie protokołów operacji administrowania, podejmowanie adekwatnych działań w przypadku wykrycia usterek itp.);
3. Organizacja prac ukierunkowanych na podnoszenie kwalifikacji administratorów systemów informacyjnych i ochrony danych;
4. Zapewnienie zgodności niezbędnych (tj. zgodnych z zasadami polityki bezpieczeństwa i przypisanymi do pracownika obowiązkami służbowymi) praw dostępu użytkowników systemów z aktualnie wykorzystywanymi;
5. Organizacja nadawania i wykorzystania w systemach specjalnych uprawnień administracyjnych (tzw. superuser);

6. Organizacja prac, w przypadku wykrycia naruszeń bezpieczeństwa oraz przywracania działania systemu po awariach lub atakach;
7. Podejmowane środki ochrony antywirusowej (właściwe korzystanie z programów antywirusowych, uwzględnianie wszystkich infekcji, organizacja prac przy usuwaniu ich skutków itp.);
8. Zapewnienie bezpieczeństwa nabywanego oprogramowania i sprzętu (posiadanie certyfikatów i gwarancji, wsparcie ze strony producenta przy usuwaniu stwierdzonych wad bądź usterek);
9. Zagwarantowanie bezpieczeństwa oprogramowania własnej produkcji (obecność niezbędnych wymogów w dokumentacji projektowej systemów informatycznych, odpowiedni poziom jakości oprogramowania przeznaczonego do realizacji mechanizmów ochrony itp.);
10. Organizacja prac instalacyjnych i aktualizacyjnych, a także kontrola ciągłości oprogramowania;
11. Podejmowanie działań mających na celu ewidencję i zapewnienie bezpieczeństwa nośników informacji (dysków, dyskietek, taśm, pamięci flash itp.), a także gwarantujące ich zniszczenie po zakończeniu eksploatacji;
12. Efektywność współdziałania użytkowników systemów informatycznych ze służbami bezpieczeństwa (w szczególności, w zakresie reagowania na zagrożenia i usuwania ich skutków).

Jednym z najważniejszych kierunków audytu jest kontrola tego, jak szybko i kompleksowo przepisy oraz wymagania dotyczące bezpieczeństwa oraz inne dokumenty organizacyjne są przekazywane personelowi przedsiębiorstwa. W tym przypadku, należy ocenić na ile systematycznymi i ukierunkowanymi są szkolenia (w przypadku objęcia stanowisk przez pracownika oraz w trakcie normalnej pracy), a także w jakim stopniu personel rozumie stawiane przed nim wymagania, czy jest świadomy swoich obowiązków związanych z zapewnieniem bezpieczeństwa, a także ewentualnej odpowiedzialności w przypadku naruszenia ustalonych wymagań.

W proces przeprowadzania wywiadów, spotkań i rozmów z pracownikami, należy włączyć jak największą ich liczbę, szczególnie tych, którzy mają jakikolwiek kontakt z systemami lub procedurami przetwarzania informacji. W spotkaniach, powinni brać również udział administratorzy, programiści, operatorzy, a także personel pomocniczy. W trakcie bezpośredniego kontaktu z pracownikami, rewident powinien zapoznać się z przebiegiem poszczególnych procesów biznesowych, roli poszczególnych pracowników w ich realizacji oraz potencjalnymi możliwościami wpływu na ich bezpieczeństwo. Ponadto należy ocenić, w jakim stopniu pracownicy faktycznie wykonują swoje obowiązki odnoszące się do bezpieczeństwa informacyjnego.

Jednym z najważniejszych zadań audytu może być ustalenie, na ile przedsiębiorstwo jest w stanie przeciwdziałać zagrożeniom wewnętrznym ze strony własnych pracowników dysponujących możliwościami naniesienia szkody swojemu pracodawcy. W szczególności, analizie powinny podlegać:

1. Procedury doboru i zatrudniania nowych pracowników, a także ich wstępnej weryfikacji;
2. Procedury śledzenia działań pracowników;
3. Zasady rejestracji użytkowników i przyznawania im uprawnień w systemach informacyjnych;
4. Podział funkcji między pracownikami i minimalizacja ich uprawnień, a także ewentualny nadmiar praw u wybranych użytkowników, jak i administratorów.

Sprawdzanie stanu fizycznego bezpieczeństwa infrastruktury informatycznej, obejmuje najczęściej:

1. Weryfikację, czy najważniejsze obiekty infrastruktury i systemów ochrony informacji znajdują się w miejscach chronionych przez odpowiednie służby, wyposażone w kamery telewizji przemysłowej i inne środki kontroli;
2. Sprawdzenie obecności i poprawności działania urządzeń technicznych, zapewniających stabilną pracę sprzętu komputerowego i telekomunikacyjnego (źródeł awaryjnego zasilania, klimatyzacji itp.);
3. Weryfikację istnienia oraz poprawności działania środków sygnalizacji i gaszenia pożarów;
4. Określenie podziału odpowiedzialności za stan techniczny obiektów infrastruktury informatycznej.

Kolejny etap audytu, *pomocnicza kontrola bezpieczeństwa*, jest przede wszystkim zadaniem o charakterze technicznym i bazuje na wykorzystaniu specjalistycznego oprogramowania, za którego pomocą automatycznie zbiera się wszystkie możliwe informacje, takie jak: wersje systemów operacyjnych oraz oprogramowania, dane o używanych protokołach sieciowych, numery zamkniętych i otwartych portów protokołów komunikacyjnych, dane o zainstalowanych aktualizacjach itp. Innymi zadaniami tej klasy kontroli są:

1. Bezpośrednia analiza funkcjonowania poszczególnych serwerów, stacji roboczych i urządzeń sieciowych. Do tego celu, wykorzystywane są specjalistyczne techniki sprawdzające różnorodne aspekty ich funkcjonowania, na przykład: procedury startu, wykaz uruchomionych procesów, zawartość plików konfiguracyjnych, prawa dostępu najważniejszych plików, datę i czas uruchomienia itp.;
2. Gromadzenie, a następnie analiza informacji o procedurach tworzenia kopii zapasowych, a także innych procedur technicznych przewidzianych w polityce bezpieczeństwa;
3. Kontrola jakości oprogramowania, samodzielnie opracowanego przez przedsiębiorstwo (przykładowo, poprzez analizę kodów źródłowych i jego dokumentacji projektowej), wykrywanie błędów, które mogą stać się przyczyną awarii, nielegalnych włamań, niszczenia lub ujawniania informacji;
4. Analiza funkcjonowania sieci, w szczególności ruchu i protokołów wykorzystywanych w jej segmentach;

5. Przeprowadzenie kontrolowanych naruszeń bezpieczeństwa informacji niepowodujących, w miarę możliwości, powstawania realnych szkód. Ataki typu odmowa usługi (DoS) powinny być realizowane poza normalnymi godzinami pracy audytowanego przedsiębiorstwa.

Celowym jest również wykonanie ataków korzystających z różnych luk w zabezpieczeniach pozwalających na określenie konkretnych ustawień bezpieczeństwa, stabilności i niezawodności testowanego systemu informatycznego.

Proces audytu powinien objąć analizę najważniejszych dzienników (logów) systemów informacyjnych oraz urządzeń sieciowych. Zaleca się także badanie innych narzędzi gromadzenia i analizy informacji wykorzystywanych do zapewnienia bieżącej kontroli nad przestrzeganiem wymagań bezpieczeństwa oraz terminowego reagowania na incydenty. Przykładem takich narzędzi są m. in. detektory włamań i analizatory pracy sieci. Informacje zgromadzone w plikach *logów* w trakcie korzystania z audytowanych systemów są jednym z kluczowych elementów prowadzonej analizy. Na podstawie zgromadzonych w nich danych, mogą być wykonane oceny oraz zdefiniowane wnioski dotyczące przestrzegania ustalonych warunków korzystania z systemów, skuteczności stosowanych środków ochrony informacji, zachowania użytkowników, a także ujawnione informacje o potencjalnych problemach pojawiających się w trakcie eksploatacji.

Interpretacja informacji uzyskanych w procesie badania dokumentów udostępnionych przez zleceniodawcę, weryfikacji wykonania zaleceń polityki bezpieczeństwa, sugestii otrzymanych od pracowników lub pozyskanych w trakcie analizy funkcjonowania sprzętu i oprogramowania, weryfikacji skuteczności ochrony fizycznej oraz pomocniczych testów powinna być wykonana z uwzględnieniem stwierdzonych zagrożeń i potrzeb przedsiębiorstwa w obszarze bezpieczeństwa.

W szczególności, analiza taka powinna określić konkretne cechy oprogramowania i sprzętu, procedur biznesowych, zasad organizacyjnych oraz rozkładu obowiązków i uprawnień, które mogą negatywnie wpływać na bezpieczeństwo informacji. Ponadto, wyszukiwane powinny być relacje przyczynowo-skutkowe, występujące pomiędzy określonymi cechami funkcjonowania przedsiębiorstwa a wzrostem ryzyka naruszenia bezpieczeństwa informacji.

Wszystkie przebadane okoliczności, stwierdzone wady i cechy muszą być uogólnione. Tak więc, powinna zostać zdefiniowana ogólna charakterystyka stanu bezpieczeństwa w audytowanym przedsiębiorstwie, odzwierciedlająca podstawowe zalety i wady obecnego systemu ochrony zasobów informacyjnych. Powinny zostać również określone jego priorytety oraz kierunki dalszego rozwoju i doskonalenia.

Wyniki analizy powinny być przedstawiane w formie krótkich, ogólnych sformułowań, charakteryzujących bezpieczeństwo informacji (skierowanych do dyrekcji i właścicieli), jak i w postaci listy konkretnych uwag i wniosków odnoszących się do poszczególnych obszarów pracy (adresowanych do szefa departamentu bezpieczeństwa, szefa służby bezpieczeństwa, dyrektorów branżowych oraz kierowników jednostek organizacyjnych przedsiębiorstwa).

Końcowym rezultatem analizy wykonanej w trakcie audytu jest raport, który powinien zawierać:

1. Ocenę poziomu bezpieczeństwa zasobów informacyjnych i systemów informatycznych;
2. Wnioski dotyczące praktycznego spełnienia wymagań, o których jest mowa w polityce bezpieczeństwa informacji oraz innych przepisach i dokumentach;
3. Konkluzję o poziomie zgodności rzeczywistego bezpieczeństwa w relacji, do wymagań określonych w dokumentach normatywnych;
4. Propozycje zmian zasad bezpieczeństwa oraz realizacji dodatkowych działań praktycznych w tym obszarze (zarówno w odniesieniu do działań organizacyjnych, jak i technicznych), a także o pracach, które należy podjąć w celu certyfikacji zgodności z określoną normą (jeżeli w wyniku przeprowadzonego audytu definiuje się wniosek, że aktualny poziom bezpieczeństwa nie spełnia takich wymagań);
5. Konkluzję o stopniu zgodności polityki bezpieczeństwa przedsiębiorstwa i całego kompleksu podejmowanych działań w obszarze ochrony danych osobowych z przepisami prawnymi i branżowymi aktami normatywnymi;
6. Ocenę efektywności ekonomicznej inwestycji w środki ochrony informacji, w tym również organizacyjne;
7. Ilościową (tj. w wyrażeniu pieniężnym) ocenę możliwych strat powstałych w wyniku nieprawidłowości, które mogą pojawić się przy istniejącym poziomie zabezpieczeń, a także określenie nakładów, które należy ponieść, w celu osiągnięcia wymaganego poziomu bezpieczeństwa.

Na podstawie wyników audytu, mogą zostać sformułowane dodatkowe zalecenia, w szczególności dotyczące:

1. Rewizji poszczególnych procesów biznesowych oraz procedur;
2. Doskonalenia pracy z pracownikami przedsiębiorstwa w obszarze bezpieczeństwa informacji;
3. Wdrożenia i wykorzystania nowoczesnych środków technicznych przetwarzania i ochrony informacji;
4. Zastosowania alternatywnych metod organizacji pracy zapewniających lepszą ochronę informacji;
5. Określenia priorytetów rozwiązywania istniejących niedoskonałości.

Wzór wstępnego rozdziału Sprawozdania pokazano w przykładzie 1. Założono w nim, że audyt dotyczy przedsiębiorstwa i ma on weryfikować zgodność eksploatowanego systemu zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001.

Przykład 1. Wzór preambuły sprawozdania pokontrolnego

Niniejsze opracowanie powstało na zlecenie Przedsiębiorstwa XYZ, określanego dalej jako *Zleceniodawca*. Opisuje ono poziom spełnienia przez system informacyjny Zleceniodawcy wymagań stawianych przez normę PN-ISO/IEC 27001, nazywaną dalej Normą.

Dokument posiada następująca budowę:

1. Poszczególne rozdziały odpowiadają celom stosowania zabezpieczeń, zgodnym z Załącznikiem A do Normy;
2. Każdy z rozdziałów rozpoczyna się od prezentacji celów zastosowania zabezpieczenia;
3. Opisywane są wymagane przez Normę zabezpieczenia;
4. Przedstawiany jest stan zabezpieczeń w systemie informacyjnym Zleceniodawcy;
5. Prezentowane są zalecenia dotyczące wdrożenia u Zleceniodawcy zabezpieczeń danej grupy;
6. Braki w systemie ochrony Zleceniodawcy są podkreślane, szacowany jest ich poziom ważności;
7. Dokument kończą uwagi i zalecenia dotyczące uzyskania Certyfikatu ISO.

Poprzez skrótem PBI oznaczana jest Polityka Bezpieczeństwa Informacyjnego. Skrótem SZBI oznaczać będziemy System Zarządzania Bezpieczeństwem Informacji. ■

1.5. Podsumowanie

Chociaż przeprowadzenie audytu bezpieczeństwa informacyjnego może wydawać się działaniem złożonym i czasochłonnym, powinien być on systematyczne wykonywany w praktycznie każdym przedsiębiorstwie gromadzącym i przetwarzającym dane. Jeżeli wartość informacji i konsekwencje wynikające z ich utraty są niewielkie, audyt może być wykonany siłami przedsiębiorstwa. W przeciwnym przypadku sugeruje się okresowe zlecanie prac kontrolnych wyspecjalizowanym firmom. Wykonanie procedur audytorskich, zgodnych z aktami normatywnymi, niesie wiele istotnych korzyści i powinno być preferowane.

W ciągu ostatnich 20 lat obserwuje się permanentne rozszerzenie obszaru wykorzystania technik informacyjnych. Metody i środki, pierwotnie przeznaczone do zastosowań w obszarze nauki oraz techniki wojskowej, dziś używane są powszechnie. Z wykorzystaniem metod i środków informatyki zbudowano szereg systemów złożonych, bez których istnienie współczesnej cywilizacji jest niemożliwe. Do grupy tej należą dostarczające wiedzę systemy informacyjne, systemy zarządzania, systemy telekomunikacyjne, diagnostyczne itp. Ponadto, techniki informatyczne są powszechnie stosowane w procesie autonomicznego zarządzania produkcją, finansami, sprzętem domowym itp. Systemy i sieci komputerowe XXI wieku charakteryzują nowe, wymienione poniżej właściwości, utrudniające efektywne wykorzystanie dotychczasowych organizacji i architektur.

Rozdział 2

Kontekst organizacji i przywódcza rola kierownictwa

2.1. Wymagania aktów normatywnych

Nie istnieje jedna uogólniona recepta gwarantująca zapewnienie bezpieczeństwa informacyjnego. Dlatego, kluczowa rola w tym procesie przypada osobom odpowiadającym za eksploatację systemu informacyjnego przedsiębiorstwa, które jednocześnie są decyzyjne finansowo. Dlatego wymaga się, aby najwyższe kierownictwo organizacji (Prezes, Prezydent, Dyrektorzy, Kierownicy działów) wykazywało wiodącą rolę i zaangażowanie w budowie i eksploatacji systemu zarządzania bezpieczeństwem informacji. W szczególności wymagane są:

1. Aby polityka bezpieczeństwa oraz cele bezpieczeństwa informacji były ustanowione i zgodne z kierunkiem strategicznym przedsiębiorstwa (organizacji);
2. Zapewnienie zintegrowania wymagań systemu zarządzania bezpieczeństwem z procesami biznesowymi organizacji;
3. Zagwarantowanie dostępności programowych, sprzętowych i organizacyjnych zasobów potrzebnych do funkcjonowania systemu zarządzania bezpieczeństwem;
4. Kierowanie i wspieranie osób przyczyniających się do osiągnięcia skuteczności systemu zarządzania bezpieczeństwem;
5. Promowanie ciągłego doskonalenia systemu zarządzania bezpieczeństwem oraz wspieranie innych właściwych członków kierownictwa w wykazywaniu przywództwa, zgodnie z obszarem ich odpowiedzialności.

Aby uzyskać informacje na powyższe tematy, należy przeprowadzić wywiad, najlepiej z osobą bezpośrednio odpowiedzialną za funkcjonowanie systemu informacyjnego przedsiębiorstwa, ewentualnie jego kierownictwem. Pytania powinny być opracowane na etapie przygotowawczym audytu, celowym jest wcześniejsze zapoznanie z nimi zainteresowanych osób z organizacji. W przykładzie 2 przedstawiono typowe pytania zadawane na tym etapie audytu.

Przykład 2. Pytania dotyczące przywódczej roli kierownictwa

1. Czy celowe są systematyczne działania zmierzające do zapewnienia bezpieczeństwa informacji w przedsiębiorstwie?
2. Czy działania zmierzające do zapewnienia bezpieczeństwa są podejmowane i czy mają one regularny charakter?
3. W jaki sposób podzielono odpowiedzialność za zapewnienie bezpieczeństwa informacji wewnątrz organizacji?

4. Czy istnieje dokument obligujący cały personel do zachowania pewnych środków ostrożności podczas korzystania z informacji i systemów informacyjnych, podnoszenia swoich kwalifikacji w tej dziedzinie i określający odpowiedzialność za ewentualne naruszenia?
5. Jaki jest stosunek kierownictwa przedsiębiorstwa do faktów naruszenia wymagań ochrony oraz osób dokonującym takie naruszenia? ■

Wbrew panującemu przekonaniu, określenie poziomu zaangażowania kierownictwa w rozwiązywaniu problemów bezpieczeństwa nie jest proste. W większości polskich przedsiębiorstw panuje przekonanie, że jakiekolwiek deprecjonowanie przełożonego, tym bardziej właściciela lub zarządzającego, nie powinno mieć miejsca. Dlatego otrzymywane w wywiadach oceny subiektywne mają małe znaczenie przy późniejszym formułowaniu wniosków pokontrolnych. Z doświadczeń autorów wynika, że poziom nieszczerości osiąga maksimum u średniego personelu kierowniczego. Znacznie cenniejsze informacje można uzyskać u szeregowych pracowników zaangażowanych w bezpieczeństwo. Oczywiście, w rękach audytora jest jeszcze szereg działań pozwalających jednoznacznie określić zaangażowanie personelu kierowniczego. Wiążą się one z działaniami, które są podejmowane lub nie przez te osoby celem zapewnienia bezpieczeństwa informacji.

Czy jednak zarządzający i właściciele przedsiębiorstw w jakikolwiek sposób oczekują od podległego sobie personelu jakiegokolwiek kolorowania rzeczywistości? Zdaniem autorów są to sytuacje nadzwyczaj rzadkie i zdarzające się wyłącznie w przypadkach czasowego powierzenia zarządzania majątkiem publicznym. W przedsiębiorstwach prywatnych, gdzie pracownicy mają bezpośrednią styczność z właścicielem lub jego reprezentantem występują sytuacje odwrotne, zbyt krytycznej oceny personelu zarządzającego.

Najczęściej, kierownictwo organizacji jest świadome zagrożeń i zaangażowane w rozwiązywanie problemów bezpieczeństwa informacyjnego, chociaż świadomość ta jest zazwyczaj powierzchowna. Pojawiające się często w raportach pokontrolnych stwierdzenie, że z *inicjatywy kierownictwa podejmowane są systematyczne działania zmierzające do zapewnienia bezpieczeństwa informacji* jest w większości przypadków kurtuazyjne – wszelkie działania są praktycznie zawsze podejmowane przez służby informatyczne przedsiębiorstwa bądź są oddolną inicjatywą szeregowych pracowników.

W swojej pracy autorzy stykali się z różnym podejściem kierownictwa do swoich pracowników i zadań bezpieczeństwa informacji: od autorytarnego po przyjacielskie. Analizując poszczególne przypadki okazuje się, że takie działania nie przynoszę oczekiwanych efektów, a nawet są szkodliwe. Do rzadkości należały przypadki, kiedy kierownictwo było świadomie oszukiwane w temacie bezpieczeństwa. Przypadki te zdążały się wyłącznie w podmiotach ze skrajnym traktowaniem personelu.

Zazwyczaj, w tym obszarze, największe zastrzeżenia audytorów budziły skromne zasoby ludzkie oddelegowane do utrzymania systemów informacyjnych

w stanie funkcjonalności. Szacuje się, że na jednego pracownika komórki informatycznej powinno przypadać od 25 do 50 użytkowników komputerów. Zalecenia amerykańskie (2017 rok) są jeszcze bardziej rygorystyczne i pokazują, że personel informatyczny powinien stanowić około 3% osób wykorzystujących komputery.

Rozdział 3

Polityki bezpieczeństwa informacji

3.1. Komponenty Polityki Bezpieczeństwa podmiotu

Podstawowym zadaniem kierownictwa podmiotu jest opracowanie wytycznych dotyczących działań na rzecz bezpieczeństwa informacji, zgodnie z zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami wewnętrznymi. Wytyczne te stanowią podstawę tworzenia Polityki Bezpieczeństwa Informacyjnego – podstawowego dokumentu określającego działania personelu podmiotu, mające na celu zagwarantowanie bezpieczeństwa informacji gromadzonej, przetwarzanej i udostępnianej przez pracowników podmiotu za pośrednictwem jego systemów informacyjnych.

Zgodnie z Normą, podmiot w obszarze *polityk bezpieczeństwa*, powinien posiadać PBI, odpowiadającą celowi istnienia organizacji, zawierającą cele działań w obszarze bezpieczeństwa informacji. Polityka powinna zawierać zobowiązanie do spełnienia wymagań dotyczących bezpieczeństwa informacji, a także obligować pracowników do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. PBI powinna być przygotowana w formie zatwierdzonego przez Zleceniodawcę dokumentu, ogłoszonego i dostępnego dla właściwych stron. Zbiór polityk bezpieczeństwa informacji, będących opisem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), dotyczących różnych aspektów jego funkcjonowania, powinien być opracowany przez powołany do tego celu zespół i zatwierdzony przez kierownictwo, a następnie, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym. Ponadto, polityki należy poddawać okresowym przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, w celu potwierdzenia, że nadal są one właściwe, adekwatne i skuteczne.

3.2. Działania audytorów

Audytor powinien poprosić przedstawiciela organizacji o przedstawienie istniejącej Polityki Bezpieczeństwa Informacyjnego (PBI). W badanych podmiotach spotykano różne struktury PBI. Najczęściej był to jeden zwarty dokument przygotowany zgodnie z wymaganiami Ustawy o ochronie danych osobowych (Dz. U. 2014, poz. 1182), rzadziej z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016). W niewielkiej części przypadków przedstawiana PBI miała postać strukturalizowanego dokumentu, w którym dokument główny opisywał podstawowe działania

związane z ochroną informacji, a przypadki szczegółowe definiowane były w politykach, regulaminach i instrukcjach, będącymi ich załącznikami.

W przykładzie 3 zaprezentowano przykładowe dokumenty składowe PBI. Polityka podmiotu powinna zawierać wyłącznie te spośród nich, które dotyczą działań wykonywanych w systemie informacyjnym podmiotu. Rzadko zdarza się, aby PBI podmiotu zawierała więcej niż 50-60% przedstawionych poniżej dokumentów. Czasami, osoby odpowiadające za bezpieczeństwo zasobów podmiotu, chcąc maksymalnie uprościć korzystanie z PBI starają się uprościć (zminimalizować rozmiar) Polityki. W ten sposób spotykano *kompletne* dokumenty o objętości 5 stron. Oczywiście, nie należy kierować się objętością dokumentów jako kryterium ich przydatności. Możemy zatem przyjąć, że wzorcowa PBI jednego przedsiębiorstwa ma objętość kilku- kilkunastu stron, innego zaś kilkuset. W większości przypadków rozmiar znajduje się w zakresie 70-150 standardowych stron.

Przykład 3. Dokumenty Polityki Bezpieczeństwa Informacyjnego

1. Wykaz celów i zadań zapewniania bezpieczeństwa informacji;
2. Wykaz zagrożeń bezpieczeństwa informacji;
3. Wykaz przetwarzanych danych wrażliwych;
4. Polityka ochrony antywirusowej;
5. Polityka zarządzania hasłami;
6. Polityka zarządzania danymi osobowymi;
7. Polityka szyfrowania:
    a. Zasady zarządzania kluczami szyfrowania;
    b. Zakres wykorzystania narzędzi kryptograficznych;
8. Polityka zarządzania incydentami bezpieczeństwa informacyjnego;
9. Instrukcja obsługi komputerów i pracy w systemie informacyjnym;
10. Instrukcja pracy z oprogramowaniem aplikacyjnym;
11. Regulamin dopuszczalnego użytkowania systemu informacyjnego;
12. Regulamin korzystania z poczty e-mail;
13. Regulamin korzystania z sieci Internet;
14. Regulamin przyznawania dostępu do zasobów informacyjnych i aplikacji;
15. Regulamin przyznawania dostępu do zasobów sieci zewnętrznych;
16. Regulamin przyznawania dostępu do pomieszczeń;
17. Regulamin obsługi technicznej i modernizacji zasobów programowych i technicznych:
    a. Zasady zapewniania fizycznej niezmienności zasobów sprzętowych;
18. Regulamin zarządzania systemem bezpieczeństwa informacji;
19. Regulamin zatwierdzania i wnoszenia zmian do obowiązujących zasad zapewniania bezpieczeństwa informacji;

20. Zasady zakładania, usuwania i modyfikacji kont dostępowych użytkowników:
    a. Wzór wniosku o założenie konta;
    b. Wzór karty konta użytkownika;
21. Rozporządzenie dotyczące zarządzania strumieniami informacyjnymi;
22. Rozporządzenie dotyczące kształcenia i weryfikacji wiedzy z obszaru bezpieczeństwa informacyjnego;
23. Rozporządzenie dotyczące zasad sporządzania i magazynowania kopii zapasowych;
24. Rozporządzenie dotyczące skanowania zagrożeń bezpieczeństwa informacji;
25. Rozporządzenie dotyczące wykorzystania urządzeń mobilnych i nośników informacji;
26. Rozporządzenie dotyczące zasad funkcjonowania i dostępu do węzłów serwerowych:
    a. Wzór karty dostępu do pomieszczeń serwerowych;
27. Polityka zapewniania zdalnego dostępu do zasobów systemu informacyjnego:
    a. Zasady korzystania z prywatnych kanałów komunikacyjnych VPN;
28. Polityka zapewniania ochrony fizycznej systemu informacyjnego;
29. Metodyka analizy ryzyka w bezpieczeństwie informacyjnym.
30. Regulamin pracy Departamentu Informatyki;
31. Rozporządzenie o bezpieczeństwie płatności elektronicznych;
32. Wzór umowy o pracę, uwzględniający wymagania zachowania poufności.
33. Rozporządzenie o klasyfikacji zasobów systemu informacyjnego;
34. Rozporządzenie o inwentaryzacji zasobów systemu informacyjnego;
35. Polityka zapewniania ciągłości pracy systemu informacyjnego;
36. Alternatywny plan działań awaryjnych;
37. Instrukcje stanowiskowe pracowników, np.:
    a. Opis stanowiska pracy Administratora bezpieczeństwa informacji;
    b. Opis stanowiska pracy Kierownika działu oprogramowania aplikacyjnego;
    c. Opis stanowiska pracy pracownika działu oprogramowania aplikacyjnego;
    d. Opis stanowiska pracy Administratora systemu informacyjnego itp.;
38. Polityka rozwoju systemu informacyjnego;
39. Wzory formularzy:
    a. Zapotrzebowanie na sprzęt komputerowy;
    b. Przyjęcie środka trwałego;
    c. Przemieszczanie środka trwałego;

d. Ochrona obszaru przetwarzania i monitorowania ochrony zasobów danych osobowych;
e. Instrukcja zarządzania sprzętem komputerowym:
    i. Zapotrzebowanie na sprzęt komputerowy;
    ii. Przyjęcie środka trwałego;
    iii. Protokół do typowania likwidacji sprzętu komputerowego;
    iv. Procedura zarządzania oprogramowaniem;
    v. Zapotrzebowanie na oprogramowanie;
    vi. Porozumienie w sprawie właściwego korzystania z oprogramowania;
    vii. Rejestr porozumień;
    viii. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
    ix. Upoważnienie do przetwarzania danych osobowych poza bazą danych systemu informatycznego;
    x. Wniosek o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych;
    xi. Upoważnienie do wykonywania czynności związanych z przetwarzaniem danych osobowych we wskazanym zakresie;
    xii. Ewidencja osób upoważnionych do przetwarzania danych osobowych. ■

Jak dotąd, autorzy jeden raz spotkali się z brakiem jakiejkolwiek polityki w przedsiębiorstwie. Miały miejsce również przypadki, kiedy w przedsiębiorstwie funkcjonowały niezależne instrukcje i regulaminy, które powinny jako zintegrowana całość tworzyć PBI. Dlatego, autorzy w swojej pracy wykorzystują następująca sekwencję kroków:

1. Przedstawiciel podmiotu jest informowany o konieczności przedstawienia PBI;
2. Podmiotowi przekazywana jest lista typowych komponentów PBI, na przykład zgodna z przykładem 3 oraz lista pytań, które będą zadawane w trakcie wspólnej analizy przedstawionej PBI. Zestaw typowych pytań pokazano w przykładzie 4;
3. Podmiot, w zależności od potrzeb otrzymuje 7-14 dni na przygotowanie się do wspólnej analizy posiadanej Polityki Bezpieczeństwa Informacyjnego.

Przykład 4. Typowe pytania dotyczące Polityki

1. Czy znane są główne zasoby informatyczne, takie jak systemy informacyjne, bazy danych, informacje o poszczególnych faktach i zjawiskach, które mają najwyższy priorytet dla całego przedsiębiorstwa?

2. W jaki sposób określono zasady, kryteria i wymagania dotyczące procedur obiegu informacji, elementów infrastruktury informatycznej, oprogramowania i sprzętu itp.?
3. Czy istnieje w firmie dokument opisujący podział ról i funkcji odnoszących się do rozwiązywania konkretnych problemów bezpieczeństwa?
4. Czy w firmie istnieją dokumenty opisujące procedury wykonywane w przypadku wykrycia zagrożeń bezpieczeństwa informacyjnego?
5. W jaki sposób podejmowane są decyzje o odstępstwie od standardowych procedur i podejmowania nieszablonowych badań w obszarze bezpieczeństwa informacji?
6. Czy istnieje wykaz osób lub jednostek, odpowiedzialnych za bezpośrednią pracę z pracownikami przedsiębiorstwa w sprawach dotyczących bezpieczeństwa?
7. Czy w firmie istnieje podział informacji względem poziomu jej ważności i poufności?
8. Czy przewidziano specjalny sposób postępowania z informacją będącą wynikiem prac naukowo-badawczych realizowanych w przedsiębiorstwie, przykładowo:
    a. Specjalne wymagania tworzenia kopii zapasowych danych (wyższa częstotliwość tworzenia kopii, kopiowanie i korzystanie z bardziej niezawodnych nośników danych);
    b. Specjalne wymagania dotyczące identyfikacji i uwierzytelniania użytkowników (łączenie biometrycznej identyfikacji i uwierzytelniania za pomocą hasła);
    c. Dodatkowe wymagania określające wykorzystanie kopiarek do powielania poufnych informacji;
    d. Specjalne wymagania w stosunku do pomieszczeń, w których odbywają się spotkania o tajnej tematyce i przetwarzane są odpowiednie informacje (grubość i materiał ścian, położenie pomieszczeń w budynkach, bezpieczeństwo okien, niezawodność drzwi i zamknięć, a także wykorzystanie sygnalizacji przeciwwłamaniowej i badania pod kątem urządzeń podsłuchujących itp.);
9. Czy określone są formalne zasady publikowania jawnych materiałów informacyjnych, w tym zasady organizacji strony internetowej przedsiębiorstwa i jego wewnętrznego portalu informacyjnego (w celu zapobiegania ewentualnym wyciekom i zniekształceniom informacji)?
10. W jaki sposób normowane są zasady korzystania z sieci Internet (w celu zapobiegania ewentualnym wyciekom i zniekształceniom informacji)?
11. Czy istnieją zasady korzystania z konkretnych technologii informacyjnych i komunikacyjnych, w tym wspólne dla całego przedsiębiorstwa zasady korzystania z mobilnych komputerów i smartfonów, zdalnego dostępu do korporacyjnych

systemów informatycznych, a także korzystania z osobistych komputerów pracowników do firmowych celów?

12. Czy dokonano klasyfikacji systemów informatycznych, zasobów informacyjnych oraz innych obiektów zawierających informacje z punktu widzenia ich znaczenia i nakładów, które należy ponieść w celu ich ochrony?
13. Jakie są zasady zakupu, instalacji, modyfikacji i aktualizacji oprogramowania, a także outsourcingu tworzenia i projektowania oprogramowania?
14. Czy istnieją zdefiniowane zasady zakupów sprzętu, systemów informatycznych, systemów bezpieczeństwa?
15. W jaki sposób uregulowano korzystanie przez użytkowników z własnego oprogramowania?
16. Czy zdefiniowana jest polityka ochrony przed złośliwymi programami?
17. Czy zdefiniowana jest polityka wykorzystania środków telekomunikacji?
18. Czy zdefiniowana jest polityka wykorzystania sieci VPN?
19. Czy istnieją ogólne (dla całego przedsiębiorstwa) zasady użycia haseł i innych środków osobistej identyfikacji?
20. Czy sformalizowano zasady korzystania z podpisu cyfrowego i infrastruktury kluczy publicznych?
21. W jaki sposób uregulowano korzystanie z poczty elektronicznej? W szczególności, czy uwzględniono następujące wymagania:
    a. Zakaz używania adresu e-mail do celów osobistych;
    b. Specjalne wymagania dotyczące wysyłania i odbierania załączników, które mogą potencjalnie zawierać szkodliwe oprogramowanie;
    c. Zakaz używania adresu e-mail przez pracowników tymczasowych;
    d. Obligatoryjność szyfrowania wysyłanych wiadomości;
    e. Monitorowanie wszystkich przychodzących i wysyłanych wiadomości;
    f. Ograniczenia na przekazywanie poufnych informacji za pomocą poczty e-mail;
22. Czy stworzony został regulamin fizycznej ochrony aktywów informacyjnych?
23. Jak uregulowano zasady dostępu do wewnętrznych zasobów informacyjnych użytkowników (organizacji) zewnętrznych? W szczególności:
    a. Jakie dokumenty uprawniają do wejścia na teren zakładu? Na podstawie jakich dokumentów władzy państwowej możliwe jest wejście na teren przedsiębiorstwa?
    b. W jaki sposób limitowane jest wykorzystanie dokumentów uprawniających do wejścia na teren zakładu (ograniczony czas ważności legitymacji, czas ewentualnego wejścia na teren zakładu)?
    c. Jak określono zasady wydawania, wymiany, przedłużenia przepustek, a także sposoby postępowania w przypadku ich utraty?

d. Czy sformalizowano obieg dokumentów, stosowanych przy wejściu zwiedzających na teren zakładu, jakie są zasady wydawania jednorazowych przepustki?
e. Jakie są zasady kontroli pojazdów wpuszczanych na teren zakładu?

24. Czy istnieją wspólne dla całego przedsiębiorstwa zasady pociągania do odpowiedzialności za naruszenie zasad bezpieczeństwa?
25. Czy uregulowano postępowanie w przypadku pojawienia się sytuacji nadzwyczajnych?■

3.3. Przykład Głównej Polityki Bezpieczeństwa Informacyjnego

W przykładzie 5 przedstawiono wzór głównej Polityki Bezpieczeństwa. Jego opis przedstawiamy na końcu paragrafu.

Przykład 5. Dokument główny Polityki bezpieczeństwa informacyjnego

Wersja dokumentu	1.0	Data	28.02.2018

Zatwierdzam

_____
(*Data i podpis Kierownika jednostki*)

POLITYKA BEZPIECZEŃSTWA INFORMACJI JEDNOSTKI ORGANIZACYJNEJ

METRYKA

Nazwa jednostki organizacyjnej	Jednostka organizacyjna		
Tytuł dokumentu	Polityka bezpieczeństwa informacji – dokument główny		
Opis	Polityka bezpieczeństwa informacji jest dokumentem określającym cele i zadania systemu zarządzania bezpieczeństwem informacji oraz wprowadzającym zbiór zasad, wymagań i wytycznych w zakresie, którymi jednostka organizacyjna kieruje się w swej działalności w obszarze bezpieczeństwa informacji.		
Zastosowanie	Polityka bezpieczeństwa informacji obejmuje swym działaniem wszystkie działy jednostki organizacyjnej, a jej przestrzeganie jest obowiązkowe dla wszystkich pracowników. Postanowienia niniejszej Polityki przeznaczone są do wykorzystania w wewnętrznych dokumentach normatywnych i metodycznych, a także w podpisywanych umowach.		
Plik	00 - Polityka bezpieczeństwa - dokument główny ver6.docx		
Status	Dokument roboczy	Liczba stron	16

HISTORIA DOKUMENTU

Wersja	Data wersji	Opis	Akcja[1]	Rozdziały[2]	Autorzy	Zatwierdził

[1] Utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.
[2] Wymienić rozdziały, w których dokonano zmian.

I. Deklaracja kierownictwa

1. Kierownik jednostki organizacyjnej oświadcza, że kierownictwo jednostki ma świadomość znaczenia przetwarzanych informacji dla realizacji misji jednostki organizacyjnej i potrzeby ochrony informacji poprzez budowę systemu zarządzania jej bezpieczeństwem.
2. Kierownik jednostki deklaruje wspieranie wszelkich działań mających na celu poprawę bezpieczeństwa informacji gromadzonej, przetwarzanej i udostępnianej przez jednostkę. W szczególności działania te obejmować będą:
    a. Permanentną weryfikację celów bezpieczeństwa informacji i dostosowanie ich do strategicznych kierunków rozwoju jednostki organizacyjnej;
    b. Integrację procedur zarządzania bezpieczeństwem informacji z procesami jednostki organizacyjnej;
    c. Troskę o zapewnienie dostępności wiedzy i zasobów technicznych, potrzebnych do zarządzania bezpieczeństwem informacji;
    d. Systematyczne akcentowanie na forum jednostki organizacyjnej znaczenia skutecznego zarządzania bezpieczeństwem informacji oraz konieczności stosowania się do zaleceń PBI;
    e. Wspieranie osób przyczyniających się do poprawy skuteczności systemu zarządzania bezpieczeństwem informacji;
    f. Promowanie wśród pracowników ciągłego doskonalenia wiedzy z obszaru bezpieczeństwa informacji.
3. Kierownictwo jednostki organizacyjnej dołoży wszelkich starań, aby PBI:
    a. Odpowiadała celowi istnienia jednostki organizacyjnej;
    b. Stymulowała ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji.
4. Zasady działania, kompetencje i zakresy odpowiedzialności, opisane w dokumentach PBI obowiązują wszystkich pracowników jednostki organizacyjnej oraz podmiotów z nią współpracujących.
5. PBI będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy PBI, będą odbywać się nie rzadziej niż raz w roku.
6. Niniejsza Polityka Bezpieczeństwa Informacji jest oparta na normie PN-ISO/IEC 27001:2014-12.

II. Terminy, definicje, wykorzystywane skróty

II.1. Terminy i definicje

1. *Administrator bezpieczeństwa informacji* – specjalista, sprawujący nadzór nad zapewnieniem ochrony informacji w systemie informacyjnym, a także organi-

zujący działania mające na celu wykrywanie i zapobieganie pojawianiu się kanałów wycieku informacji, a także możliwości niesankcjonowanego dostępu do chronionych informacji.

2. *Administrator systemów informacyjnych* – specjalista, sprawujący nadzór nad systemami informatycznymi, przeznaczonymi do gromadzenia, przetwarzania i udostępniania informacji.
3. *Aktywa informacyjne* – systemy informacyjne, narzędzia informacyjne, zasoby informacyjne.
4. *Analiza ryzyka* – systematyczne korzystanie z dostępnych informacji w celu określenia źródeł i oceny poziomu ryzyka.
5. *Audyt bezpieczeństwa informacyjnego* – proces kontroli wypełnienia ustalonych wymagań w zakresie bezpieczeństwa informacji. Może być realizowany samodzielnie (audyt wewnętrzny), jak i przez niezależne organizacje zewnętrzne (audyt zewnętrzny). Wyniki kontroli potwierdzane są przez świadectwo audytu.
6. *Bezpieczeństwo informacyjne* – mechanizm ochronny, zapewniający poufność, integralność, dostępność informacji, gwarantujący bezpieczeństwo aktywów informacyjnych społeczeństwa w warunkach zagrożeń w sferze informacyjnej. Zagrożenia mogą być spowodowane zamierzonymi błędami pracowników, nieprawidłowym funkcjonowaniem urządzeń technicznych, klęskami żywiołowymi lub awariami (pożar, powódź, wyłączenie zasilania, uszkodzenie kanałów telekomunikacyjnych i in.), bądź celowymi działaniami przestępczymi, prowadzącymi do naruszenia aktywów informacyjnych.
7. *Bezpieczny kanał transmisji danych* – logiczne i fizyczne kanały komunikacji sieciowej, chronione przed podsłuchaniem przez potencjalnych cyberprzestępców za pomocą szyfrowania, albo poprzez ich fizyczną izolację i rozmieszczenie w chronionej przestrzeni.
8. *Dostęp do informacji* – możliwość uzyskania informacji i jej wykorzystania.
9. *Dostępność* – właściwość systemu informacyjnego gwarantująca, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
10. *Identyfikacja* – przypisanie podmiotom (użytkownikom procesów) i obiektom dostępu (zasobom informacyjnym, urządzeniom) identyfikatora i/lub porównanie okazanego identyfikatora z listą przypisanych identyfikatorów.
11. *Identyfikator dostępu* – unikalna cecha podmiotu lub obiektu dostępu.
12. *Incydent bezpieczeństwa* – zrealizowane lub prawdopodobne zagrożenie bezpieczeństwa informacji, prowadzące do naruszenia dostępności, poufności i integralności aktywów informacyjnych.

13. *Informacja poufna* – informacja z ograniczonym dostępem, nie zawierająca jednak treści stanowiących tajemnicę państwową, do których dostęp jest ograniczony, zgodnie z ustawodawstwem Rzeczypospolitej Polskiej.
14. *Informacje* – aktywa, które podobnie jak inne aktywa posiadające wartość, wymuszają ich odpowiednią ochronę.
15. *Integralność* – właściwość systemu informacyjnego zapewniająca, że informacje są kompletne i dokładne oraz że są przetwarzane w kontrolowany sposób.
16. *Narzędzia informacyjne* – narzędzia programowe, techniczne, lingwistyczne, prawne i organizacyjne wykorzystywane lub tworzone w trakcie projektowania systemów informacyjnych i umożliwiające ich późniejszą eksploatację.
17. *Poufność* – właściwość systemu informacyjnego zapewniająca, że chroniona informacja dostępna jest jedynie dla osób upoważnionych.
18. *System informacyjny* – zestaw programów i środków technicznych służący do przechowywania, przetwarzania i przesyłania informacji w celu rozwiązania zadań.
19. *System przetwarzania* – system, składający się z pracowników oraz zestawu środków programowo-technicznych, realizujący informacyjną technologię wykonywania określonych funkcji.
20. *System zarządzania bezpieczeństwem informacyjnym* – zestaw środków programowych, technicznych i organizacyjnych przeznaczonych do zarządzania bezpieczeństwem zasobów informacyjnych.
21. *Technologie informacyjne* – procesy oraz metody wyszukiwania, gromadzenia, przechowywania, przetwarzania, udostępniania, rozpowszechniania informacji i sposoby realizacji takich procesów i metod.
22. *Uwierzytelnienie* – sprawdzenie przynależności podmiotowi dostępu, zadeklarowanej przez niego tożsamości, potwierdzenie jego autentyczności.
23. *Zapewnienie bezpieczeństwa przetwarzanych informacji* rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka dotyczącego zasobów stanowiących przedmiot niniejszej Polityki.
24. *Zarządzanie ryzykiem* to proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.
25. *Zasoby informacyjne* – zbiór informacji zawartych w bazach danych i technologii informacyjnych zapewniających ich przetwarzanie.
26. *Źródło zagrożenia* – zamiar lub metoda, ukierunkowana na celowe wykorzystanie luki w zabezpieczeniach, albo sytuacja bądź metoda, które mogą przypadkowo ujawnić lukę w zabezpieczeniach.

II.2. Wykorzystywane skróty

IOD	–	Inspektor Ochrony Danych
ASI	–	Administrator Systemów Informacyjnych
DIP	–	Dział Informatyki Przedsiębiorstwa
SIP	–	System Informacyjny Przedsiębiorstwa
SZBI	–	System Zarządzania Bezpieczeństwem Informacji
PBI	–	Polityka Bezpieczeństwa Informacji

II.3. Postanowienia ogólne

1. Polityka bezpieczeństwa informacyjnego Przedsiębiorstwa określa cele i zadania zarządzania bezpieczeństwem informacji oraz wprowadza metody, środki zasady, wymagania i wytyczne, którymi kieruje się Przedsiębiorstwo w swej działalności w obszarze bezpieczeństwa informacji.
2. DIP jest jednostką organizacyjną Przedsiębiorstwa odpowiadającą za eksploatację SIP. SIP to zestaw środków programowo-technicznych wspomagających informacyjne funkcjonowanie Przedsiębiorstwa.
3. PBI oparta została na założeniu, że największe zagrożenie destabilizacji działania SIP stwarza personel zarządzający. Jego działania mogą być motywowane zamiarem wyrządzenia szkód, albo mieć niezamierzenie błędny charakter. Przyjęto, że w realizacji swoich działań, osoba atakująca może mieć wspólników, zarówno wewnątrz jak i na zewnątrz struktury organizacyjnej SIP.
4. Poziom ryzyka awarii i niesprawności technicznych warunkuje stan wyposażenia SIP, niezawodności systemów zaopatrzenia w energię i usługi telekomunikacyjne, kwalifikacje personelu i jego zdolność do skutecznych działań przy pojawieniu się zagrożeń.

III. Polityki bezpieczeństwa informacyjnego

III.1. Cele PBI

1. Głównym celem PBI jest ochrona informacji pozyskiwanej, gromadzonej i przetwarzanej przez Przedsiębiorstwo za pośrednictwem SIP oraz zapewnienie efektywnego funkcjonowania SIP przy wykonywaniu działalności określonej w Statucie Przedsiębiorstwa.
2. Celami szczegółowymi PBI są:
    a. Zapewnienie zgodności z obowiązującym prawem procedur gromadzenia, przetwarzania i udostępniania informacji;
    b. Ochrona zasobów informacyjnych przed utratą lub niewłaściwym wykorzystaniem;
    c. Ochrona wizerunku Przedsiębiorstwa przed kompromitacją będącą skutkiem niewłaściwego wykorzystania informacji;

d. Uzyskanie i permanentne utrzymanie akceptowalnego poziomu bezpieczeństwa zasobów, rozumianego jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań;
e. Zagwarantowanie ciągłości procesów biznesowych i właściwej reakcji na incydenty bezpieczeństwa;
f. Zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników i współpracowników Przedsiębiorstwa.

III.2. Zadania PBI

1. PBI ma na celu ochronę aktywów informacyjnych i technicznych przed zagrożeniami będącymi wynikiem działań niezgodnych z prawem, niezamierzonych błędnych czynności personelu, awarii technicznych, niewłaściwych technologii i rozwiązań organizacyjnych w procesach gromadzenia, przetwarzania, przesyłania i przechowywania informacji, zmniejszenie ryzyka oraz minimalizację potencjalnych szkód będących wynikiem awarii, a także zapewnienie prawidłowego funkcjonowania procesów technologicznych Przedsiębiorstwa.
2. Do szczegółowych zadań PBI należą:
    a. Wsparcie Kierownictwa Przedsiębiorstwa w procesie budowy i eksploatacji SZBI;
    b. Zdefiniowanie szczegółowych PBI;
    c. Budowa i eksploatacja SZBI, bazującego na udokumentowanej PBI;
    d. Zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu;
    e. Ochrona informacji, a w szczególności informacji prawnie chronionych;
    f. Zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności SIP;
    g. Ochrona informacji związanych z zawartymi umowami;
    h. Wdrażanie, eksploatacja i rozwój SIP z zachowaniem zasad bezpieczeństwa informacji;
    i. Edukacja użytkowników SIP;
    j. Okresowe przeglądy SZBI.

III.3. Okres funkcjonowania i zasady wprowadzania zmian

1. Niniejsza PBI zostaje wprowadzona w życie decyzją Prezesa.
2. PBI zostaje wycofana z użycia decyzją Prezesa.
3. Zmiany w PBI są wnoszone na podstawie decyzji Prezesa.
4. Wniesienie zmian w PBI mogą inicjować:
    a. Prezes;

b. Dyrektor DIP oraz ASI SIP.

5. Planowa aktualizacja PBI ma na celu zapewnienie zgodności określonych przez nią środków bezpieczeństwa z warunkami rzeczywistymi i aktualnymi formalno-prawnymi wymogami ochrony informacji.
6. Nadzwyczajna aktualizacja PBI jest wykonywana obligatoryjnie w następujących przypadkach:
    a. W przypadku zmiany polityki Rzeczpospolitej Polskiej w obszarze bezpieczeństwa informacyjnego, zmiany ustaw i rozporządzeń w obszarze ochrony informacji;
    b. Przy zmianie wewnętrznych dokumentów normatywnych (instrukcji, zasad, wytycznych) Przedsiębiorstwa, dotyczących zarządzania bezpieczeństwem informacji;
    c. Po wykryciu i identyfikacji zdarzenia (zdarzeń) naruszającego bezpieczeństwa informacji, skutkującego materialną lub niematerialną szkodą Przedsiębiorstwa.
7. Osobą odpowiedzialną za planową i nieplanową aktualizację PBI jest Dyrektor DIP.
8. Nadzór nad przestrzeganiem wymagań niniejszej PBI oraz utrzymaniem jej w aktualnym stanie spoczywa na Dyrektorze DIP.

III.4. Przeglądy okresowe polityk bezpieczeństwa informacji

1. Zarówno PBI i DIP jak i stanowiące jej załączniki polityki cząstkowe powinny być regularnie weryfikowane.
2. Weryfikacji PBI i jej polityk cząstkowych dokonuje zespół powoływany przez Dyrektora DIP, w którego skład wchodzą:
    a. Inspektorzy ochrony danych IOD wszystkich podmiotów w funkcjonowaniu SIP, będących w prawnej zależności od Przedsiębiorstwa;
    b. Administrator systemów informacyjnych ASI Przedsiębiorstwa;
    c. Przedstawiciel Biura prawnego Przedsiębiorstwa;
    d. Dyrektor DIP, będący właścicielem polityki, odpowiadającym za jej opracowanie, wykorzystanie, przegląd oraz ocenę.
3. PBI i jej polityki cząstkowe powinny być poddawane weryfikacji raz w roku kalendarzowym lub wtedy, gdy wystąpią istotne zmiany, mogące wpłynąć na ich adekwatność i skuteczność.
4. Przegląd polityk powinien obejmować określenie możliwości ich udoskonalenia poprzez zmiany w środowisku organizacyjnym, warunkach biznesowych, prawnych lub środowisku technicznym.
5. Zmiany w Polityce i politykach cząstkowych, zaproponowane przez zespół zatwierdza Prezes. Zmodyfikowane polityki wchodzą w życie 30 dni po ich zatwierdzeniu.

IV. Szczegółowe polityki bezpieczeństwa informacji

1. Zasady postępowania regulują szczegółowe polityki bezpieczeństwa, będące załącznikami do niniejszej Polityki.
2. Szczegółowe zasady zapewniania bezpieczeństwa zasobów ludzkich zostały przedstawione w Załączniku 1 do niniejszej PBI.
3. Szczegółowe zasady zarządzania kontami dostępowymi użytkowników zostały przedstawione w Załączniku 2 do niniejszej PBI.
4. Szczegółowe zasady zarządzania hasłami dostęp, zostały przedstawione w Załączniku 3 do niniejszej PBI.
5. Szczegółowe zasady ochrony przed programami złośliwymi zostały przedstawione w Załączniku 4 do niniejszej PBI.
6. Szczegółowe zasady komunikacji elektronicznej zostały przedstawione w Załączniku 5 do niniejszej PBI.
7. Szczegółowe zasady korzystania z sieci lokalnej zostały przedstawione w Załączniku 6 do niniejszej PBI.
8. Szczegółowe zasady wykorzystania sieci Internet zostały przedstawione w Załączniku 7 do niniejszej PBI.
9. Szczegółowe zasady wykorzystania zdalnego dostępu zostały przedstawione w Załączniku 8 do niniejszej PBI.
10. Szczegółowe zasady korzystania z urządzeń mobilnych zostały przedstawione w Załączniku 9 do niniejszej PBI.
11. Szczegółowe zasady dostępu do pomieszczeń, w których przetwarzane są informacje niejawne, zostały przedstawione w Załączniku 10 do niniejszej PBI.
12. Szczegółowe zasady kształcenia w zakresie bezpieczeństwa zostały przedstawione w Załączniku 11 do niniejszej PBI.
13. Szczegółowe zasady archiwizacji zasobów informacyjnych zostały przedstawione w Załączniku 12 do niniejszej PBI.
14. Szczegółowe zasady postępowania z danymi osobowymi zostały przedstawione w Załączniku 13 do niniejszej PBI.
15. Szczegółowe zasady postępowania w przypadku obliczania ryzyka utraty danych przedstawione zostały w załączniku 14 do niniejszej PBI.

V. Organizacja bezpieczeństwa informacji

1. Ogólny nadzór nad bezpieczeństwem informacji sprawuje Prezes. Odpowiedzialność za organizację i przeprowadzenie działań w obszarze bezpieczeństwa informacji oraz kontrolę nad przestrzeganiem przepisów PBI ponosi Dyrektor DIP spełniający jednocześnie, o ile nie postanowiono inaczej, funkcję IOD Przedsiębiorstwa.
2. Dyrektorzy jednostek organizacyjnych Przedsiębiorstwa są odpowiedzialni za realizację wymagań PBI w swoich jednostkach.

3. Pracownicy Przedsiębiorstwa są zobowiązani do przestrzegania zasady postępowania z poufnymi dokumentami, nośnikami kluczowych informacji i inną chronioną informacją, w szczególności do przestrzegania niniejszej Polityki i innych dokumentów SZBI.

VI. Zakres stosowania i rozpowszechniania PBI

1. Niniejszy dokument PBI jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji w jednostce organizacyjnej.
2. Zasady określone przez dokumenty PBI mają zastosowanie do całego systemu informacyjnego Przedsiębiorstwa, w szczególności do:
    a. Wszystkich systemów informatycznych, w których są lub będą przetwarzane informacje podlegające ochronie;
    b. Informacji będących w dyspozycji Przedsiębiorstwa lub innych podmiotów, o ile zostały one przekazane na podstawie umów;
    c. Wszystkich nośników magnetycznych, optycznych i innych, na których są lub będą znajdować się informacje podlegające ochronie;
    d. Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
3. Do stosowania zasad określonych przez dokumenty PBI zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.
4. Z treścią niniejszego dokumentu oraz właściwymi dokumentami niższego rzędu, powinni zapoznać się wszyscy pracownicy Przedsiębiorstwa i inne osoby mające dostęp do informacji przetwarzanej w jednostce, przed przystąpieniem do przetwarzania danych.
5. Niniejszy dokument może być przedstawiany podmiotom, z którymi Przedsiębiorstwo związane jest umowami lub innym jednostkom współpracującym.

VII. Podstawy prawne

1. Niniejszy dokument oraz dokumenty szczegółowe z niego wynikające są zgodne z obowiązującymi przepisami, w szczególności z:
    a. Konstytucją Rzeczpospolitej Polskiej (art. 47, 51);
    b. Ustawą o ochronie danych osobowych (Dz. U. 2014, poz. 1182);
    c. Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 2004, poz. 1502);
    d. Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 nr 182, poz. 1228);
    e. Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2013, poz. 262);
    f. Ustawą z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 Nr 171, poz. 1800);

g. Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934);
h. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536);
i. Rozporządzeniem Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011, Nr 225, poz. 1350);
j. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
k. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
l. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601);
m. Rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 10 lipca 2009 r. zmieniające rozporządzenie w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. 2009 Nr 115, poz. 971);
n. Rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2011 Nr 159, poz. 948);
o. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526);
p. 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 (ogólne rozporządzenie o ochronie danych).

2. Niniejszy dokument będzie aktualizowany w każdym przypadku zmiany przepisów związanych z PBI.
3. Do tworzenia i rozwijania PBI wykorzystane zostały obowiązujące w tym zakresie normy i standardy, a w szczególności:
    a. PN-ISO/IEC 27000:2014 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia;
    b. PN-ISO/IEC 27001:2014 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania;
    c. PN-ISO/IEC-27002:2014 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zabezpieczania informacji.■

Rozdział 4

Organizacja bezpieczeństwa informacji

4.1. Wymagania aktów normatywnych

Celem działań w danym obszarze jest ustanowienie struktury zarządzania dla zainicjowania oraz nadzorowania, wdrażania i eksploatacji bezpieczeństwa informacji u Zleceniodawcy.

Zgodnie z aktami normatywnymi, w obszarze organizacji bezpieczeństwa, podmiot powinien określić i przypisać osobom lub podmiotom odpowiedzialność za bezpieczeństwo informacji. Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą powinny być rozdzielone, co powinno ograniczyć możliwości nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów. Zaleca się również utrzymywanie stosownych kontaktów z właściwymi organami władzy oraz grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa. Ponadto, bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.

Zazwyczaj wymagania normy w powyższym obszarze są w podmiotach spełnione. Obowiązki zarządzania bezpieczeństwem są przypisane do konkretnych pracowników, zostały one określone w zakresie ich obowiązków oraz w stosownych regulaminach PBI. Najczęściej dopracowania wymagają: zasady nadzoru oraz rozliczania pracowników odpowiedzialnych za bezpieczeństwo informacji, formalizacja sposobów komunikowania się (w obszarze bezpieczeństwa) z organami władzy i grupami specjalistów, ustalenie zasad uwzględniania bezpieczeństwa w nowych przedsięwzięciach. Zdaniem autorów rozwiązanie niedociągnięć dotyczących sposobów komunikowania w dużej części leży poza możliwościami działów informatyki większości podmiotów.

W zakresie bezpieczeństwa telepracy i stosowania urządzeń mobilnych, Norma zaleca wprowadzenie polityk oraz wspierających ją zabezpieczeń, w celu zarządzania ryzykiem, wynikającym z użytkowania urządzeń mobilnych. Norma sugeruje również wdrożenie polityk oraz wspierających ją zabezpieczeń, w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.

Podmioty zazwyczaj ograniczają korzystanie z urządzeń mobilnych, najmniejsze ograniczenia spotykamy w samorządach, największe w przedsiębiorstwach prywatnych. W przypadku ograniczania dostępu, urządzenia mobilne wykorzystywane są do obsługi poczty elektronicznej oraz monitorowania firmowego Internetu wyłącznie przez upoważnionych pracowników. Powyższe działania, a także sam dostęp do zasobów Internetu powinien regulować stosowny Regulamin, który

w większości znanych podmiotów nie został wdrożony. Krytyczną jest usługa dostępu zdalnego do zasobów administracyjnych systemu informacyjnego podmiotu. W takim przypadku regulamin powinien być obowiązkowo opracowany i wdrożony.

4.2. Przykładowe polityki, regulaminy

Przykładowy regulamin określający zasady korzystania ze zdalnego dostępu do zasobów pomiotu stanowi treść przykładu 6. Zauważmy, że zapisy poniższego regulaminu należy wykorzystywać szczególnie w przypadku do zasobów administracyjnych systemu. Dostęp do zasobów udostępnianych klientom może być realizowany na zasadach ogólnych.

Przykład 6. Regulamin korzystania z dostępu zdalnego

I. Terminy, definicje, wykorzystane skróty

I.1. Terminy i definicje

1. *Administrator Systemów Informacyjnych* to specjalista odpowiadających za uruchomienie, bieżącą eksploatację oprogramowania i jej zakończenie.
2. *Dostęp zdalny do zasobów* to wykorzystanie zasobów przez użytkownika, ze stacji roboczej lub dowolnego innego urządzenia dostępowego, spoza fizycznej lokalizacji jednostki organizacyjnej.
3. *Kanał VPN* to tunel wykorzystywany do przesyłania informacji po sieci publicznej, wykorzystujący szyfrowanie do ochrony przesyłanych treści.
4. *Bramka VPN* to urządzenie zlokalizowane w jednostce organizacyjnej, obsługujące kanały VPN i umożliwiające użytkownikowi zdalny dostęp do zasobów systemu informacyjnego.
5. *Urządzenie dostępowe* to urządzenie komputerowe, telekomunikacyjne lub inne, zapewniające użytkownikowi dostęp do zasobów sieci informatycznej.
6. *Informacja niejawna* to wszelki zasób informacyjny, którego treść jest chroniona prawem.
7. *Użytkownik* to pracownik jednostki organizacyjnej, wykorzystujący zasoby informacyjne do realizacji zadań wynikających z zakresu swoich obowiązków.

I.2. Wykorzystane skróty

ASI – Administrator Systemów Informacyjnych
IOD – Inspektor Ochrony Danych
DZ – Dostęp zdalny
PBI – Polityka Bezpieczeństwa Informacji
SIP – System Informacyjny Przedsiębiorstwa

II. Postanowienia ogólne

1. Niniejszy Regulamin określa standardy wykorzystania zasobów SIP za pośrednictwem dowolnej stacji roboczej, zlokalizowanej poza siedzibą Przedsiębiorstwa.
2. Celem wprowadzenia Regulaminu jest minimalizacja ryzyka strat, które mogą powstać w wyniku zdalnego dostępu do zasobów SIP. Straty mogą dotyczyć utraty informacji niejawnych lub ważnych dla jednostki organizacyjnej, własności intelektualnej, szkody na reputacji, uszkodzenia krytycznych systemów wewnętrznych jednostki organizacyjnej i in.
3. Niniejszy Regulamin jest częścią PBI SIP i obowiązuje we wszystkich jednostkach organizacyjnych korzystających z zasobów SIP.
4. Podstawowymi zasadami bezpiecznego wykorzystania zdalnego dostępu do zasobów są:
    a. Użytkownicy korzystający z dostępu zdalnego do zasobów SIP są zobowiązani do bezwzględnego unikania wszelkich działań naruszających bezpieczeństwo informacji;
    b. Zdalny dostęp do zasobów SIP należy wykorzystywać wyłącznie w ramach obowiązków służbowych;
    c. Użytkownik korzystający z DZ, ponosi pełną odpowiedzialność za swoje działania.

III. Zasady wykorzystania dostępu zdalnego do zasobów

1. Decyzja o przyznaniu użytkownikowi jednostki organizacyjnej zdalnego dostępu do zasobów SIP wydawana jest przez IOD, na wniosek bezpośredniego przełożonego użytkownika, po uzyskaniu pozytywnej opinii ASI w zakresie możliwości technicznych realizacji dostępu.
2. Wzór wniosku o przyznanie DZ stanowi treść Załącznika 1 do niniejszego Regulaminu.
3. Każdy z użytkowników, wykorzystujących DZ, musi mieć ściśle określony zakres praw dostępu do systemu, aplikacji i usług SIP, a także zaakceptowany przez ASI rodzaj sprzętu, z którego połączenie będzie realizowane. Zakres dostępu jest określany przez bezpośredniego przełożonego użytkownika i wpisywany do Wniosku o przyznanie dostępu zdalnego.
4. Zmiany zakresu dostępu wykorzystywanego sprzętu, a także blokowanie DZ realizowane są na pisemny wniosek bezpośredniego przełożonego użytkownika, zaopiniowany pozytywnie przez IOD i ASI w zakresie możliwości technicznych. Jeżeli działania użytkownika, wykorzystującego DZ, zagrażają bezpieczeństwu SIP, ASI niezwłocznie blokuje DZ, o czym informuje IOD oraz bezpośredniego przełożonego użytkownika.

5. IOD prowadzi ewidencję Użytkowników posiadających zdalny dostęp do zasobów SIP, która zawiera datę uzyskania, zmiany i zablokowania dostępu, zakres dostępu oraz informacje na temat rodzaju sprzętu wykorzystywanego do połączeń i jego zmian. Wszelkie informacje dotyczące dostępu zdalnego użytkownika powinny być umieszczane w Karcie ewidencyjnej użytkownika, o której mowa Polityce zarządzania kontami dostępu.
6. ASI jest odpowiedzialny za możliwości techniczne dostępu zdalnego, eksploatację bramek VPN, weryfikację stanu bezpieczeństwa jednostki komputerowej, z której uzyskiwany będzie zdalny dostęp.
7. Zdalny dostęp do zasobów SIP, realizowany spoza siedziby jednostki organizacyjnej, jest możliwy wyłącznie za pośrednictwem prywatnych kanałów wirtualnych VPN.
8. Korzystając z DZ, należy przestrzegać następujących zasad:
    a. Udostępnianie kanału VPN, przez użytkownika posiadającego dostęp zdalny, innemu użytkownikowi, w celu realizacji dostępu do zasobów SIP jest zabronione;
    b. Dostęp do zasobów przez kanały VPN musi odbywać się na podstawie jednorazowego hasła, generowanego za pomocą tokenu, infrastruktury kluczy publicznych lub innej metody opartej na hasłach jednorazowych;
    c. Jeżeli połączenie VPN jest aktywne, pełny wychodzący i przychodzący ruch użytkownika musi być przesyłany poprzez kanał VPN, pozostały ruch ma być blokowany. Jednoczesne dołączenie komputera do innych sieci, za wyjątkiem sieci prywatnych, nad którymi użytkownik ma pełną kontrolę, jest zabronione;
    d. Zezwala się na jednoczesną realizację wyłącznie jednego prywatnego połączenia sieciowego;
    e. Wszystkie komputery podłączone do SIP przez kanały VPN powinny być wyposażone w aktualne wersje oprogramowania chroniącego przed programami złośliwymi. Jeżeli komputer może stanowić zagrożenie dla bezpieczeństwa SIP, w tym zawartej w nim informacji, ASI ma prawo nie dopuścić do wykorzystania jego jako narzędzia uzyskania dostępu zdalnego;
    f. Zdalny dostęp do zasobów SIP może odbywać się wyłącznie za pośrednictwem jednostki komputerowej zweryfikowanej przez ASI na etapie uzyskiwania dostępu. Na zmianę sprzętu zezwala IOD po uzyskaniu wniosku bezpośredniego przełożonego użytkownika, pozytywnie zaopiniowanego przez ASI;
    g. Użytkownicy spoza jednostki organizacyjnej mogą uzyskać dostęp do kanałów VPN dopiero po dostosowaniu swojego sprzętu do wymagań stawianych przez ASI i niniejszą Politykę. Za sprawdzenie sprzętu pod

kątem dostosowania do wymagań i zapoznanie użytkownika z wymogami PBI odpowiedzialny jest ASI. Decyzję o przyznaniu dostępu zdalnego, podejmuje IOD;

h. Do użytku, dopuszcza się wyłącznie sprzęt i oprogramowanie klienta VPN, które uzyskały pozytywną opinię InfoSec Institute;
i. Sprzęt i oprogramowanie sieciowe, niespełniające wymagań, o których mowa w pkt. 8.h, w celu zastosowania go do dostępu zdalnego, musi uzyskać akceptację ASI;
j. Po upływie 30 minut nieaktywności użytkownika, kanał VPN musi być rozłączany, a użytkownik w celu powtórnego dołączenia się do sieci musi ponowić procedurę uwierzytelniania. Wykorzystanie jakiejkolwiek metody sztucznego potrzymania trwania sesji jest zabronione;
k. Czas trwania nieprzerwanej sesji z wykorzystaniem kanału VPN powinien być ograniczony do 8 godzin.

IV. Odpowiedzialność

1. W obszarze przestrzegania Regulaminu wykorzystania dostępu zdalnego, ustala się następujące zakresy odpowiedzialności:
    a. IOD jest odpowiedzialny za monitorowanie przestrzegania niniejszego Regulaminu. Jest on odpowiedzialny również za działalność edukacyjną, mającą na celu podniesienie poziomu świadomości i zrozumienia odpowiedzialności, wynikającej z niniejszego Regulaminu;
    b. ASI jest odpowiedzialny za organizację, konfigurację, użytkowanie i konserwację programowo-sprzętowego systemu obsługującego DZ, w tym za podsystemy zapewniające ochronę przed złośliwym oprogramowaniem oraz realizację kanału VPN;
    c. ASI jest odpowiedzialny za pomoc pracownikom w obsłudze DZ i pełni rolę punktu zbierania informacji o incydentach związanych z wykorzystaniem dostępu zdalnego;
    d. ASI systematycznie raportuje IOD funkcjonowanie dostępu zdalnego, w szczególności powiadamia go o zaistniałych incydentach;
    e. Wszyscy pracownicy, dla których niniejszy Regulamin jest przedmiotowy, ponoszą odpowiedzialność za jego przestrzeganie. Niniejszy dokument odnosi się także do pracowników innych podmiotów działających w obrębie jednostki organizacyjnej, niezależnie od tego, czy są one związane z PBI Przedsiębiorstwa jawnie, za pomocą punktów umowy, czy też niejawnie, za pomocą ogólnie przyjętych norm postępowania.
2. IOD ma prawo, w dowolnym czasie, ocenić spełnienie wymagań niniejszego Regulaminu przez każdego z użytkowników korzystających z DZ.

3. Niestosowanie się pracownika Przedsiębiorstwa do postanowień niniejszego regulaminu, będzie traktowane jako naruszenie dyscypliny pracy, z wszelkimi tego konsekwencjami. Odpowiedzialność pracowników firm zewnętrznych za naruszenie niniejszego Regulaminu wynika ze stosownych umów i porozumień.
4. Za wnoszenie zmian i uzupełnień do niniejszego Regulaminu odpowiada IOD. Po uzgodnieniu wnoszonych zmian z kierownikami zainteresowanych jednostek organizacyjnych oraz ASI, Regulamin jest zatwierdzany przez osobę sprawującą nadzór właścicielski nad jednostką organizacyjną. Wszystkie zmiany i uzupełnienia niniejszego Regulaminu wchodzą w życie w momencie ich zatwierdzenia.

Załącznik 1

Wniosek o przyznanie dostępu zdalnego – WZÓR

Nazwisko i imię pracownika:	
Jednostka organizacyjna:	
Stanowisko:	
Miejsce pracy:	
Numer telefonu:	
Nazwisko i imię przełożonego:	
Nazwisko i imię IOD:	
Data:	

Lp.	**Nazwa zasobu, lokalizacja, tryb dostępu**
1.	
2.	
3.	
4.	

Lp.	**Cele przyznania zasobów**
1.	
2.	

---------- ----------

(*Data i podpis pracownika*) (*Data i podpis przełożonego*)

Oświadczam, że zostałem zapoznany z PBI SIP i zobowiązuję się do jej przestrzegania.

(*Data i podpis pracownika*)

---------- ----------

(*Decyzja IOD z uzasadnieniem*) (*Data i podpis IOD*)■

Podobne problemy jak w przypadku dostępu zdalnego pojawiają się przy eksploatacji urządzeń mobilnych, w szczególności smartfonów, tabletów i laptopów. Dlatego, większość z podmiotów ogranicza ich zastosowanie za pomocą odpowiednich regulaminów. Regulamin taki pokazano w przykładzie 7. Pojęciem urządzenia mobilnego określamy komputery przenośne typu laptop i tablet oraz smartfony.

Przykład 7. Regulamin wykorzystania urządzeń mobilnych

I. Terminy, definicje, wykorzystane skróty

I.1. Terminy i definicje

1. *Administrator Systemów Informacyjnych* to specjalista odpowiadających za uruchomienie, bieżącą eksploatację oprogramowania i jej zakończenie.
2. *Urządzenie mobilne* to przenośna jednostka komputerowa, pozwalająca przyjmować, gromadzić, przetwarzać, odwzorowywać i wysyłać informację.
3. *Nośnik informacji* to dowolny obiekt materialny, wykorzystywany przechowywania i przenoszenia informacji elektronicznej.
4. *Karta ewidencyjna* komputera to dokument zawierający pełny wykaz sprzętu i oprogramowania stacji roboczej.
5. *Oprogramowanie złośliwe* to oryginalny lub zmodyfikowany program, naruszający poufność, spójność i dostępność informacji.
6. *Użytkownik* to pracownik jednostki organizacyjnej, wykorzystujący zasoby informacyjne do realizacji zadań wynikających z zakresu swoich obowiązków.

I.2. Wykorzystane skróty

ASI – Administrator Systemów Informacyjnych
IOD – Administrator Bezpieczeństwa Informacji
DZ – Dostęp zdalny
SIP – System Informacyjny Przedsiębiorstwa

II. Postanowienia ogólne

1. Niniejszy Regulamin określa standardy udostępniania urządzeń mobilnych i nośników informacji oraz ich wykorzystania poza siedzibą Przedsiębiorstwa.
2. Celem wprowadzenia Regulaminu jest minimalizacja ryzyka strat, które mogą powstać w wyniku wykorzystania urządzeń mobilnych i nośników informacji. Straty mogą dotyczyć utraty informacji niejawnych lub ważnych dla jednostki organizacyjnej, własności intelektualnej, szkody na reputacji, uszkodzenia krytycznych systemów wewnętrznych jednostki organizacyjnej i in.
3. Niniejszy Regulamin jest częścią PBI SIP i obowiązuje we wszystkich jednostkach organizacyjnych korzystających z zasobów SIP.

4. Podstawowymi zasadami bezpiecznego wykorzystania urządzeń mobilnych i nośników informacji:
    a. Użytkownicy korzystający z urządzeń mobilnych i nośników informacji są zobowiązani do bezwzględnego unikania wszelkich działań naruszających bezpieczeństwo informacji;
    b. Urządzenia mobilne i nośniki informacji, należy wykorzystywać wyłącznie w ramach obowiązków służbowych;
    c. Użytkownik korzystający z urządzeń mobilnych i nośników informacji, ponosi pełną odpowiedzialność za swoje działania.

III. Zasady wykorzystania urządzeń mobilnych i nośników informacji

1. Pod wykorzystaniem urządzeń mobilnych i nośników informacji w SIP rozumie się ich podłączenie do infrastruktury systemu, w celu przetwarzania, przyjmowania lub przekazywania informacji pomiędzy SIP, a urządzeniem mobilnymi lub nośnikiem informacji.
2. W SIP dozwolone jest wyłącznie korzystanie z urządzeń mobilnych i nośników informacji będących własnością jednostki organizacyjnej, poddawanych regularnej okresowej kontroli bezpieczeństwa.
3. Na urządzeniach mobilnych oddanych do czasowej dyspozycji użytkownika zezwala się wykorzystywać wyłącznie oprogramowanie wpisane do Rejestru oprogramowania dopuszczonego do użytku oraz wpisanego do Karty ewidencyjnej komputera.
4. Na urządzeniach mobilnych oddanych do czasowej dyspozycji użytkownika obowiązują te same wymagania bezpieczeństwa jak na urządzeniach stacjonarnych. Celowość zastosowania dodatkowych środków bezpieczeństwa jest określana przez ABI.
5. Urządzenia mobilne i nośniki informacji są oddawane do dyspozycji użytkowników, na wniosek kierownika jednostki organizacyjnej Przedsiębiorstwa, w następujących przypadkach:
    a. Urządzenie mobilne lub nośnik informacji są niezbędne nowoprzyjętemu użytkownikowi do wykonywania prac wynikających z zakresu jego obowiązków;
    b. Urządzenie mobilne lub nośnik informacji są niezbędne użytkownikowi do wykonania prac wynikających z eksploatacji SIP.
6. Procedura przekazania użytkownikowi urządzeń mobilnych lub nośników informacji przebiega w następujących krokach:
    a. Przygotowanie wniosku w formie przedstawionej w Załączniku 1, zatwierdzonego przez bezpośredniego przełożonego pracownika wnioskującego o dostęp mobilny;
    b. Zatwierdzenie wniosku, o którym mowa w pkt. 6.a przez IOD;

   c. Przekazanie oryginału wniosku do ASI celem wpisania przekazywanego urządzenia mobilnego lub nośnika informacji działu na Listę użytkowników uprawnionych do korzystania z urządzeń mobilnych poza jednostką organizacyjną, nazywaną dalej Listą, a także weryfikacji jego ustawień technicznych i dopuszczenia do wykorzystania w SIP. Lista stanowi treść Załącznika 2 do niniejszego Regulaminu.

7. Na teren jednostki organizacyjnej wnoszone, a poza nią wynoszone mogą być wyłącznie urządzenia mobilne przekazane użytkownikom i zarejestrowane na Liście. Za prowadzenie Listy odpowiada ASI. Wpisy na Listę obywają się wyłącznie na podstawie zatwierdzonych Wniosków. Wzór wniosku stanowi treść Załącznika 3.
8. Wnoszenie na teren jednostki organizacyjnej urządzeń mobilnych przez osoby trzecie, niebędące pracownikami jednostki organizacyjnej odbywa się na podstawie wypełnionego Formularza zgłoszeniowego, zatwierdzonego przez kierownika jednostki organizacyjnej Przedsiębiorstwa oraz IOD.
9. Użytkownik korzystający z urządzenia mobilnego lub nośnika informacji jest zobowiązany:
   a. Przestrzegać wytyczne niniejszego regulaminu;
   b. Wykorzystywać urządzenia mobilne i nośniki informacji wyłącznie do wykonywania swoich obowiązków służbowych;
   c. Informować IOD o wszelkich naruszeniach niniejszego Regulaminu;
   d. Zachować wymaganą ostrożność w wykorzystaniu urządzeń mobilnych i nośników informacji;
   e. Wykorzystując i transportując urządzenia mobilne i nośniki informacji stosować się do wymagań producentów;
   f. Zapewniać fizyczne bezpieczeństwo urządzeń i nośników informacji wszystkimi dostępnymi sposobami;
   g. Niezwłocznie informować IOD o fakcie utraty urządzeń i nośników informacji.
10. Korzystając z przekazanych użytkownikom urządzeń mobilnych i nośników informacji zabrania się:
   a. Wykorzystywać je w celach prywatnych;
   b. Przekazywać innym osobom (z wyjątkiem ASI i IOD);
   c. Pozostawiać urządzenia mobilne i nośniki danych bez nadzoru, jeśli nie podjęto kroków w celu zapewnienia ich bezpieczeństwa fizycznego.
11. Każda inicjowanie przez użytkownika współdziałanie (przetwarzanie, odbieranie lub przekazywanie informacji) pomiędzy SIP, a urządzeniami mobilnymi i nośnikami informacji spoza Listy, będzie jako podlegające karze nieuprawnione wykorzystanie SIP. W powyższych sytuacjach, ASI na wniosek IOD blokuje dostęp urządzeń mobilnych i nośników informacji użytkownika do SIP. Wykorzystanie urządzeń i nośników spoza listy wymaga wcześniejszego uzgodnienia z ASI i IOD.

12. Informacje na temat korzystania przez użytkowników z urządzeń mobilnych i nośników informacji są rejestrowane i mogą być przekazywane kierownikowi jednostki organizacyjnej Przedsiębiorstwa oraz IOD. Sprawozdania takie przygotowuje ASI.
13. W przypadku podejrzenia użytkownika o korzystania z urządzeń mobilnych i nośników informacji niezgodne z niniejszym Regulaminem, powoływana jest komisja, której zadaniem jest określenie zasadności zarzutów. Komisji przewodniczy IOD, w jej skład wchodzą ASI oraz kierownik właściwej jednostki organizacyjnej Przedsiębiorstwa.
14. Jeżeli komisja, o której mowa w pkt. 13 potwierdza zasadność zarzutów, właściwej kierownik jednostki organizacyjnej jest zobowiązany podjąć działania zgodne z wewnętrznymi przepisami Przedsiębiorstwa oraz obowiązującym prawem.
15. Urządzenia mobile oraz nośniki informacji przekazane użytkownikowo podlegają bezwarunkowej kontroli na nieobecność oprogramowania złośliwego.
16. W przypadku ustania stosunku pracy lub przeniesienia użytkownika do innej jednostki organizacyjnej, przekazane urządzenia i nośniki podlegają bezzwłocznemu zwrotowi.

IV. Odpowiedzialność

1. W obszarze przestrzegania Regulaminu wykorzystania zasobów mobilnych, ustala się następujące zakresy odpowiedzialności:
    a. IOD jest odpowiedzialny za monitorowanie przestrzegania niniejszego Regulaminu. Jest on odpowiedzialny również za działalność edukacyjną, mającą na celu podniesienie poziomu świadomości i zrozumienia odpowiedzialności, wynikającej z niniejszego Regulaminu;
    b. ASI jest odpowiedzialny za pomoc pracownikom w obsłudze urządzeń mobilnych i nośników informacji i pełni rolę punktu zbierania informacji o incydentach związanych z ich wykorzystaniem;
    c. ASI systematycznie raportuje IOD wykorzystanie urządzeń i nośników przekazanych użytkownikom, w szczególności powiadamia go o zaistniałych incydentach;
    d. Wszyscy pracownicy, dla których niniejszy Regulamin jest przedmiotowy, ponoszą odpowiedzialność za jego przestrzeganie. Niniejszy dokument odnosi się także do pracowników innych podmiotów działających w obrębie jednostki organizacyjnej, niezależnie od tego, czy są one związane z Polityką bezpieczeństwa jednostki organizacyjnej jawnie, za pomocą punktów umowy, czy też niejawnie, za pomocą ogólnie przyjętych norm postępowania.

2. IOD ma prawo, w dowolnym czasie, ocenić spełnienie wymagań niniejszego Regulaminu przez każdego z użytkowników korzystających z urządzeń mobilnych i nośników informacji.
3. Niestosowanie się pracownika Przedsiębiorstwa do postanowień niniejszego Regulaminu, będzie traktowane jako naruszenie dyscypliny pracy, z wszelkimi tego konsekwencjami. Odpowiedzialność pracowników firm zewnętrznych za naruszenie niniejszego regulaminu, wynika ze stosownych umów i porozumień.
4. Za wnoszenie zmian i uzupełnień do niniejszego Regulaminu odpowiada IOD. Po uzgodnieniu wnoszonych zmian z kierownikami zainteresowanych jednostek organizacyjnych oraz ASI, Regulamin jest zatwierdzany przez Prezesa. Wszystkie zmiany i uzupełnienia niniejszego Regulaminu wchodzą w życie w momencie ich zatwierdzenia.

Załącznik 1

Wniosek o przekazanie urządzenia mobilnego – WZÓR

Nazwisko i imię pracownika:	
Jednostka organizacyjna:	
Stanowisko:	
Miejsce pracy:	
Numer telefonu:	
Nazwisko i imię przełożonego:	
Nazwisko i imię IOD:	
Data:	

Lp.	Opis przekazywanych urządzeń mobilnych
1.	
2.	
3.	
4.	

Lp.	Wykaz zadań, rozwiązywanych przez urządzenie mobilne
1.	
2.	

---------- ----------

(*Data i podpis pracownika*) (*Data i podpis przełożonego*)

Oświadczam, że zostałem zapoznany z PBI i zobowiązuję się do jej przestrzegania.

(*Data i podpis pracownika*)

---------- ----------

(*Decyzja IOD z uzasadnieniem*) (*Data i podpis* IOD)

Wniosek o przekazanie nośnika informacji – WZÓR

Nazwisko i imię pracownika:	
Jednostka organizacyjna:	
Stanowisko:	
Miejsce pracy:	
Numer telefonu:	
Nazwisko i imię przełożonego:	
Nazwisko i imię IOD:	
Data:	

Lp.	**Opis przekazywanych nośników informacji**
1.	
2.	
3.	

Lp.	**Wykaz rozwiązywanych zadań**
1.	
2.	

---------- ----------

(*Data i podpis pracownika*) (*Data i podpis przełożonego*)

Oświadczam, że zostałem zapoznany z PBI i zobowiązuję się do jej przestrzegania.

(*Data i podpis pracownika*)

---------- ----------

(*Decyzja IOD z uzasadnieniem*) (*Data i podpis IOD*)

Załącznik 2

Lista użytkowników uprawnionych do korzystania z urządzeń mobilnych poza jednostką organizacyjną – WZÓR

L.p.	Nazwisko i imię	Stanowisko	Jednostka organizacyjna	Dokładna nazwa urządzenia	Numer inwentarzowy
1.					
2.					
3.					
4.					
5.					
6.					

Załącznik 3

Wniosek o wyniesienie urządzenia mobilne poza jednostkę organizacyjną – WZÓR

Nazwisko i imię pracownika:	
Jednostka organizacyjna:	
Stanowisko:	
Miejsce pracy:	
Numer telefonu:	
Nazwisko i imię przełożonego:	
Nazwisko i imię IOD:	
Data:	

Lp.	Opis wynoszonego urządzenia mobilnego
1.	
2.	

Lp.	Cel wynoszenia urządzenia mobilnego
1.	
2.	

---------- ----------

(*Data i podpis pracownika*) (*Data i podpis przełożonego*)

Oświadczam, że zostałem zapoznany z PBI SIP i zobowiązuję się do jej przestrzegania.

(*Data i podpis pracownika*)

---------- ----------

(*Decyzja IOD z uzasadnieniem*) (*Data i podpis IOD*)■

Rozdział 5

Bezpieczeństwo zasobów ludzkich

5.1. Wymagania dokumentów normatywnych

Celem zalecanych działań jest zapewnienie zrozumienia przez pracowników i kontrahentów podmiotu swojej odpowiedzialność w obszarze bezpieczeństwa informacji, a także weryfikacja, czy będą oni odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani. Podejmowane działania dotyczą okresu przed zatrudnieniem, w jego trakcie, a także po jego zakończeniu.

Przed zatrudnieniem, zaleca się weryfikację historii zatrudnienia wszystkich kandydatów do pracy, zgodną z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonego ryzyka. Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji. Wszelkie działania podejmowane w danym obszarze powinny być ściśle zdefiniowane.

W trakcie zatrudnienia, przewiduje się nałożenie na kierownictwo obowiązku wymagania od wszystkich pracowników i kontrahentów stosowania zasad bezpieczeństwa informacji, zgodnie z obowiązującymi w organizacji politykami, regulaminami i procedurami. Wszyscy pracownicy organizacji oraz w stosownych wypadkach kontrahenci, powinni przejść stosowne szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur bezpieczeństwa związanych z ich stanowiskiem pracy. Powinny być określone zasady postępowania dyscyplinarnego wobec pracowników naruszających zasady bezpieczeństwa informacji. Zasady te powinny być przedstawione pracownikom.

Po *zakończeniu lub zmianie zatrudnienia* zalecane jest określenie i przedstawienie pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwowanie ich. Po zakończeniu zatrudnienia administrator blokuje dostęp na podstawie informacji z Działu kadr.

Niestety polskie prawodawstwo jest bardzo rygorystyczne pod względem troski o prawa pracownicze. Stosowanie zasad przewidzianych przez normę ISO27001 najprawdopodobniej byłoby naruszeniem prawa. W wielu przypadkach (np. organy samorządowe) zatrudnianie pracowników reguluje stosowne ustawodawstwo szczegółowe.

5.2. Wzory dokumentów

W przykładzie 8 pokazano wzory stosownych polityk i regulaminów.

Przykład 8 Polityki i regulaminy zarządzania zasobami ludzkimi

I. Terminy, definicje, wykorzystane skróty

I.1. Terminy i definicje

1. Terminem *Pracobiorca* określać się będzie osobę zatrudnioną w Przedsiębiorstwie na podstawie umowy o pracę, umowy cywilno-prawnej lub przedstawiciela Kontrahenta, z którym zawarto stosowną umowę na świadczenie usług.
2. Terminem *Pracownik* określać się będzie osobę zatrudnioną w Przedsiębiorstwie na podstawie umowy o pracę lub umowy cywilno-prawnej.
3. Terminem *Podwykonawca* określać się będzie osobę świadczącą pracę na podstawie umowy z podmiotem zewnętrznym.

I.2. Wykorzystane skróty

SIP – System Informatyczny Przedsiębiorstwa
IOD – Inspektor Ochrony Danych
PBI – Polityka Bezpieczeństwa Informacji

II. Postanowienia ogólne

1. Za wszelkie działania związane z rekrutacją, świadczeniem pracy oraz rozwiązaniem umów Pracobiorców odpowiada Dział Kadr Przedsiębiorstwa. Jeżeli działania dotyczą osób mających dostęp do informacji, w podejmowaniu decyzji uczestniczy IOD Przedsiębiorstwa.
2. Przedstawione dalej procedury dotyczą wszystkich Pracobiorców wykorzystujących zasoby informacyjne SIP, stosownie do sposobu zatrudnienia.

III. Działania podejmowane przed zatrudnieniem

III.1. Informacje ogólne

1. Obowiązki wynikające z konieczności zapewniania bezpieczeństwa informacji należy omówić z Pracobiorcą, na podstawie obowiązujących zarządzeń i instrukcji, już na etapie postępowania sprawdzającego, przed podpisaniem właściwej umowy.
2. Postępowaniu sprawdzającemu powinny być poddane wszystkie osoby mające dostęp do zasobów informacyjnych, zatrudniane na podstawie umowy o pracę, umowy cywilno-prawnej, a także będące pracownikami firm zewnętrznych.

3. Osoby zatrudnione na podstawie umowy o pracę, powinny podpisywać umowy zawierające obowiązki pracownika w obszarze bezpieczeństwa informacji. Pozostali Pracobiorcy powinni podpisywać oświadczenie określające role i obowiązki w zakresie bezpieczeństwa informacji.

III.2. Role i obowiązki

1. Formalny opis ról i obowiązków Pracowników w obszarze bezpieczeństwa informacji powinien być zawarty w umowie lub dokumentach opisujących zakres obowiązków na danym stanowisku pracy. W zakresie obowiązków pracownika posiadającego dostęp do informacji należy zawrzeć:
    a. Obowiązek przestrzegania zasad zdefiniowanych w PBI oraz politykach, regulaminach i instrukcjach pochodnych;
    b. Obowiązek ochrony aktywów informacyjnych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
    c. Obowiązek wykonywania konkretnych działań i procesów ochronnych;
    d. Zasady odpowiedzialności osoby za jej działania;
    e. Obowiązek informowania o zdarzeniach związanych lub potencjalnie związanych z naruszeniem bezpieczeństwa.
2. Role i obowiązki w zakresie bezpieczeństwa osób zatrudnianych na innych zasadach niż umowa o pracę, muszą być jasno określone w podpisywanych przez nie stosownych dokumentach.

III.3. Postępowanie sprawdzające

1. Zatrudnienie każdego Pracobiorcy mającego dostęp do zasobów informacyjnych należy poprzedzić postępowaniem sprawdzającym, prowadzonym zgodnie z obowiązującym prawem, instrukcjami wewnętrznymi oraz zasadami etyki. O postępowaniu sprawdzającym oraz jego zakresie należy poinformować każdą osobę starającą się o zatrudnienie.
2. Prowadząc postępowanie sprawdzające, należy zapewnić poufność i ochronę danych osobowych zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* Dz. U. 2014 poz. 1182, a także zgodność wykorzystywanych procedur z *Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy* Dz. U. 2014 poz. 1502.
3. Zakres czynności sprawdzających, należy dostosować do rodzaju informacji, do której dany Pracobiorca będzie miał dostęp:
    a. Dla osób posiadających standardowy dostęp do zasobów informacyjnych, postępowanie sprawdzające powinno obejmować następujące działania:

i. Przedstawienie przez kandydata referencji, w tym przynajmniej jednego świadectwa pracy oraz dwóch referencji osobistych. Przedstawione referencje powinny być zweryfikowane;

ii. Przedstawienie przez kandydata dokumentów potwierdzających deklarowane wykształcenie oraz kwalifikacje zawodowe;

iii. Potwierdzenie przez kandydata swojej tożsamości na podstawie dwóch dokumentów.

b. W postępowaniu sprawdzającym kandydatów na stanowiska posiadające uprzywilejowany dostęp do informacji, w tym IOD oraz ASI zaleca się dodatkowo uwzględnić:

i. Weryfikację autentyczności przedstawionych dokumentów tożsamości;

ii. Przedstawienie przez kandydata uprawnień niezbędnych do pełnienia roli związanej z bezpieczeństwem;

iii. Wyniki kontroli poziomu wiedzy kandydata, dotyczącej bezpieczeństwa informacji;

iv. Kontrolę zadłużenia kandydata oraz jego niekaralności.

4. Procedury sprawdzające powinny być wykonywane również w przypadku zatrudnienia w drodze awansu, o ile zmienia się zakres dostępu pracownika do informacji.
5. Od procedury sprawdzającej można odstąpić w przypadku zatrudnienia w drodze awansu, kiedy nie zmienia się zakres dostępu pracownika do informacji.
6. Za przeprowadzenie procedury sprawdzającej kandydatów na IOD odpowiada Prezes zatrudniający danego pracownika.
7. Za przeprowadzenie procedury sprawdzającej kandydatów na pracowników, mających dostęp do informacji, w tym ASI, odpowiada IOD.
8. Jeżeli Podwykonawca, będzie posiadał dostęp do informacji niejawnych, powinien on również podlegać procedurze sprawdzającej. Wymaganie dotyczące sprawdzenia Podwykonawców powinno być zawarte w stosownej umowie z Kontrahentem, która dodatkowo powinna określać sposób jego powiadomienia o wynikach sprawdzenia i płynących z tego konsekwencji. Zlecane zapisy umowy z Kontrahentem zawarte są w Załączniku 1 do niniejsze Polityki cząstkowej.

III.4. Warunki i zasady zatrudnienia

1. Zdefiniowane w stosownej umowie warunki i zasady zatrudnienia powinny odzwierciedlać PBI, polityki cząstkowe oraz zawierać dodatkowe uszczegółowienia i ustalenia dotyczące:

a. Obowiązku podpisania przez każdą osobę posiadającą dostęp do gromadzonych i przetwarzanych informacji niejawnych, przed uzyskaniem dostępu do nich, umowy zawierającej zapisy o zachowaniu poufności i nieujawnianiu informacji;
b. Praw i obowiązków pracowników, wykonawców i innych użytkowników w odniesieniu do wykorzystywanej przez nich informacji, w szczególności do praw autorskich i ochrony danych osobowych;
c. Obowiązku klasyfikacji informacji i bezpiecznego zarządzania aktywami organizacji, związanymi z systemami informacyjnymi i usługami realizowanymi przez Pracobiorcę;
d. Odpowiedzialności Pracobiorców w zakresie przetwarzania informacji otrzymywanej od podmiotów zewnętrznych;
e. Odpowiedzialności w kwestii przetwarzania danych osobowych pracowników i klientów, a także danych kadrowych i rozliczeń finansowych;
f. Odpowiedzialności dotyczącej pracy wykonywanej poza Przedsiębiorstwem, w przypadku świadczenia pracy w miejscu zamieszkania oraz poza normalnymi godzinami pracy;
g. Działań podejmowanych w sytuacjach zagrożeń, w szczególności w przypadku nieprzestrzegania przez Pracobiorcę wymagań PBI i dokumentów pokrewnych.

2. Zapisy umowy o zachowaniu poufności i nieujawnianiu informacji powinny chronić informacje należące do jednostki organizacyjnej oraz uświadamiać ich sygnatariuszy o odpowiedzialności w zakresie ochrony oraz konieczności wykorzystania i ujawniania informacji w sposób odpowiedzialny i autoryzowany.
3. Dodatkowe wymagania określające zasady udostępniania pracownikom informacji niejawnych, zgodnie z PBI, zawarte są w:
   a. Wytyczne dotyczące wymaganych treści umowy o zachowaniu poufności i nieujawnianiu informacji zgodne z PN-ISO/IEC 27002:2014-12, przedstawiono w Załączniku 2 do niniejszej Polityki;
   b. Zalecane zapisy umowy o pracę, dotyczące zachowania poufności i nieujawniania informacji zawarto w Załączniku 3 do niniejszej Polityki;
   c. Zlecane zapisy umowy o poufności pomiędzy jednostką organizacyjną a Kontrahentem uzyskującym dla swoich pracowników dostęp do poufnych danych zaprezentowano w Załączniku 1 do niniejszej Polityki.

IV. Działania podejmowane w trakcie zatrudnienia

IV.1. Wymagania podstawowe

1. Pracownik może przystąpić do świadczenia pracy dopiero po zapoznaniu go z wykazem jego obowiązków. Zakres obowiązków Pracownika przygotowuje jego bezpośredni przełożony. W obszarze bezpieczeństwa informacji zakres zatwierdza IOD. Zakres powinien wykorzystywać zasadę *rozdzielenia funkcji*, zapewniającą grupowe podejmowanie decyzji kluczowych z punktu widzenia bezpieczeństwa informacji.
2. Prawa dostępu Pracownika do zasobów powinny zezwalać mu na wykonanie wszystkich zadań przewidzianych w zakresie jego obowiązków i należy je przydzielić na podstawie zasady *minimalnej wystarczalności*, tj. Pracownik nie powinien posiadać praw dostępu, zbędnych z punktu widzenia wykazu jego obowiązków.
3. Wykorzystanie przez Pracownika uprzywilejowanych praw dostępu należy śledzić i systematycznie weryfikować. Za ich śledzenie odpowiada IOD Przedsiębiorstwa. Za weryfikację przywilejów IOD odpowiada Prezes.
4. Weryfikację dostępów uprzywilejowanych należy przeprowadzać jeden raz w roku kalendarzowym i powinna być ona potwierdzona stosownym protokołem.
5. Każdy pracownik Przedsiębiorstwa, posiadający dostęp do informacji, powinien zostać zobligowany do zapoznania się z wewnętrznym kodeksem etyki zawodowej, a także do jego przestrzegania.
6. Podwykonawców, a także osoby zatrudnione w oparciu o umowy cywilno-prawne należy zobligować do przestrzegania zasad etyki zawodowej ich Przedsiębiorstwa lub do stosowania kodeksu etyki uznawanego w obrębie informatyki. Podwykonawcy i osoby zatrudnione w oparciu o umowy cywilno-prawne powinny podpisać zobowiązanie do przestrzegania zasad etyki zawodowej.

IV.2. Odpowiedzialność kierownictwa

1. Odpowiedzialność za egzekwowanie od Pracobiorców stosowania zasad bezpieczeństwa, zgodnie z wprowadzoną PBI i dokumentami pokrewnymi, ponoszą:
    a. Na poziomie Przedsiębiorstwa – IOD;
    b. Na poziomie relacji z podmiotami zewnętrznymi – Prezes.
2. Do obowiązków IOD należą:
    a. Wprowadzanie Pracobiorców w obowiązki i zaznajamianie z odpowiedzialnością związaną z bezpieczeństwem informacji, przed przyznaniem im dostępu do systemów informacyjnych zawierających informacje niejawne;
    b. Informowanie Pracobiorców o wymaganiach w zakresie bezpieczeństwa informacji, związanych z ich obowiązkami w jednostkach organizacyjnych;
    c. Motywowanie Pracobiorców do stosowania PBI i dokumentów pokrewnych;
    d. Troska o poziom świadomości bezpieczeństwa informacji Pracobiorców, odpowiedni do ich ról i obowiązków;

e. Weryfikacja spełnienia warunków zatrudnienia Pracobiorcy, uwzględniających PBI oraz bezpieczne metody pracy;
f. Dbałość o odpowiednie umiejętności i kwalifikacje Pracobiorców, w tym organizacja szkoleń;
g. Zapewnienie możliwości anonimowego zgłaszania naruszeń PBI lub przewidzianych przez nią procedur.

3. Nadzór nad działaniami IOD – Prezes.

IV.3. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

IV.3.1. Kodeks etyki zawodowej

1. Do wewnętrznego Kodeksu etyki zawodowej Przedsiębiorstwa, dalej Kodeksu, należy wnieść elementy dotyczące bezpieczeństwa informacji. Najważniejsze elementy Kodeksu powinny stanowić treść umowy o pracę. Zasady zawarte w Kodeksie nie powinny być bardziej rygorystyczne niż przepisy wynikające z obowiązującego ustawodawstwa oraz wewnętrznych regulaminów i instrukcji.
2. Wyciąg z Kodeksu obejmujący zapisy odnoszące się do bezpieczeństwa informacji powinien być wręczany Pracownikowi w momencie podpisywania umowy, a pracownikowi Kontrahenta w chwili rozpoczęcia wykonywania obowiązków przewidzianych umową z Kontrahentem.
3. Treść Kodeksu powinna być podana do ogólnej wiadomości wszystkich osób zatrudnionych w Przedsiębiorstwie.

IV.3.2. Szkolenia pracowników

1. Pracobiorca mający w zakresie swoich obowiązków korzystanie z informacji niejawnej, może uzyskać dostęp do zasobów dopiero po odbyciu szkolenia z zakresu bezpieczeństwa informacji. Zaleca się, aby program szkolenia obejmował m.in.:
   a. Znaczenie bezpieczeństwa informacji dla funkcjonowania SIP;
   b. Zapoznanie z organizacją i podstawowymi wymaganiami PBI w zakresie uwzględniającym obowiązki Pracobiorcy;
   c. Odpowiedzialność za nieprzestrzeganie obowiązujących przepisów.
2. Wszyscy Pracobiorcy mający dostęp do informacji raz w roku powinni przechodzić jednodniowe szkolenie z zakresu bezpieczeństwa informacji. Tematyka szkoleń powinna obejmować m. in.:
   a. Zapoznanie z zasadami bezpieczeństwa informacji oraz obowiązkami określonymi w PBI, normach, przepisach prawnych, regulacjach, umowach i porozumieniach;
   b. Przedstawienie osobistej odpowiedzialności pracowników za swoje działania i zaniechania oraz ogólnych obowiązków w kwestii zabezpieczenia lub ochrony informacji należących do Przedsiębiorstwa i podmiotów zewnętrznych;

   c. Prezentację podstawowych procedur bezpieczeństwa informacji oraz najważniejszych zabezpieczeń;
   d. Poinformowanie o źródłach uzyskania dodatkowej wiedzy w sprawach związanych z bezpieczeństwem informacji, w tym możliwości dalszego kształcenia w tym obszarze;
   e. Zbieranie wniosków Pracobiorców dotyczących poprawy bezpieczeństwa informacji.
3. Szkolenia mogą być realizowane tradycyjnie, w postaci webinariów lub za pomocą interaktywnych aplikacji dydaktycznych.
4. Na zakończenie każdego ze szkoleń zaleca się przeprowadzenie testu weryfikującego wiedzę nabytą przez słuchaczy. Wynik testu może być wykorzystany przy okresowej ocenie Pracownika.
5. Za organizację i przeprowadzenie szkoleń z obszaru bezpieczeństwa informacji odpowiada IOD.

IV.4. Postępowanie dyscyplinarne

1. Po naruszeniu bezpieczeństwa lub podejrzeniu, że naruszenie takie miało miejsce, IOD wykonuje działania mające na celu potwierdzenie naruszenia. Jeżeli naruszenie miało miejsce, IOD wnioskuje o rozpoczęcie postępowania dyscyplinarnego.
2. Za naruszenia bezpieczeństwa Pracobiorca może ponieść odpowiedzialność dyscyplinarną i karną.
3. Określając zakres odpowiedzialności Pracobiorcy należy uwzględnić rodzaj i wagę naruszenia, jego wpływ na funkcjonowanie SIP, czy jest to pierwsze, czy kolejne naruszenie, czy winny został prawidłowo przeszkolony oraz inne stosowne czynniki.
4. Postępowanie dyscyplinarne powinno zapewnić bezstronne i obiektywne traktowanie osób naruszających bezpieczeństwo informacji.
5. W przypadku potwierdzonych, poważnych naruszeń, skutkujących zagrożeniem dla funkcjonowania SIP zaleca się natychmiastowe anulowanie praw dostępu do zasobów osobie odpowiedzialnej za naruszenie.
6. W przypadku potwierdzonych, poważnych naruszeń, skutkujących zagrożeniem zdrowia i życia innych osób, zaleca się natychmiastowe rozwiązanie umowy z Pracobiorcą.
7. W stosunku do osób ujawniających informacje niejawne, realizujących nieautoryzowany dostęp do chronionych zasobów informacyjnych bądź świadomie narażających zdrowie i życie innych osób, należy rozważyć możliwość pociągnięcia ich do odpowiedzialności karnej. Decyzję taką, na wniosek IOD, podejmuje Biuro prawne Przedsiębiorstwa.

V. Działania związane z zakończeniem lub zmianą zatrudnienia

V.1. Odpowiedzialność związana z zakończeniem lub zmianą zatrudnienia

1. Zmiana obowiązków lub stanowiska osób posiadających dostęp do informacji SIP powinny być traktowane jak rozwiązanie umowy wiążącej Pracobiorcę z jednostką organizacyjną.
2. O fakcie rozwiązania lub zmiany umowy z Pracobiorcą powinni być informowani pozostali Pracobiorcy Przedsiębiorstwa. Obowiązek poinformowania spoczywa na Dziale kadr Przedsiębiorstwa.
3. Zapisy określające zobowiązania Pracobiorcy po zakończeniu zatrudnienia powinny stanowić treść podpisywanych umów. Zapisy zalecane w przypadku umów z Pracownikiem stanowią treść Załącznika 3. Zapisy zalecane w przypadku umów z Kontrahentem stanowią treść Załącznika 1.
4. O zobowiązaniach Pracowników po zakończeniu zatrudnienia należy informować kandydatów na etapie rekrutacji, a Podwykonawców w chwili podejmowania obowiązków wynikających ze stosownej umowy.

V.2. Zwrot zasobów przekazanych do wykorzystania

1. Pracobiorca jest zobowiązany do zwrotu wszelkich zasobów, będących własnością Przedsiębiorstwa. W szczególności dotyczy to:
    a. Oprogramowania oraz sprzętu komputerowego i sieciowego;
    b. Urządzeń telekomunikacyjnych;
    c. Kart kredytowych;
    d. Kart dostępowych;
    e. Podręczników i dokumentacji, w tym przechowywanych na nośnikach elektronicznych.
2. Jeżeli Pracobiorca wykorzystuje własny sprzęt lub wykupuje sprzęt wypożyczony mu na czas zatrudnienia, wszelkie zasoby informacyjne znajdujące się na nim muszą zostać przed odsprzedażą przekazane Przedsiębiorstwu, a następnie bezpiecznie usunięte ze sprzętu.
3. Jeżeli Pracobiorca dysponuje wiedzą ważną dla toczących się operacji, zaleca się jej utrwalenie na nośnikach i przekazanie jednostce organizacyjnej.
4. Wszelkie działania związane ze zwrotem zasobów powinny zostać zakończone najpóźniej w ostatnim dniu zatrudnienia Pracobiorcy. Zwrot zasobów związanych z gromadzeniem i przetwarzaniem informacji jest nadzorowany przez IOD.

V.3. Anulowanie praw dostępu do zasobów

1. Anulowanie Pracobiorcy praw dostępu do zasobów, dalej praw dostępu, obejmuje:
    a. Dostęp fizyczny do pomieszczeń, kluczy, kart identyfikacyjnych, środków przetwarzania informacji;
    b. Dostęp logiczny do kont systemów operacyjnych, poczty elektronicznej, list subskrypcji, aplikacji, danych itp.;

c. Dokumenty, w których występuje on jako pracownik Przedsiębiorstwa.

2. Wszelkie działania związane z anulowaniem Pracobiorcy praw dostępu, należy zakończyć najpóźniej w ostatnim dniu jego zatrudnienia lub pracy na poprzednim stanowisku, o ile nie określono inaczej.
3. Za anulowanie lub zmianę praw dostępu Pracobiorcy odpowiada IOD. Stosowne działania podejmowane są na wniosek osoby nadzorującej Pracobiorcę. Za anulowanie lub zmianę praw dostępu IOD opowiada Prezes.
4. Jeżeli zwalniany Pracobiorca dysponował hasłami do kont, które pozostają aktywne, to hasła te powinny zostać bezzwłocznie zmienione.
5. Jeżeli zwalniany Pracobiorca dysponował prawami dostępu przyznawanymi większej liczbie osób na podstawie identyfikatorów grupowych, należy podjąć działania wykluczające go z każdej z grup oraz zmieniające wspólne hasła dostępu.
6. Jeżeli dla Pracobiorcy zmieniony zostanie zakres obowiązków, należy dokonać przeglądu jego praw dostępu.
7. Jeżeli anulowanie lub zmiana praw dostępu dotyczy Podwykonawcy i nie jest konsekwencją wygaśnięcia lub zmiany stosownej umowy, pracownik Przedsiębiorstwa nadzorujący podwykonawcę, informuje o podjętych działaniach IOD, który przesyła Kontrahentowi pisemne zawiadomienie o podjętych działaniach i ich bezpośrednich przyczynach.
8. Jeżeli zdaniem IOD, zwalniany Pracobiorca, może celowo niszczyć informacje, uszkadzać narzędzia przetwarzania lub gromadzić dane celem późniejszego wykorzystania, anulowanie praw dostępu do zasobów powinno nastąpić przed poinformowaniem Pracobiorcy o planowanych ograniczeniach dostępu.

Załącznik 1

Zalecane elementy umowy o poufności, dotyczące zachowania poufności i nieujawniania informacji przez pracowników firm zewnętrznych

Przedsiębiorstwo, będące dysponentem informacji niejawnej, nazywane dalej *Właścicielem* i Przedsiębiorstwo X nazywane dalej *Kontrahentem*, zawarli Umowę następującej treści:

§1. Przedmiot Umowy

1. Właściciel, na życzenie Kontrahenta zobowiązuje się dostarczyć jego pracownikom niewyłączne prawo dostępu do informacji na warunkach określonych przez niniejszą Umowę.

2. Rodzaj uprawnień, wykaz pracowników i udostępnianych zasobów informacyjnych, każdorazowo będzie określany przez IOD Właściciela na podstawie zgłoszenia Kontrahenta, przygotowanego w postaci przedstawionej w Załączniku 1 do niniejszej Umowy.
3. Kontrahent zobowiązuje się nie ujawniać informacji, udostępnionej mu przez Właściciela.

§2. Obowiązki Właściciela

1. Zapewnienie określonych w Umowie, trybów dostępu do informacji niejawnej.
2. Dostarczenie Kontrahentowi niewyłącznego prawa dostępu do informacji niejawnej, zgodnie z wymaganiami określonymi w PBI Właściciela i innymi obowiązującymi Właściciela dokumentami z obszaru bezpieczeństwa informacji.
3. Zapoznanie Kontrahenta, za potwierdzeniem, z wykazem informacji niejawnych, do których zostaje mu zapewniony dostęp.
4. Zapoznanie Kontrahenta, za potwierdzeniem, z koniecznością przestrzegania wymagań PBI Właściciela, w zakresie ochrony poufności, integralności i dostępności informacji niejawnej.
5. Zapoznanie Kontrahenta, za potwierdzeniem, o dyscyplinarnej, cywilno-prawnej lub/i karnej odpowiedzialności w przypadku naruszenia funkcjonalności zasobów programowo-sprzętowych, do których uzyskał on dostęp lub naruszenia poufności, integralności i dostępności przechowywanych na nich informacji.

§3. Prawa Właściciela

1. Właściciel zastrzega sobie prawo przeprowadzenia procedury sprawdzającej pracowników Kontrahenta, mających dostęp do informacji poufnych. Procedura sprawdzająca może objąć następujące działania:
    a. Udokumentowanie przez kandydata swojej tożsamości na podstawie dwóch dokumentów;
    b. Weryfikację autentyczności przedstawionych dokumentów tożsamości;
    c. Kontrolę zadłużenia kandydata oraz jego niekaralności.
2. Blokowanie dostępów do zasobów programowo-sprzętowych w przypadku zmiany, wygaśnięcia lub rozwiązania Umowy.
3. Sprawowanie kontroli i monitorowanie dostępu Kontrahenta do informacji niejawnej.
4. Rejestracja i badanie incydentów zagrażających bezpieczeństwu informacji, w tym również wynikających z działań lub zaniechań Kontrahenta.
5. Przeprowadzenia kontroli realizacji przez Kontrahenta wymagań niniejszej Umowy.

§4. Obowiązki Kontrahenta

1. Nie ujawniać informacji, będącej dla Właściciela informacją niejawną, a przekazanej mu poprzez przewidzianą niniejszą Umową, procedurę uzyskiwania dostępu.
2. Przestrzegać wytycznych PBI Właściciela i innych dokumentów regulujących zasady zapewnienia bezpieczeństwa informacji niejawnej Właściciela.
3. W celu rejestracji i analizy incydentów bezpieczeństwa, Kontrahent jest zobowiązany niezwłocznie poinformować Właściciela o wszelkich znanych mu faktach ujawnienia lub zagrożenia ujawnieniem udostępnianej mu informacji niejawnej lub nielegalnego korzystania z niej przez osoby trzecie.
4. Zachować poufność informacji innych podmiotów, z którym łączą Właściciela relacje biznesowe, a udostępnianych Kontrahentowi w ramach niniejszej Umowy.
5. Nie wykorzystywać informacji niejawnej udostępnianej przez Właściciela w ramach niniejszej Umowy, do prowadzenia jakiejkolwiek działalności konkurencyjnej względem Właściciela;
6. Wynagrodzić Właścicielowi informacji niejawnej szkody, wynikłe z zawinionego przez Kontrahenta ujawnienia udostępnionych informacji niejawnych. Kontrahent nie ponosi odpowiedzialności, jeżeli ujawnienie informacji było skutkiem siły wyższej, skrajnej konieczności, dostępu uzyskanego w wyniku błędu lub niewykonaniem przez Właściciela obowiązków zapewniania trybów dostępu do informacji niejawnej.
7. W przypadku wygaśnięcia, rozwiązania lub zmiany niniejszej Umowy wszystkie informacje niejawne, znajdujące się w posiadaniu Kontrahenta, muszą być zniszczone lub zwrócone Właścicielowi.

§5. Postanowienia dodatkowe

1. Każda ze Stron zobowiązuje się do zachowania poufności informacji i dokumentacji uzyskanych w ramach niniejszej Umowy. Zobowiązanie do zachowania poufności obowiązuje w okresie 3 lat po upływie okresu obowiązywania niniejszej Umowy.

ZAŁĄCZNIK 1

Wykaz użytkowników i poufnych zasobów informacyjnych, do których realizowany jest dostęp

L.p.	Imię i nazwisko	Stanowisko	Nazwa stacji roboczej	Nazwa zasobu	Lokalizacja zasobu	Prawa dostępu
1	2	3	4	5	6	7

Załącznik 2

Zalecane elementy umowy o zachowaniu poufności i nieujawnianiu informacji według PN-ISO/IEC 27001:2014-12

Umowy o zachowaniu poufności i nieujawnianiu informacji mają zastosowanie do podmiotów zewnętrznych i pracowników organizacji. Jakiekolwiek udostępnienie informacji niejawnej powinno być poprzedzone podpisaniem stosownej umowy. Forma i treść umowy powinny być dostosowane do konkretnych okoliczności. W odniesieniu do umów zaleca się:

1. Regularne identyfikowanie, weryfikację i dokumentowanie wymagań odnoszących się do zachowania poufności lub nieujawniania informacji, na poziomie odzwierciedlającym potrzeby jednostki organizacyjnej w zakresie ochrony informacji.
2. Formułowanie umów o zachowaniu poufności i nieujawnianiu informacji w sposób prawnie skuteczny.
3. Dostosowanie treści umowy do typu podmiotu, z którym jest ona zawierana, oferowanego trybu dostępu oraz zasad utrzymania poufności informacji.
4. Określenie w umowie:
    a. Wykazu informacji, które mają być chronione;
    b. Czasu trwania umowy, łącznie z przypadkami, w których obowiązek zachowania poufności może być bezterminowy;
    c. Działań wymaganych w momencie zakończenia umowy;
    d. Zakresu działań i odpowiedzialności sygnatariuszy podejmowanych w celu uniknięcia nieupoważnionego ujawnienia informacji;
    e. Prawa własności informacji, tajemnic przemysłowych oraz własności intelektualnej w odniesieniu do ochrony informacji niejawnych;
    f. Sposobów dozwolonego użycia informacji niejawnych oraz prawa sygnatariusza do ich wykorzystania;
    g. Zasad audytu i monitorowania działań związanych z informacjami niejawnymi;
    h. Zasad powiadamiania i raportowania w przypadku nieuprawnionego ujawnienia lub wypłynięcie informacji niejawnych;
    i. Zasad zwrotu lub niszczenia informacji po wygaśnięciu umowy;
    j. Działań podejmowanych w przypadku naruszenia warunków umowy;
    k. Innych elementów wynikających z potrzeby zapewnienia bezpieczeństwa informacji w jednostce organizacyjnej.
5. Okresowe przeglądanie umów o zachowaniu poufności i nieujawnianiu informacji nie rzadziej niż raz w roku oraz zawsze wtedy, gdy pojawią się zmiany wpływające na te wymagania.

6. Odpowiedzialność za przygotowanie, podpisanie, przestrzeganie oraz okresową weryfikację ponosi IOD.

Załącznik 3

Zalecane elementy umowy o pracę, dotyczące zachowania poufności i nieujawniania informacji

§1. Przedmiot Umowy

1. Pracownik w czasie świadczenia pracy będzie miał dostęp do informacji niejawnych, będących własnością Pracodawcy na poziomie odpowiadającym jego stanowisku pracy i zakresowi obowiązków, a także zapewniającym możliwość wykorzystania sprzętu Pracodawcy.

§2. Prawa i obowiązki stron

1. Pracownik ma obowiązek:
    a. Niezwłocznie poinformować bezpośredniego przełożonego o wystąpieniu sytuacji stanowiącej zagrożenie dla niejawnych informacji Pracodawcy;
    b. W okresie obowiązywania niniejszej Umowy oraz po jej zakończeniu w przeciągu kolejnych 3 (trzech) lat, za wyjątkiem przypadków przewidzianych prawem Rzeczypospolitej Polskiej:
        i. Nie ujawniać danych i informacji stanowiących tajemnicę handlową i innych niejawnych informacji Pracodawcy, które zostały mu powierzone lub zostały poznane w czasie świadczenia usługi pracy;
        ii. Nie przekazywać osobom trzecim i nie ujawniać publicznie informacji stanowiących tajemnice handlowe i innych informacji niejawnych Pracodawcy bez jego pisemnej zgody;
        iii. Zakazuje się bez zgody przełożonego gromadzić i przechowywać informacje stanowiące tajemnicę handlową i/lub inne chronione prawem Rzeczypospolitej Polskiej informacje organizacji i osób znajdujących się w relacjach biznesowych z Pracodawcą;
        iv. Wykonywać wszystkie dotyczące pracownika wymagania zawarte w rozporządzeniach, regulaminach, instrukcjach oraz przepisach dotyczących ochrony tajemnic handlowych i innych informacji niejawnych Pracodawcy;
        v. W przypadku podjęcia przez osoby niepowołane próby uzyskania od Pracownika informacji niejawnych będących własnością Pracodawcy, natychmiast poinformować o tym swojego bezpośredniego przełożonego, a w przypadku jego nieobecności – IOD;

vi. Nie wykorzystywać tajemnic handlowych i innych informacji niejawnych Pracodawcy do dowolnej innej działalności, która jako działalność konkurencyjna może wyrządzić szkodę Pracodawcy;

vii. Bezzwłocznie poinformować swojego bezpośredniego przełożonego, a w przypadku jego nieobecności – IOD o utracie lub braku identyfikatorów, przepustek, kluczy, osobistych pieczęci i o innych faktach, które mogą doprowadzić do ujawnienia tajemnic handlowych i innych informacji niejawnych Pracodawcy, a także o przyczynach i warunkach ewentualnego wycieku informacji, stanowiących tajemnicę handlową lub innych niejawnych informacji Pracodawcy;

viii. Do naprawienia Pracodawcy szkód wynikających z ujawnienia danych i informacji stanowiących tajemnicę handlową lub innych informacji niejawnych Pracodawcy.

c. W przypadku wygaśnięcia lub rozwiązania umowy o pracę, przed dokonaniem ostatecznego rozliczenia, przekazać Pracodawcy wszystkie będące w jego dyspozycji nośniki, zawierające informacje niejawne i inne mienie Pracodawcy, w tym oprogramowanie;

d. Nie występować w jakikolwiek sposób w imieniu Pracodawcy, o ile jawnie nie przewidują tego jego stosowne dyspozycje;

e. Powiadomić pisemnie Pracodawcę o bezpośrednim lub pośrednim udziale w jakimkolwiek przedsięwzięciu komercyjnym, niezwiązanym z Pracodawcą;

f. Nie używać materialnych, informacyjnych i innych zasobów Pracodawcy do uzyskiwania własnych korzyści lub korzyści osób trzecich, bez pisemnej zgody Pracodawcy;

g. Przekazywać Pracodawcy informacje o wszystkich wynalazkach, odkryciach, ulepszeniach, technologiach i know-how, opracowanych lub uzyskanych samodzielnie lub w zespole na potrzeby Pracodawcy, a także otrzymanych przy użyciu sprzętu Pracodawcy lub informacji będących jego własnością;

h. Niezwłocznie informować Pracodawcę o wystąpienia konfliktu interesów w przypadku, kiedy Pracownik lub członek jego rodziny będzie finansowo zaangażowany w firmie, będącej dostawcą lub odbiorcą usług Pracodawcy;

i. Niezwłocznie informować Pracodawcę o faktach otrzymania nagród i prezentów o wartości ponad 1000 (jeden tysiąc) zł rocznie, od klientów i partnerów Pracodawcy;

j. Nie dopuszczać do jakiejkolwiek reklamy własnej firmy i innych firm z wykorzystaniem zasobów Pracodawcy;

k. Niezwłocznie informować Pracodawcę o podejrzanych kontaktach z przedstawicielami konkurencji, grup przestępczych i ugrupowań totalitarnych. Za podejrzane uważane są kontakty nawiązane przez Pracownika, zarówno w okresie poprzedzającym zatrudnienie, jak i po podpisaniu umowy o pracę,

charakteryzujące się zainteresowaniem drugiej strony działalnością Pracodawcy i jego pracowników.

2. Pracodawca ma prawo:
    a. Przekazywać podmiotom, które oficjalnie zwróciły się o referencje Pracownika, informacje o jego nieuczciwych lub nieetycznych działaniach (jeżeli dotyczy);
    b. Prowadzić audyt przetwarzania i przechowywania zasobów informacyjnych oraz danych przesyłanych i przetwarzanych przez Pracownika za pomocą technicznych środków przesyłania i przetwarzania informacji Pracodawcy;
    c. Wykorzystywać wyniki audytu przetwarzania i przechowywania zasobów informacyjnych oraz danych przekazywanych i przetwarzanych w systemie Pracodawcy, w celu optymalizacji procesów biznesowych i rozwiązywania sytuacji konfliktowych.
3. Pracodawca jest zobowiązany:
    a. Zapewnić dostęp Pracownika do poufnych informacji Pracodawcy, w zakresie niezbędnym do wykonywania przez niego zadań, wynikających z ustalonego zakresu obowiązków, na zasadach ustalonych przez Pracodawcę;
    b. Przestrzegania autorskich praw majątkowych na narzędzia, programy i bazy danych wytworzone w ramach zatrudnienia Pracownika, zgodnie z *Ustawą z dnia 4 lutego 1994 o prawie autorskim i prawach pokrewnych* Dz. U. 1994 nr 24 poz. 83. oraz *Ustawą z dnia 23 kwietnia 1964 Kodeks cywilny* Dz. U. 1964 nr 16 poz. 93.

§3. Postanowienia dodatkowe

1. Wyłączne prawo wykorzystania narzędzi, programów i baz danych utworzonych w trakcie zatrudnienia Pracownika lub przekazanych przez Pracodawcę w celu realizacji określonego zadania, należy do Pracodawcy.
2. Jeżeli po zakończeniu umowy o pracę, jakiekolwiek efekty zatrudnienia Pracownika lub uzyskane z wykorzystaniem zasobów Pracodawcy będą zgłoszone przez Pracownika do ochrony patentowej lub ujawnione przez niego osobie trzeciej, to dane produkty oraz wszystkie prawa do korzystania z nich będą należeć do Pracodawcy, o ile nie zostanie udowodnione, że były one stworzone już po ustaniu stosunku pracy, bez korzystania z informacji i innych zasobów Pracodawcy.
3. Wszystkie środki transmisji i przetwarzania informacji Pracodawcy, a także przetwarzane na nich i przekazywane za ich pomocą informacje, należą do Pracodawcy. Pracownikowi nie wolno używać środków przesyłania i przetwarzania informacji Pracodawcy do przetwarzania i przesyłania prywatnych danych.
4. Pracownik został zapoznany z wykazem informacji sklasyfikowanej jako niejawna.

Rozdział 6

Zarządzanie aktywami

6.1. Wymagania dokumentów normatywnych

Celem działań podejmowanych w danym obszarze jest identyfikacja aktywów, definicja odpowiedzialności w obszarze ich ochrony, a także przypisanie i zapewnienie informacjom odpowiedniego poziomu ochrony.

W obszarze *odpowiedzialności za aktywa*, przewiduje się obowiązkową identyfikację aktywów związanych z informacjami i środkami przetwarzania oraz sporządzenie i utrzymywanie ewidencji tych aktywów. Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom. Ponadto, należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz związanych z nią aktywów i środków przetwarzania informacji. Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia powinni zwrócić wszystkie posiadane aktywa organizacji.

W obszarze *klasyfikacji informacji*, przewiduje się podział informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Zaleca się opracowanie i wdrożenie zbioru procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem jej klasyfikacji. Ponadto, należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji.

W zakresie *postępowania z nośnikami*, zaleca się wdrożenie procedur zarządzania nośnikami wymiennymi, zgodne ze schematem klasyfikacji przyjętym w organizacji. Nośniki, które nie będą dłużej wykorzystywane, powinny zostać bezpiecznie wycofane, zgodnie z formalnymi procedurami. Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.

6.2. Przykłady dokumentów

Przykład 9. Polityka archiwizacji informacji

I. Terminy, definicje, wykorzystane skróty

I.1. Terminy i definicje

1. *Administratorzy systemu*, to uprzywilejowani pracownicy działu zarządzania systemem informacyjnym, zapewniający poprawne funkcjonowanie, usuwanie niesprawności oraz rozwój systemu informacyjnego.

2. *Archiwizacja*, to długoterminowe przechowywanie informacji zawartych w systemie lub danych o jego stanie. Zbiory archiwalne tworzone są za pomocą operacji kopiowania na dodatkowe nośniki informacji.
3. *Zasób*, to folder, plik z danymi, oprogramowanie lub serwis zlokalizowany na serwerze bądź stacji roboczej.
4. *Odpowiedzialny za zasoby informacyjne*, to pracownik kierownictwa jednostki organizacyjnej, podejmujący decyzje o tworzeniu nowych Zasobów.
5. *Główny węzeł przetwarzania*, to węzeł w którym zlokalizowane zostały najważniejsze zasoby sprzętowo-programowe, w oparciu o które wykonywane jest bieżące zarządzanie system informacyjnym.
6. *System tworzenia kopii zapasowych*, to zestaw środków programowo-sprzętowych, odpowiedzialnych za tworzenie kopii zapasowych i odzyskiwanie z nich danych.
7. *Tworzenie kopii zapasowych*, to zapis kolejnego aktualnego stanu informacji z systemu, bez obowiązku zachowania stanu poprzedniego.
8. *Etykieta prywatności*, to identyfikator zbioru nadawany w procesie klasyfikacji poziomu prywatności zbiorów.
9. *Klasyfikacja poziomu prywatności zbiorów*, to działanie wykonywane przez ABI dla każdego nowopowstającego zbioru, określające stopień niezależności zbioru od użytkowników i innych źródeł danych.
10. *Polityka bezpieczeństwa archiwizacji informacji* nazywana dalej Polityką, to zbiór reguł zarządzania tworzeniem, przechowywaniem i wykorzystaniem kopii zapasowych.

I.2. Wykorzystane skróty

AAI – Administrator Archiwizacji Informacji
IOD – Inspektor Ochrony Danych
ASI – Administrator Systemów Informacyjnych
STKZ – System Tworzenia Kopii Zapasowych
SIP – System Informacyjny Przedsiębiorstwa

II. Postanowienia ogólne

1. Podstawowym celem niniejszej Polityki jest zapobieganie utracie danych gromadzonych i przetwarzanych w SIP, w przypadku wystąpienia awarii jego sprzętu, oprogramowania, w sytuacjach kryzysowych itp.
2. Zakłada się, że najczęstszymi przyczynami utraty danych w SIP, będą:
    a. Awarie sprzętu tworzącego system informacyjny;
    b. Usterki systemu operacyjnego i aplikacji;
    c. Pojawienie się w systemie informacyjnym złośliwego oprogramowania;
    d. Nieumyślne niszczenie informacji, będące wynikiem błędów użytkowników;
    e. Celowe niszczenie informacji przez użytkowników lub osoby z zewnątrz.

3. Dodatkowym celem niniejszej Polityki jest uporządkowanie informacji i procedur jej wykorzystania. W szczególności, porządkowaniu podlegają:
    a. Miejsca przechowywania informacji;
    b. Poprawny sposób wykorzystania przez użytkowników danych i oprogramowania;
    c. Sposoby oceny ilościowych i jakościowych charakterystyk gromadzonej i przetwarzanej informacji.
4. Niniejsza Polityka zakłada, że cykl życia informacji zapasowej jest niezmienny i włącza następujące etapy:
    a. Tworzenie informacji;
    b. Kopiowanie informacji na nośnik zapasowy;
    c. Przechowywanie informacji na kopii zapasowej:
        i. Bieżące (wymagane również do tworzenia kopii zapasowych);
        ii. Długoterminowe (wymagane do późniejszego wykorzystania).
    d. Wykorzystanie informacji z kopii zapasowych.
5. Zgodnie z niniejszą Polityką, tworzenie kopii zapasowych usuwa przypisanie informacji do konkretnego miejsca przetwarzania. Staję się ona mobilną i nie jest związana z jedną jednostką przetwarzająca lub pomieszczeniem. Realizując wytyczne niniejszej Polityki należy zagwarantować, aby w przypadku wystąpienia sytuacji kryzysowych, prowadzących do przerwania funkcjonowania podstawowego systemu informacyjnego, można ją w krótkim czasie przenieść na rezerwową jednostkę przetwarzania.
6. Zgodnie z niniejszą Polityką, miejscami przetwarzania i okresowego magazynowania informacji elektronicznej są:
    a. Serwery przetwarzające;
    b. Stacje robocze użytkowników;
    c. Urządzenia sieciowe.
7. Niniejsza Polityka obejmuje następujące rodzaje przetwarzanych i gromadzonych informacji:
    a. System operacyjny i jego programy narzędziowe;
    b. Oprogramowanie aplikacyjne;
    c. Dane gromadzone i przetwarzane w systemie;
    d. Dzienniki serwerów, stacji roboczych i urządzeń sieciowych;
    e. Konfiguracje urządzeń sieciowych.
8. W niniejszej Polityce, uwzględniono następujące metody tworzenie kopii zapasowych:
    a. Klonowanie, tj. tworzenie kilku fizycznych kopii woluminów;
    b. Tworzenie kopii natychmiastowej w postaci logicznej kopii dysku lub jego fragmentów;

   c. Kopiowanie:
      i. Kopiowanie pełne, tj. tworzenie pełnej kopii zasobów;
      ii. Kopiowanie inkrementalne, tj. tworzenie wyłącznie kopii danych, które zostały zmodyfikowane od ostatniego kopiowania pełnego, inkrementalnego lub różnicowego;
      iii. Kopiowanie różnicowe, tj. tworzenie kopii danych zmodyfikowanych od czasu przeprowadzenia ostatniego pełnego kopiowania.
9. Zgodnie z niniejszą Polityką, kopie zapasowe będą tworzone dla następujących kategorii informacji:
   a. Dane prywatne użytkowników, zawarte w ich katalogach domowych na serwerach i stacjach roboczych;
   b. Zbiorcze informacje użytkowników, zawarte we współdzielonych katalogach serwerów i stacji roboczych;
   c. Informacje niezbędne do odtworzenia pracy serwerów, urządzeń sieciowych oraz systemów zarządzania bazami danych;
   d. Osobiste profile kont użytkowników systemu;
   e. Informacje z systemów gromadzenia i przetwarzania, w tym z baz danych;
   f. Kopie zainstalowanych składników oprogramowania stacji roboczych;
   g. Informacje z rejestrów systemu ewidencjonowania pracy i bezpieczeństwa informacji.
10. Zaleca się, aby każdemu nośnikowi informacji, zawierającemu kopię zapasową, przypisać etykietę prywatności, odpowiadającą najwyższej spośród etykiet zbiorów zawartych na nośniku.

III. System tworzenia kopii zapasowych

1. STKZ ma na celu zapewnienie wysokiej dostępności informacji wykorzystywanych przez SIP i jest przeznaczony do tworzenia kopii zapasowych i odzyskiwania danych.
2. System tworzenia kopii zapasowych, eksploatowany w SIP powinien mieć scentralizowaną, wielowarstwową architekturę obejmującą:
   a. Serwer zarządzania kopiami zapasowymi, nazywany dalej serwerem zarządzania. Dopuszcza się jego dodatkowe wykorzystanie jako serwera kopii danych;
   b. Grupę serwerów kopii danych, nazywanych dalej serwerami kopii, obsługujących nośniki informacji;
   c. Komputery-klienci, z zainstalowanymi aplikacjami agentów, nazywanych dalej agentami, odpowiadającymi za tworzenia kopii zapasowych. Komputerem-klientem nazywany jest zarówno serwer, jak i stacja robocza użytkownika;
   d. Konsolę administratora STKZ, nazywaną dalej konsolą.
3. Zgodnie z harmonogramem lub na życzenie AAI, serwer zarządzania wydaje polecenie agentowi zainstalowanemu na komputerze-kliencie rozpoczęcia tworzenia

kopii zapasowej, zgodnie z przyjętym harmonogramem. Agent gromadzi i przesyła dane przeznaczone do archiwizacji na wskazany serwer kopii, który zapisuje dane na obsługiwanym przez niego nośniku informacji. Informacje o przebiegu procesu archiwizacji są zapisywane w bazie danych serwera zarządzania.

4. STKZ jest podsystemem narzędziowym SIP i musi posiadać następujące cechy:
   a. Proces tworzenia kopii zapasowej nie jest niezbędny do wykonania podstawowych zadań SIP, jego awaria nie może prowadzić do ograniczenia dostępności podstawowych serwisów SIP;
   b. Obciążenie serwerów SIP, wnoszone przez proces tworzenia kopii zapasowej, nie może być istotne z punktu widzenia świadczenia podstawowych usług SIP.
5. Utworzone kopie zapasowe zaleca się sprawdzać pod kątem spójności i sprawności odtworzenia.

IV. Strategie tworzenia kopii zapasowych

IV.1. Kopiowanie interakcyjne i nadmiarowe

1. Niezawodność i dostępność krytycznych komponentów informacyjnych SIP należy zagwarantować jednoczesnym wykorzystaniem kopiowania interaktywnego (ang. *online backup*) i nadmiarowego (ang. *standby backup*). Komponenty danych serwerów SIP oraz pliki podstawowego kontrolera domeny należy archiwizować z wykorzystaniem obu metod archiwizacji, pozostałe, w tym rezerwowy kontroler domeny, z wykorzystaniem kopiowania nadmiarowego.
2. Zaleca się, aby kopiowanie interaktywne informacyjnych komponentów SIP było realizowane za pomocą narzędzi systemów zarządzania bazą danych, a plików podstawowego kontrolera domeny za pomocą narzędzi systemu operacyjnego.
3. Wskazane jest, aby kopiowanie nadmiarowe serwerów i stacji roboczych SIP było wykonywane za pomocą narzędzi STKZ.
4. Zaleca się, aby kopiowanie interaktywne było wykonywane jednocześnie na dwa serwery kopii, przy czym jeden z nich powinien znajdować się poza siedzibą głównego węzła przetwarzania SIP.
5. Kopiowanie nadmiarowe należy wykonywać bezpośrednio na podstawowy serwer kopii. Następnie, obraz z podstawowego serwera kopii, powinien być zapisany na rezerwowym serwerze kopii, zlokalizowanym poza główny węzłem przetwarzania.
6. Zaleca się, aby przechowywanie informacji w serwerach kopii odbywało się w oparciu o technologię RAID. Jako wystarczającą, uważa się zastosowanie technologii dysków lustrzanych.

IV.2. Serwer zarządzania kopiami zapasowymi

1. Serwer zarządzania kopiami zapasowymi jest dedykowaną jednostką komputerową przeznaczoną do organizacji i nadzoru nad procesem tworzenia kopii zapasowych. Powinien być on zlokalizowany w głównym węźle przetwarzającym SIP, dodatkowo może on wypełniać funkcję serwera kopii.
2. Jeżeli w dodatkowych lokalizacjach jednostki organizacyjnej, zlokalizowana jest znaczna liczba jednostek, których zasoby wymagają archiwizacji, należy zlokalizować w nich dodatkowe serwery zarządzania kopiami zapasowymi lub połączyć je z węzłem głównym za pomocą dedykowanej linii transmisyjnej.

IV.3. Serwery rezerwowe

1. STKZ obsługujący SIP powinien być wyposażony w nie mniej niż jeden rezerwowy serwer zarządzający, zlokalizowany poza główny węzłem SIP.
2. W przypadku awarii głównego serwera zarządzania kopiami zapasowymi, jego rolę przejmuje serwer zapasowy, a kopiowanie nadal odbywa się w trybie interakcyjnym. Jeżeli kopiowanie w trybie interakcyjnym nie jest możliwe, następuje przejście do kopiowania nadmiarowego.
3. W procesie opracowywania nowego oprogramowania wykorzystywane mogą być wyłącznie rezerwowe serwery zarządzające.

V. Ilościowe i jakościowe charakterystyki kopii

1. Ilościowe charakterystyki tworzenia kopii zapasowych określają załączniki 4 oraz 5 do niniejszej Polityki.
2. W procesie tworzenia kopii, AAI powinien:
    a. Wykonywać procedury tworzenia kopii nadmiarowych w czasowym oknie tworzenie kopii, dopuszczającym zatrzymanie serwisów informacyjnych, uwzględniając przy tym wymóg całodobowej pracy SIP;
    b. Jeżeli do kopiowania nie wykorzystuje się dedykowanych kanałów komunikacyjnych, to powinno się minimalizować objętość danych przesyłanych po sieci LAN. Jeżeli ich ilość jest znaczna i może zakłócać funkcjonowanie SIP, zastosowanie kanałów dedykowanych jest obowiązkowe.
3. Procedury kopiowania danych powinny uwzględniać wymagania krytyczności utraty informacji. W szczególności zaleca się:
    a. Wykonanie procedur kopiowania nadmiarowego powinno odbywać się w okresie minimalnej aktywności SIP, tj. w nocy.
    b. Wskazanym jest przechowywanie czterech kopii zapasowych informacji krytycznych dla funkcjonowania SIP: po jednej kopii nadmiarowej na głównym serwerze kopii i serwerze rezerwowym oraz na dwóch serwerach kopiowania interaktywnego;

c. Dla informacji kluczowych dla funkcjonowania SIP dopuszcza się dodatkowe przechowywanie poza serwerami kopii, na specjalnie do tego celu wyznaczonych stacjach roboczych;
d. Zaleca się, aby STKZ uwzględniał tworzenie i długoterminowe przechowywanie kopii rocznych. W pierwszym roku kopie te powinny być przechowywane w trzech egzemplarzach: pierwsza – na serwerach kopii w głównym węźle, druga – na serwerze kopii, poza siedzibą głównego węzła, trzecia wykorzystująca nośnik wymienny – poza siedzibą głównego węzła.

4. Proces tworzenia kopii zapasowej należy zorganizować tak, aby operacje przenoszenia i archiwizacji plików lokalnych prowadzone były w ciągu dnia, a operacje kopiowania zawartości serwerów, a także wymiana kopii pomiędzy stacjami roboczymi a serwerem kopii – w godzinach wieczornych, nocnych lub w dni minimalnego obciążenia SIP.

VI. Organizacja tworzenia kopii zapasowych

1. Kierownik jednostki organizacyjnej wyznacza osobę, odpowiedzialną za tworzenie i przechowywanie kopii zapasowych, wypełniającą funkcję AAI. AAI podlega IOD, a wykonywanie przez niego zadań związanych z archiwizacją danych jest dodatkowo nadzorowane przez ASI.
2. AAI w swoich działaniach opiera się na niniejszej Polityce oraz innych aktach prawnych, normatywnych i wewnętrznych.
3. Do podstawowych zadań i obowiązków AAI należy:
   a. Planowanie procedur tworzenia kopii zapasowych i odzyskiwania danych;
   b. Ustalenie cyklu życia i kalendarza operacji archiwizacji;
   c. Systematyczny przegląd logów procesu tworzenia kopii zapasowych;
   d. Ochrona bazy danych tworzenia kopii zapasowych;
   e. Definicja czasowych okien tworzenia kopii zapasowych;
   f. Tworzenie i obsługa raportów dotyczących zaistniałych problemów z tworzeniem kopii zapasowych;
   g. Konsultacje z dostawcami sprzętu i oprogramowania przeznaczonego do tworzenia kopii zapasowych;
   h. Rozwój systemu tworzenia kopii zapasowych.
4. Do codziennych zadań AAI należą:
   a. Monitorowanie realizacji zadań tworzenia kopii zapasowych;
   b. Kontrola raportów o awariach i poprawnie wykonanych zadaniach tworzenia kopii zapasowych;
   c. Analiza pojawiających się problemów i ich bezzwłoczne rozwiązywanie;
   d. Zarządzanie kopiami zapasowymi i ich biblioteką;
   e. Śledzenie przestrzegania harmonogramów realizacji zadań archiwizacji.

5. Do cotygodniowych, comiesięcznych i nieokresowych zadań AAI należą:
    a. Analiza wydajności zadań archiwizacji;
    b. Nadzorowanie i prognozowanie zmian objętości archiwów, troska o nieprzekraczanie dopuszczalnego poziomu zapełnienia nośników magazynujących;
    c. Analiza efektywności metod tworzenia kopii zapasowych;
    d. Weryfikacja możliwości odzyskiwania danych z kopii zapasowych;
    e. Weryfikacja stanu technicznego nośników informacji;
    f. Planowanie rozwoju systemu archiwizacji, określenie i weryfikacja skuteczności dziennych, tygodniowych, miesięcznych i rocznych zadań tworzenia kopii zapasowych.
6. Permanentnymi obowiązkami AAI są:
    a. Zapewnienie i utrzymanie sprawności narzędzi STKZ;
    b. Natychmiastowe informowanie IOD oraz ASI o wykrytych błędach i awariach podczas tworzenia kopii zapasowych, a także podejmowanie odpowiednich działań zmierzających do ich usunięcia;
    c. Wspólnie ze specjalistami służb informatycznych Przedsiębiorstwa, podejmowanie działań w celu przywrócenia sprawności STKZ.
7. AAI ma prawo:
    a. Wymagać od wszystkich użytkowników SIP bezwarunkowego przestrzegania ustalonej instrukcji tworzenia kopii zapasowych i odzyskiwania danych;
    b. Wymagać zaprzestania przetwarzania informacji w przypadkach naruszenia ustalonej technologii tworzenia kopii zapasowych lub zakłócania funkcjonowania STKZ;
    c. Zwracać się do dowolnej jednostki organizacyjnej Przedsiębiorstwa z prośbą o pomoc techniczną i metodologiczną w zakresie tworzenia kopii zapasowych lub odzyskiwania danych;
    d. Przygotowywać propozycje poprawy funkcjonowania STKZ.
8. AAI jest osobiście odpowiedzialny za wszelkie prace w zakresie tworzenia kopii zapasowych i odzyskiwania informacji, zgodnie z obowiązkami określonymi w niniejszej Polityce.

VII. Zasady tworzenia kopii zapasowych

1. Tworzenie kopii zapasowych SIP odbywa się na podstawie następujących założeń i dokumentów:
    a. Wykazu archiwizowanych danych i ich objętości, przedstawionego w Załączniku 4 oraz częstotliwości ich tworzenia, pokazanego w Załączniku 5;
    b. Maksymalny okres przechowywania nadmiarowych krótkoterminowych kopii zapasowych, o których mowa w pkt. 1.c.i-1.c.iii wynosi 1 rok. Coroczne

nadmiarowe kopie długoterminowe, o których mowa w pkt. 1.c.iv przechowywane są przez okres 10 lat.

c. Dla serwerów przechowuje się 4 różne kopie nadmiarowe:
   i. Kopię wykonaną w nocy, w piątek (pełna kopia);
   ii. Kopię wykonaną w nocy, od poniedziałku do czwartku (kopia inkrementalna);
   iii. Kopię wykonaną w nocy, w piątek pierwszego tygodnia nowego miesiąca (pełna kopia);
   iv. Kopię wykonaną w nocy, w piątek, w pierwszym tygodniu pierwszego miesiąca nowego roku (pełna kopia).
d. Dla stacji roboczych przechowywana jest jedna kopia;
   i. Dla stacji roboczych typu A, kopia wykonana w ciągu piątku (pełna kopia);
   ii. Dla stacji roboczych typu B, kopia wykonana w ciągu dnia 15-go każdego miesiąca (kopia pełna).
e. Lokalizacja przechowywania kopii:
   i. Na terenie głównej siedziby jednostki organizacyjnej;
   ii. Na terenie innej siedziby jednostki organizacyjnej.

2. System programowo-sprzętowy, wykorzystywany do tworzenia kopii zapasowych, musi dysponować wydajnością umożliwiającą tworzenie i przechowywanie kopii zdefiniowanych w Planie tworzenia kopii zapasowych (Załącznik 4) w określonym czasie i zadaną częstotliwością, zgodnie z Harmonogramem tworzenia kopii zapasowych (Załącznik 5).
3. W czasie, kiedy SIP funkcjonuje w trybie awaryjnym, pełna kopia powinna być wykonywana codziennie. Do tego celu można wykorzystać wszystkie serwery kopii, dysponujące niezbędną ilością miejsca do przechowywania kopiowanych zasobów.
4. O wszelkich wykrytych próbach nieautoryzowanego dostępu do skopiowanej informacji, a także innych naruszeń bezpieczeństwa, do których doszło w trakcie tworzenia kopii zapasowych, AAI niezwłocznie informuje IOD.

VIII. Kontrola wyników tworzenia kopii zapasowych

1. Każdy użytkownik stacji roboczej, który wykryje wszelkie nieprawidłowości w procedurach tworzenia kopii zapasowych, ma obowiązek poinformowania o tym AAI lub IOD.
2. Kontrolę wyników wszystkich procedur tworzenia kopii zapasowych wykonuje AAI, przed godziną 14.00 dnia roboczego, następującego bezpośrednio po dniu, w którym wykonywane było kopiowanie.
3. W przypadku wykrycia błędu, AAI bezzwłocznie informuje IOD o zaistniałym zdarzeniu.

4. AAI jest zobowiązany do okresowej weryfikacji poprawności procedury odzyskiwania informacji z plików kopii. W zależności od wykorzystywanej metody kopiowania, sprawdzanie poprawności kopii zapasowej włącza regenerację poszczególnych folderów i plików i/lub całej kopii. Sprawdzanie kopii zapasowych przeprowadza się nie rzadziej niż raz na dwa miesiące.
5. W przypadku wykrycia problemów z odtworzeniem zawartości kopii zapasowych, AAI ma obowiązek niezwłocznej modyfikacji procedur kopiowania, usuwającej wykryte problemy z odtworzeniem informacji lub wymiany nośnika informacji.

IX. Rotacja nośników kopii zapasowej

1. STKZ musi zapewniać możliwość okresowej wymiany nośników danych bez utraty informacji zawartych na nich.
2. STKZ musi zagwarantować przywracanie informacji w przypadku awarii któregokolwiek z nośników lub urządzeń wykorzystywanych do tworzenia kopii zapasowych.
3. Wszystkie procedury związane z przenoszeniem zawartości informacyjnej pomiędzy nośnikami wykonywane są przez AAI.
4. Jako nowych nośników można użyć ponownie tych, u których okres przechowywania zawartych na nich informacji wygasł. Przed ich ponownym wykorzystaniem, konieczne jest usunięcie z nich informacji niejawnych, za pomocą metody zgodnej ze standardem DOD 5220.22, a także diagnostyka ich sprawności technicznej.
5. Niejawne informacje zapisane na nośnikach, które zostały wycofane z użytku muszą być usunięte za pomocą metody zgodnej ze standardem DOD 5220.22.

Załącznik 4

Plan tworzenia nadmiarowych kopii zapasowych

L.p.	Zasób	Lokalizacja zasobu	Rodzaj archiwizacji	Lokalizacja kopii
1.				
2.				
3.				

Załącznik 5

Harmonogram tworzenia nadmiarowych kopii zapasowych

SERWERY

Kopiowanie codzienne

L.p.	Zasób	Poniedziałek	Wtorek	Środa	Czwartek	Piątek
1.	Serwer plików	23.00 - Kopia inkrementalna 1	23.00 - Kopia inkrementalna 2	23.00 - Kopia inkrementalna 3	23.00 - Kopia inkrementalna 4	23.00 - Kopia pełna
2.						
3.						

Kopiowanie comiesięczne

L.p.	Zasób	Piątek pierwszego tygodnia miesiąca
1.	Serwer plików	23.00 - Pełna kopia ostatniego tygodnia minionego miesiąca
2.		
3.		

Kopiowanie coroczne

L.p.	Zasób	Piątek pierwszego tygodnia pierwszego miesiąca nowego roku
4.	Serwer plików	23.00 - Pełna kopia ostatniego tygodnia minionego miesiąca
5.		
6.		

SERWERY

Kopiowanie cotygodniowe – kategoria A

L.p.	Zasób	Piątek
1.	Stacja robocza 1	13.00 – Kopia pełna
2.		
3.		

Kopiowanie cotygodniowe – kategoria B

L.p.	Zasób	15-ty dzień nowego miesiąca
1.	Stacja robocza 1	13.00 – Kopia pełna
2.		
3.		

Załącznik 6

Regulamin Administratora archiwizacji informacji

I. Postanowienia ogólne

1. Niniejszy regulamin określa obowiązki Administratora Archiwizacji Informacji, dalej AAI, określa odpowiedzialność kierowników i pracowników Przedsiębiorstwa, wykorzystujących System Tworzenia Kopii Zapasowych, dalej STKZ i odpowiedzialnych za wykonywanie kopii.
2. STKZ ma scentralizowaną, wielopoziomową architekturę włączającą:
   a. Serwer zarządzania kopiami zapasowymi, nazywany dalej serwerem zarządzania. Dopuszcza się jego dodatkowe wykorzystanie jako serwera kopii danych;
   b. Grupę serwerów kopii danych, nazywanych dalej serwerami kopii, obsługujących nośniki informacji;
   c. Komputery-klientów, z zainstalowanymi aplikacjami agentów, nazywanych dalej agentami, odpowiadającymi za tworzenia kopii zapasowych. Komputerem-klientem nazywany jest zarówno serwer, jak i stacja robocza użytkownika;
   d. Konsolę administratora STKZ, nazywaną dalej konsolą.

II. Sposób tworzenia kopii zapasowych

1. Tworzenie kopii zapasowych SIP odbywa się na podstawie następujących założeń i dokumentów:
   a. Wykazu archiwizowanych danych i ich objętości, przedstawionego w Załączniku 4 oraz częstotliwości ich tworzenia, pokazanego w Załączniku 5;
   b. Maksymalny okres przechowywania nadmiarowych krótkoterminowych kopii zapasowych, o których mowa w pkt. 1.c.i-1.c.iii wynosi 1 rok. Coroczne nadmiarowe kopie długoterminowe, o których mowa w pkt. 1.c.iv przechowywane są przez okres 10 lat;
   c. Dla serwerów przechowuje się 4 różne kopie nadmiarowe:
      i. Kopię, wykonaną w nocy w piątek (pełna kopia);
      ii. Kopię, wykonaną w nocy, od poniedziałku do czwartku (kopia inkrementalna);
      iii. Kopię, wykonaną w nocy w piątek pierwszego tygodnia nowego miesiąca (pełna kopia);
      iv. Kopię, wykonaną w nocy w piątek, w pierwszym tygodniu pierwszego miesiąca nowego roku (pełna kopia).
   d. Dla stacji roboczych przechowywana jest jedna kopia;
      i. Dla stacji roboczych typu A, kopia wykonana w ciągu piątku (pełna kopia);

ii. Dla stacji roboczych typu B, kopia wykonana w ciągu dnia 15-go każdego miesiąca (kopia pełna).

e. Lokalizacja przechowywania kopii:

f. Na terenie głównej siedziby jednostki organizacyjnej;

g. Na terenie innej siedziby jednostki organizacyjnej.

2. Schemat tworzenia kopii zapasowych dla serwerów ma poniższą postać:

L.p.	Dzień	Operacja
1.	Poniedziałek	Kopiowanie inkrementalne
2.	Wtorek	Kopiowanie inkrementalne
3.	Środa	Kopiowanie inkrementalne
4.	Czwartek	Kopiowanie inkrementalne
5.	Piątek	Pełne kopiowanie
6.	Piątek pierwszego tygodnia miesiąca	Sprawdzenie potrzeby comiesięcznego kopiowania
7.		Przeniesienie kopii do folderu miesiąca
8.	Piątek pierwszego tygodnia pierwszego miesiąca roku	Sprawdzenie potrzeby kopiowania rocznego
9.		Przeniesienie kopii do folderu roku
10.		Pełne kopiowanie

3. Schemat tworzenia kopii zapasowych dla stacji roboczych ma poniższą postać.

L.p.	Dzień	Operacja
	Stacje robocze typu A	
1.	Piątek	Pełne kopiowanie
	Stacje robocze typu B	
2.	15-ty dzień każdego miesiąca	Pełne kopiowanie

III. Zadania Administratora archiwizacji informacji

1. Do obowiązków AAI należy:
   a. Planowanie procedur tworzenia kopii zapasowych i odzyskiwania danych;
   b. Ustalenie cyklu życia i kalendarza operacji kopiowania;
   c. Analiza logów procesu tworzenia kopii zapasowych;
   d. Ochrona bazy danych tworzenia kopii zapasowych;
   e. Określanie okna czasowego tworzenia kopii zapasowych;

f. Tworzenie i obsługa raportów dotyczących pojawiających się problemów z kopiowaniem informacji;
g. Konsultacje z dostawcami sprzętu i oprogramowania przeznaczonego do tworzenia kopii zapasowych;
h. Modernizacja STKZ.

2. Do codziennych zadań AAI należą:
   a. Monitorowanie wykonania zadań archiwizacji;
   b. Analiza raportów o niepoprawnym wykonaniu operacji archiwizacji;
   c. Analiza i rozwiązywanie problemów pojawiających się przy tworzeniu kopii zapasowych;
   d. Zarządzanie biblioteką kopii zapasowych;
   e. Przygotowanie i analiza harmonogramów realizacji zadań.
3. Do cotygodniowych, comiesięcznych i innych zadań AAI należą:
   a. Analiza wydajności STKZ;
   b. Określanie tendencji zmian objętościowych i ilościowych kopii zapasowych;
   c. Analiza technik tworzenia kopii zapasowych, wprowadzanie niezbędnych zmian;
   d. Weryfikacja możliwości odzyskiwania informacji z kopii;
   e. Planowanie rozwoju STKZ, określenie dziennych, tygodniowych, miesięcznych i rocznych zadań kopiowania.

IV. Obowiązki Administratora Archiwizacji Informacji

AAI ma obowiązek:

1. Zapewnienie i utrzymanie sprawności funkcjonowania STKZ;
2. Natychmiastowe informowanie swojego przełożonego i ABI o zidentyfikowanych błędach i awariach podczas tworzenia kopii zapasowej, a także podjęcie odpowiednich działań zmierzających do ich usunięcia;
3. Wspólnie ze specjalistami służb informatycznych jednostki organizacyjnej, podejmowanie działań w celu przywrócenia sprawności narzędzi STKZ.

V. Prawa Administratora Archiwizacji Informacji

AAI ma prawo:

1. Wymagać od użytkowników SIP bezwarunkowego przestrzegania ustalonej instrukcji tworzenia kopii zapasowych i odzyskiwania danych;
2. Zgłaszać propozycje i wymagać zaprzestania przetwarzania informacji w przypadkach naruszenia ustalonej technologii tworzenia kopii zapasowych danych lub zakłócenia funkcjonowania STKZ;

3. Zwracania się do dowolnej jednostki organizacyjnej z prośbą o pomoc techniczną i metodologiczną w zakresie tworzenia kopii zapasowych i odzyskiwania danych;
4. Przygotowywać propozycje poprawy funkcjonowania STKZ.

VI. Odpowiedzialność

AAI jest osobiście odpowiedzialny za:

1. Wszelkie działania w zakresie utrzymania zdolności do pracy STKZ;
2. Usuwanie awarii STKZ, w tym również za przygotowanie zaplecza diagnostyczno-naprawczego;
3. Planowanie rozwoju istniejącej architektury STKZ i jej dalszej modernizacji w celu optymalizacji funkcjonowania;
4. Permanentne monitorowanie wyników wszystkich procedur tworzenia kopii zapasowych;
5. Okresowe sprawdzanie możliwości odzyskiwania plików z kopii zapasowych;
6. Jakość prac w zakresie tworzenia kopii zapasowych i odzyskiwania danych. ■

Rozdział 7

Ochrona danych osobowych

7.1. Wymagania aktów normatywnych

Ochrona danych osobowych jest chyba najszerzej opisanym w prawie elementem bezpieczeństwa informacji. Wynika to z rygorystycznych zapisów zawartych w obowiązującym prawodawstwie. W monografii ograniczymy się do przytoczenia przekładu polityki ochrony danych osobowych. Wymagania rozporządzenia RODO zostały przedstawione w literaturze [6], [7], [10], [12].

7.2. Przykłady dokumentów

Poniżej przedstawiono przykłady dokumentów regulujących zarządzanie danymi osobowymi.

Przykład 10. Polityka ochrony danych osobowych

I. Terminy, definicje, wykorzystane skróty

I.1. Terminy i definicje

W niniejszej Polityce wykorzystywane będą następujące terminy i określenia:

1. Terminem *Administrator danych* określamy osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2. Terminem *Dane Osobowe* (DO) określa się wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego podejścia do tożsamości tej osoby fizycznej;
3. Termin *RODO* oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
4. *Przetwarzanie danych osobowych* to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie

lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;

5. Terminem *Administrator DO* definiuje się instytucję publiczną, samorządową, podmiot gospodarczy wykonujący operacje przetwarzania danych osobowych;
6. *Ograniczenie przetwarzania* to działanie polegające na określonej identyfikacji przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
7. Terminem *Pracownik* określać się będzie osobę zatrudnioną w podmiocie będącym właścicielem niniejszej Polityki na podstawie umowy o pracę lub umowy cywilno-prawnej;
8. *Depersonalizacja* (*Anonimizacja*) to zmiana postaci zapisu danych osobowych, w wyniku której tracą one charakter danych osobowych;
9. Terminem *Podwykonawca* określać się będzie osobę świadczącą pracę na podstawie umowy z podmiotem zewnętrznym;
10. *Podmiot danych* to każda osoba fizyczna, która jest przedmiotem przetwarzanych danych;
11. *Zgoda podmiotu danych osobowych* to dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda, aby ją udowodnić musi być udokumentowana we właściwy sposób;
12. *Ocena skutków w ochronie danych* to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych. Ma ona miejsce przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych, jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;
13. *Odbiorca danych osobowych* oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
14. *Podmiot przetwarzający* to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora;
15. *Inspektor Ochrony Danych* to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi, Podmiotowi przetwarzającemu lub pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania, a także działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego;

16. *Administrator Bezpieczeństwa Informacji* to osoba wyznaczona przez Administratora, której zadaniem jest zarządzanie bezpieczeństwem informacji w systemie informacyjnym Administratora;
17. Termin *Pseudonimizacja* oznacza przetwarzanie danych osobowych w taki sposób, że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
18. *Szczególne kategorie danych* osobowych ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych i biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej. Do tej grupy można zaliczyć także dane dotyczące zdrowia, naturalnego życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego, postępowaniach administracyjnych i karnych oraz o sankcjach;
19. *Naruszenie ochrony danych osobowych* jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
20. *Profilowanie* jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

I.2. Wykorzystane skróty

SIODO	–	System Informatyczny Ochrony Danych Osobowych
IOD	–	Inspektor Ochrony Danych
PBI	–	Polityka Bezpieczeństwa Informacji

II. Postanowienia ogólne

1. Niniejszy regulamin został opracowany zgodnie z ustawodawstwem Rzeczypospolitej Polskiej (RP) o ochronie danych osobowych (dalej w tekście – DO) i dokumentami wykonawczymi organów władzy wykonawczej dotyczącymi bezpieczeństwa DO podczas ich przetwarzania w systemach informatycznych ochrony DO (dalej SIODO).

2. Zapisy niniejszego dokumentu obowiązują we wszystkich procesach pozyskiwania, systematyzacji gromadzenia, przechowywania, modyfikacji, rozpowszechniania (w tym przesyłania), depersonalizacji, profilowania, blokowania oraz niszczenia wykonywanych z zastosowaniem środków automatyzacji lub bez nich.
3. Niniejsza Polityka wchodzi w życie z chwilą jej zatwierdzenia przez Prezesa i obowiązuje przez czas nieokreślony, aż do zastąpienia jej nową Polityką.
4. Wszystkie zmiany w Polityce dokonywane są za pisemnie za pomocą Zarządzenia Prezesa.
5. Z zawartością niniejszej Polityki muszą zostać zapoznani wszyscy pracownicy Administratora mający dostęp do DO. Fakt zapoznania się z Polityką i zrozumienia zawartych w niej uregulowań potwierdzają swoim podpisem.

III. Cele i zadania przetwarzania DO

1. Przetwarzanie DO powinno ograniczać się do osiągnięcia konkretnych z góry określonych i zgodnych z prawem celów. Nie dopuszcza się przetwarzania DO niezgodnie z celami ich gromadzenia.
2. Nie jest dozwolone łączenie baz danych zawierających DO, których cele przetwarzania są odmienne.
3. Przetwarzaniu podlegają wyłącznie dane osobowe, które spełniają cele ich przetwarzania.
4. Treść i zakres przetwarzanych DO musi odpowiadać założonym celom przetwarzania. Przetwarzane DO nie powinny być nadmiarowe względem założonych celów ich obróbki.

IV. Dane osobowe przetwarzanie w SIODO

1. W SIODO przetwarzane są dane osobowe następujących podmiotów:
   a. Pracowników Administratora DO;
   b. [*Wpisać dane dotyczące danego podmiotu*].

V. Dostęp do zbiorów DO

1. Pracownicy Administratora, którzy z racji wykonywanych obowiązków stale korzystają z DO, otrzymują dostęp do odpowiednich kategorii DO, na okres wykonywania przez nich wskazanych obowiązków, na podstawie wykazu osób dopuszczonych do pracy z DO, który zatwierdza Prezesa. Wykaz sporządzany jest na podstawie zakresu obowiązków pracownika oraz Polityki bezpieczeństwa informacyjnego.
2. Administrator DO wykorzystuje do ochrony DO środki programowo-techniczne przetwarzania i ochrony DO. Jednocześnie prowadzony jest dziennik ewidencji środków ochrony.
3. Administrator DO prowadzi ewidencję zmiennych nośników informacji.

4. Środki programowo-techniczne SIODO znajdują się w obiektach Administratora.
5. Wszystkie osoby dopuszczone do pracy z DO, a także związane z eksploatacją SIODO powinny pisemnie potwierdzić zapoznanie się z niniejszą Polityką.

VI. Podstawowe wymagania dotyczące ochrony DO

1. W trakcie przetwarzania DO w SIODO należy zapewnić:
   a. Prowadzenie działań mających na celu zapobieganie nieautoryzowanym dostępom do danych osobowych i/lub przekazywania ich osobom, które nie mają praw do takich informacji;
   b. Możliwie najwcześniejsze wykrywanie nieautoryzowanego dostępu do zbiorów DO;
   c. Unikania narażania środków technicznych SIODO, czego skutkiem mogłoby być naruszenie ich poprawnego funkcjonowania;
   d. Możliwość natychmiastowego odzyskiwania DO, zmodyfikowanych lub zniszczonych w wyniku nieuprawnionego dostępu do nich;
   e. Prowadzenie stałej kontroli gwarantowanego poziomu ochrony DO.
2. Administrator zobowiązany jest do podjęcia niezbędnych prawnych, organizacyjnych, technicznych i innych środków w celu zapewnienia bezpieczeństwa DO.

VII. Rejestry prowadzone przez Administratora

1. Inspektor danych osobowych, a jeżeli stanowisko takie nie istnieje to Administrator bezpieczeństwa informacji, przygotowuje:
   a. Wykaz zbiorów danych osobowych, zgodnie ze wzorem stanowiącym treść Załącznika do niniejszej Polityki;
   b. Ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie ze wzorem stanowiącym treść załącznika do niniejszej Polityki;
   c. Upoważnienia potwierdzające prawo wskazanego pracownika do przetwarzania danych osobowych w systemach informacyjnych i zbiorach papierowych. Wzór upoważnienia stanowi treść załącznika;
   d. Dokumenty anulujące upoważnienia, o których mowa w pkt. 1.c zgodnie ze wzorem opisanym w Załączniku;
   e. Upoważnienie do przebywania w obszarze przetwarzania danych osobowych, zgodnie ze wzorem pokazanym w Załączniku;
   f. Jeżeli przetwarzanie zlecane jest innym podmiotom – Umowę powierzenia danych zgodnie ze wzorem zawartym w Załączniku oraz Rejestr umów powierzenia na podstawie wzoru zawartego w Załączniku;
2. Osoby o których mowa w pkt. 1 odpowiedzialne są okresową weryfikację aktualności ww. wykazów. Aktualizacja taka powinna mieć miejsce bezpośrednio po pojawieniu się nowych czynności, aktywów lub incydentów, jednak nie rzadziej niż

raz w kwartale. Przeprowadzenie procedury aktualizacji należy potwierdzić stosowną notatką.

3. Inspektor danych osobowych (IOD), a jeżeli stanowisko takie nie istnieje to Administrator bezpieczeństwa informacji (ABI) odpowiada za umieszczenie klauzul zgody lub klauzul informacyjnych mówiących o przetwarzaniu danych osobowych, a także prawach podmiotu danych. Wzory klauzul stanowią treść stosownego Załącznika.

VIII. Zgoda na przetwarzanie danych osobowych

1. Podmiot DO podejmuje decyzję o przyznaniu prawa przetwarzania swoich danych i wyraża zgodę na ich przetwarzanie bez przymusu, zgodnie ze swoją wolą i w swoim interesie. Zgoda na przetwarzanie DO musi być podjęta świadomie. Zgodę na przetwarzanie DO może być udzielona przez podmiot DO lub jego przedstawiciela, w każdej formie pozwalającej potwierdzić fakt jego otrzymania, o ile nie określono inaczej przez prawo. W przypadku uzyskania zgody na przetwarzanie DO od przedstawiciela podmiotu DO uprawnienia przedstawiciela są sprawdzane przez Administratora.
2. Zezwolenie na przetwarzanie DO Podmiotu jest wprowadzane do SIODO przez pracownika Administratora, po otrzymaniu od Podmiotu DO w pisemnej formie danych osobowych i zgody na ich przetwarzanie w postaci określonej przez Administratora SIODO.

IX. Prawa Podmiotu DO do informacji przetwarzanych przez Administratora

1. Podmiot danych osobowych ma prawo do:
   a. Otrzymywania od Administratora informacji, dotyczących przetwarzania jego DO. Informacje te muszą być przekazane podmiotowi DO w przystępnej formie i nie powinny zawierać DO innych podmiotów za wyjątkiem przypadków, gdy istnieją uzasadnione podstawy do ujawnienia takich danych. Zakres informacji i sposób uzyskania informacji przewidziany jest zgodnie z obowiązującymi przepisami prawa;
   b. Żądania od Administratora możliwości uszczegółowienia jego DO, ich blokowania lub zniszczenia w przypadku, gdy dane są niekompletne, nieaktualne, niedokładne, nielegalnie uzyskane lub nie są niezbędne do wyznaczonego celu przetwarzania, a także podejmować przewidziane prawem środki w celu ochrony swoich praw;
   c. Obowiązku uzyskania przez Administratora pisemnej zgody na przetwarzanie DO w celu promowania towarów, prac lub usług poprzez realizację bezpośrednich kontaktów z potencjalnym konsumentem za pomocą środków łączności, a także w celu agitacji politycznej;

d. Obowiązku uzyskania przez Administratora pisemnej zgody Podmiotu DO na podejmowanie decyzji opartej wyłącznie o automatyczne przetwarzanie DO podmiotu, generujących skutki prawne w stosunku do podmiotu DO lub w inny sposób, wpływających na jego prawa i uzasadnione interesy;
e. Zgłaszania zastrzeżeń do decyzji Administratora, podejmowanych wyłącznie na podstawie automatycznego przetwarzania DO Podmiotu i ewentualne skutki prawne takiej decyzji;
f. Skargi do organu odpowiedzialnego za ochronę praw Podmiotu DO lub sądu na działania lub zaniechania Administratora DO.

X. Prawa i obowiązki administratora SIODO

1. Administrator SIODO ma prawo:
   a. Zlecić przetwarzanie DO innej osobie za zgodą podmiotu DO, jeśli obowiązujące przepisy nie stanowią inaczej, na podstawie zawartej z tą osobą umowy, w tym umowy państwowej lub komunalnej lub przyjęcie takiej umowy;
   b. W przypadku odmowy przez podmiot DO ich przetwarzania DO, kontynuować przetwarzanie DO bez zgody podmiotu, jeżeli zezwala na to prawodawstwo Rzeczpospolitej Polskiej;
   c. Odmówić podmiotowi DO ponownego dostępu do informacji, niespełniającego warunków przewidzianych przez ustawodawstwo. Taka odmowa musi być umotywowana. Obowiązek przedstawienia dowodów zasadności odmowy spoczywa na Administratorze;
   d. Samodzielnie ustalać skład i wykaz środków, niezbędnych i wystarczających do zapewnienia wykonywania obowiązków Administratora SIODO, przewidzianych przez prawo Rzeczpospolitej Polskiej.
2. Administrator SIODO jest zobowiązany do:
   a. Przed rozpoczęciem przetwarzania DO zobowiązany jest powiadomić organ ochrony praw podmiotów DO o swoim zamiarze przetwarzanie DO, za wyjątkiem przypadków przewidzianych prawem Rzeczpospolitej Polskiej;
   b. W przypadku uzyskania dostępu do DO nie ujawniać osobom trzecim i nie rozpowszechniać DO bez zgody podmiotu DO, jeśli prawo nie stanowi inaczej;
   c. Przedstawić dowód uzyskania zgody podmiotu DO na przetwarzanie jego DO lub dowód istnienia podstaw prawnych przetwarzania DO bez zgody podmiotu;
   d. Przed rozpoczęciem realizacji transgranicznej transmisji DO upewnić się, że na terenie obcego państwa, na terytorium którego odbywa się transmisja DO, jest zapewniona odpowiednia ochrona praw podmiotów DO;
   e. Na żądanie podmiotu DO przerwać przetwarzanie jego danych, wykonywane w celu promowania towarów, prac, usług na rynku poprzez realizację

bezpośrednich kontaktów z potencjalnym konsumentem za pomocą środków łączności, a także w celu agitacji politycznej;

f. Wyjaśnić podmiotowi DO procedurę podejmowania decyzji w informatycznych systemach przetwarzania danych osobowych i ewentualne konsekwencje prawne wynikające z takiego rozwiązania, zapewnić możliwość zgłoszenia sprzeciwu wobec takiego rozwiązania, a także wyjaśnić zasady ochrony przez podmiot DO swoich praw i interesów. Administrator jest zobowiązany uwzględnić sprzeciw, w terminie trzydziestu dni od dnia jego otrzymania oraz powiadomić podmiot o wynikach rozpatrzenia jego sprzeciwu;
g. Gromadząc dane osobowe udzielić podmiotowi DO na jego wniosek informacje przewidzianej prawem Rzeczypospolitej Polskiej. Jeżeli dostarczenie DO przez podmiot jest obowiązkowe i wynika z obowiązującego prawodawstwa, Administrator jest zobowiązany wyjaśnić podmiotowi DO prawne konsekwencje odmowy ich dostarczenia;
h. Jeżeli dane osobowe zostały otrzymane nie od ich podmiotu, Administrator, z wyłączeniem przypadków przewidzianych przez obowiązujące prawodawstwo, przed rozpoczęciem przetwarzania takich danych zobowiązany jest dostarczyć ich podmiotowi następujące informacje:
    i. Nazwę lub nazwisko i imię oraz adres Administratora lub jego przedstawiciela;
    ii. Cel przetwarzania DO oraz jego podstawę prawną;
    iii. Potencjalnych użytkowników DO;
    iv. Ustanowione przez prawo Rzeczypospolitej Polskiej prawa podmiotu DO;
    v. Źródło uzyskania DO.
i. Podejmować działania niezbędne i wystarczające do zapewnienia wykonywania obowiązków Administratora SIODO, przewidzianych ustawodawstwem obowiązującym w Rzeczypospolitej Polskiej;
j. Opublikować lub w inny sposób zapewnić nieograniczony dostęp do dokumentu, który określa politykę Administratora w zakresie przetwarzania DO, w szczególności do informacji o realizowanych wymaganiach dotyczących ochrony DO;
k. Przy gromadzeniu DO z zastosowaniem sieci teleinformatycznych, opublikować we właściwej sieci teleinformatycznej dokument definiujący politykę Administratora w zakresie przetwarzania DO oraz informacje o sposobie realizacji działań chroniących DO, a także zapewnić możliwość dostępu do ww. dokumentów z wykorzystaniem narzędzi właściwej sieci teleinformatycznej;
l. Na żądanie uprawnionego organu chroniącego prawa podmiotów DO, zaprezentować dokumenty i lokalne akty prawne przewidziane przez ustawodawstwo Rzeczypospolitej Polskiej i/lub w inny sposób potwierdzić podjęcie

działań koniecznych i wystarczających dla zapewnienia należytego wykonywania obowiązków Administratora SIPDO;

m. Przetwarzając dane osobowe podejmować prawne, organizacyjne i techniczne środki, lub zapewniać ich akceptację, niezbędne do ochrony DO przed niesankcjonowanym lub przypadkowym dostępem, zniszczeniem, zamianą, blokowaniem, kopiowaniem, udostępnianiem, rozpowszechnianiem, a także przed innymi bezprawnymi działaniami w odniesieniu do DO;
n. Informować bezpłatnie, w trybie przewidzianym przez prawo Rzeczypospolitej Polskiej, podmiot DO lub jego przedstawiciela o istnieniu DO odnoszących się odpowiedniego podmiotu danych osobowych, a także oferować możliwość zaznajomienia się z tymi danymi w przypadku zwrócenia się o to podmiotu DO lub jego przedstawiciela w przeciągu nie więcej niż 30 dni od daty otrzymania stosownego wniosku;
o. W przypadku odmowy udzielenia informacji o dysponowaniu DO podmiotu, będącej odpowiedzią na wniosek podmiotu DO lub jego przedstawiciela, Administrator zobowiązany jest podmiotowi DO lub jego przedstawicielowi przedstawić pisemne uzasadnienie odmowy, zawierające odwołanie do właściwego przepisu prawa obowiązującego w Rzeczypospolitej Polskiej, będącego podstawą odmowy, w terminie 30 dni od otrzymania wniosku;
p. W terminie nie dłuższym niż siedem dni roboczych od dnia dostarczenia przez podmiot DO lub jego przedstawiciela informacji stwierdzających, że DO podmiotu są niekompletne, niedokładne lub nieaktualnymi, Administrator zobowiązany jest dokonać ich modyfikacji. W terminie nie dłuższym niż siedem dni roboczych od dnia złożenia przez podmiot DO lub jego przedstawiciela informacji potwierdzających, że przetwarzane DO zostały uzyskane nielegalnie lub nie są niezbędne do zdefiniowanego celu przetwarzania, Administrator zobowiązany jest zniszczyć takie dane. Administrator zobowiązany jest do poinformowania podmiotu DO lub jego przedstawiciela o wprowadzonych zmianach i podjętych działaniach, a także podjęcia odpowiednich kroków w celu powiadomienia osób trzecich, którym DO podmiotu zostały przekazane;
q. Po otrzymaniu wniosku od organu przewidzianego w prawodawstwie Rzeczypospolitej Polskiej do ochrony praw podmiotów DO, w terminie 30 dni od otrzymania takiego wniosku, przekazać wszelką niezbędną informację;
r. W przypadku wykrycia nieuzasadnionego przetwarzania DO wykonywanego przez Administratora lub osobę działającą w jego imieniu, Administrator w terminie nie przekraczającym trzech dni roboczych od daty wykrycia nadużycia zobowiązany jest do zakończenia niezgodnego z prawem przetwarzania DO lub zagwarantowania, że podmiot działający w imieniu Administratora zaprzestanie bezprawnego przetwarzania DO;

s. W przypadku kiedy zapewnienie legalności przetwarzania DO jest niemożliwe, Administrator w terminie nie dłuższym niż dziesięć dni roboczych od daty wykrycia nadużycia, zobowiązany jest zniszczyć takie DO lub zapewnić ich zniszczenie przez podmiot działający w jego imieniu. O usunięciu naruszeń lub o likwidacji DO, Administrator zobowiązany jest poinformować podmiot DO lub jego przedstawiciela. W przypadku, kiedy wniosek podmiotu DO lub jego przedstawiciela skierowany był dodatkowo do organu przewidzianego w prawie do ochrony DO podmiotów, Administrator ma obowiązek poinformowania również tego organu;

t. W przypadku osiągnięcia celu przetwarzania DO, Administrator zobowiązany jest do zaprzestania ich przetwarzania lub zagwarantowania zakończenia ich przetwarzania, jeżeli przetwarzanie DO wykonywane jest przez inny podmiot działający na zlecenie Administratora, zniszczyć DO lub zapewnić ich zniszczenie (jeśli przetwarzanie wykonywane jest przez podmiot działający na zlecenie Administratora). Operacje zniszczenia powinny być zrealizowane w terminie nie dłuższym niż trzydzieści dni od daty osiągnięcia celu przetwarzania DO, o ile nie postanowiono inaczej w umowie, stroną, beneficjentem lub gwarantem, której jest podmiot DO, bądź inną umową między Administratorem a podmiotem DO lub jeśli Administrator nie jest uprawniony do wykonywania przetwarzania DO bez zgody ich podmiotu, na zasadach przewidzianych przez ustawodawstwo Rzeczypospolitej Polskiej;

u. W przypadku wycofania przez Podmiot DO zgody na ich przetwarzanie Administrator jest zobowiązany do zaprzestania ich przetwarzania lub zagwarantowania zaprzestania przetwarzania przez podmiot przetwarzający dane w imieniu Administratora oraz w przypadku, kiedy zachowanie DO nie jest wymagane do celów ich przetwarzania. Administrator lub podmiot działający w jego imieniu jest zobowiązany zniszczyć przetwarzanie DO w terminie nie dłuższym niż trzydzieści dni od daty otrzymania określonego odwołania, jeżeli nie postanowiono inaczej w umowie, którego stroną, beneficjentem lub gwarantem jest podmiot DO, bądź w innej umowie pomiędzy Administratorem a Podmiotem DO lub jeśli Administrator nie jest uprawniony do wykonywania przetwarzania danych bez zgody Podmiotu DO na zasadach przewidzianych przez ustawodawstwo Rzeczypospolitej Polskiej;

v. Wyznaczyć osobę odpowiedzialną za organizację obsługi DO.

XI. Zasady przetwarzania i ochrony DO

1. Zapewnienie poufności DO przetwarzanych przez Administratora jest obowiązkiem wszystkich osób, które poznały ich zawartość.
2. Pracownicy Administratora przygotowujący dokumenty są zobowiązani do uzyskania w określonych przypadkach zgody właścicieli DO na ich przetwarzanie.

3. W przypadku naruszenia ustalonego porządku przetwarzania DO pracownicy Administratora ponoszą odpowiedzialność zgodnie z §XIII niniejszego dokumentu.
4. DO podmiotów dostępne na papierowych nośnikach, przetwarzane przez Administratora, przechowywane są w działach (lub u pracowników) posiadających uprawnienia do obsługi odpowiednich DO. Prawo do dopuszczania pracowników do ręcznego przetwarzania DO posiada Prezes.
5. Papierowe nośniki DO nie mogą pozostawać bez nadzoru. W przypadku opuszczania miejsca pracy pracownik prowadzący ręczne przetwarzanie DO powinien przenieść nośniki do sejfu, zamykanej szafy lub w inny sposób ograniczyć nieautoryzowany dostęp do nich. W przypadku utraty lub uszkodzenia DO odbywa się w miarę możliwości ich odzyskanie.
6. Miejsca przechowywania dokumentów zawierających DO:
    a. DO klientów Administratora (umowy, akty, uzgodnienia, formularze, kopie paszportów, inne podobne dokumenty zawierające DO klientów Administratora, nośniki pamięci, np. karty pamięci flash, dyski wymienne) przechowywane są w głównych i dodatkowych siedzibach Administratora, umieszczone na półkach wyposażonych w zamek lub kłódkę na kluczyk. Osoba odpowiedzialna za wypełnienie powyższych zaleceń określana jest rozporządzeniem Prezesa;
    b. DO pracowników Administratora, dokumenty, nośniki informacji (karty pamięci flash, dyski wymienne itp.) są przechowywane w zamykanym sejfie. Osoba dokonująca kontroli wypełnienia powyższych zaleceń: ABI lub IOD.
7. Wydawanie dokumentów do zapoznania się z nimi przez osoby dopuszczone w celu realizacji swoich obowiązków, realizowane jest na okres nie dłuższy niż jeden dzień roboczy.
8. Inne nośniki informacji mogą być przechowywane w głównych i dodatkowych biurach Administratora na zamykanych półkach lub w sejfie Administratora. Osobę odpowiedzialną za weryfikację wypełnienia powyższych zaleceń określa rozporządzenie Prezesa.
9. W czasie pracy w trybie przeglądania lub edycji z SIODO Administratora niedopuszczalnym jest umożliwienie osobom nie posiadającym niezbędnych uprawnień zapoznania się z zawartością ekranów zawierających DO.
10. Po otrzymaniu przez pracownika Administratora DO, który zgodnie ze swoim zakresem obowiązków otrzymuje je od klienta, pracownika Administratora lub innej osoby, obowiązkowo przeprowadzana jest kontrola ich poprawności. Wprowadzanie DO uzyskanych przez pracownika Administratora do SIODO może być realizowane wyłącznie przez pracowników posiadających prawo dostępu do odpowiednich DO. Pracownicy Administratora wprowadzający informacje do SIODO ponoszą odpowiedzialność za ich prawdziwość i kompletność.

11. Manualne przetwarzanie DO zawartych na papierowych nośnikach, bez użycia narzędzi automatyzacji (przy sporządzaniu których nie jest używany komputer) należy dostosować do obowiązującego akceptowalnego ryzyka.
12. W przypadku manualnego przetwarzania różnych kategorii DO należy wykorzystywać niezależny nośnik dla każdej kategorii DO.
13. Jeżeli DO gromadzone na nośniku papierowym są przetwarzane manualnie, należy:
    a. Nie dopuszczać do rozmieszczania na jednym nośniku papierowym DO, których cele przetwarzania są z zasady niekompatybilne;
    b. DO muszą wyróżniać się spośród innych informacji, w szczególności poprzez rozmieszczenie ich w specjalnych sekcjach lub polach formularzy.
14. W przypadku użycia standardowych formularzy dokumentów, których charakter zakłada włączenie do nich DO, należy:
    a. Standardowy formularz lub związane z nim dokumenty (instrukcja jego wypełniania, rejestry i dzienniki) muszą zawierać informacje o celu manualnego przetwarzania DO, nazwisko (nazwę) i adres Administratora, nazwisko, imię oraz adres podmiotu DO, źródło uzyskania DO, terminy przetwarzania DO, specyfikację działań nad DO, które będą odbywać się w procesie ich przetwarzania, ogólny opis stosowanych przez Administratora sposobów przetwarzania DO;
    b. Standardowy formularz powinien zawierać pole, w którym podmiot DO może potwierdzić swoją zgodę na manualne przetwarzanie DO;
    c. Standardowy formularz musi być sporządzona w taki sposób, aby każdy z podmiotów DO, zawartych w dokumencie, miał możliwość zapoznania się ze swoimi DO, nie naruszając przy tym praw i interesów innych podmiotów DO;
    d. Standardowy formularz powinien eliminować łączenie pól służących do wprowadzania DO, cele przetwarzania których są z zasady niekompatybilne.
15. Jeśli okres przechowywania DO nie jest określony ustawą, umową której stroną, beneficjentem lub gwarantem jest podmiot DO, przechowywanie DO powinno odbywać się w formie umożliwiającej określenie podmiotu DO, nie dłużej niż wymagają tego cele przetwarzania DO.
16. Przypadki usuwania, blokowania i poprawy DO:
    a. Zniszczenie lub depersonalizacja części danych osobowych, jeśli jest to dozwolone materialnym nośnikiem, powinno odbywać się w sposób uniemożliwiający dalsze przetwarzanie tych DO, z zachowaniem możliwości przetwarzania innych danych, które występowały na materialnym nośniku (np. usuwanie, zaciemnianie);
    b. Poprawa DO w przypadku ich przetwarzania manualnego odbywa się poprzez aktualizację lub zmianę danych na nośniku materialnym, a jeśli nie jest to dozwolone właściwościami technicznymi nośnika – poprzez wprowadzenie na tym samym nośniku materialnym informacji o dokonywanych w nich

zmianach lub poprzez zastosowanie nowego materialnego nośnika z poprawionymi DO.

17. Niszczenie nośników zawierających DO, odbywa się zgodnie z następującymi zasadami:
    a. DO rozmieszczone na papierowych nośnikach są niszczone poprzez wykorzystanie niszczarki zainstalowanej w biurze Administratora. Niszczarka ta powinna spełniać normę DIN 66399 (klasa nie niższa niż P3);
    b. DO rozlokowane w pamięci operacyjnej niszczone są poprzez nanoszenie losowej sekwencji 0,1 na stronie wirtualnej zawierającej usuwane DO;
    c. DO rozlokowane na nośnikach pamięci (karty flash, dysku magnetycznym lub optycznym) poprzez wielokrotne nadpisywanie zgodnie ze standardem DOD 5220.22. W razie potrzeby powinno być zastosowane fizyczne niszczenie nośnika;
    d. Niszczenie DO lub nośnika informacji potwierdzane jest stosownym protokołem, którego wzór znajduje się w załącznikach do niniejszej Polityki.
18. Biuro Administratora, po zakończeniu dnia pracy i nieobecności pracowników, powinno być zamknięte, okna muszą być zamknięte, musi zostać włączony alarm (o ile jest dostępny).
19. Urządzenia sieciowe i serwery należy umieszczać w miejscach niedostępnych dla osób niepowołanych (w specjalnych pomieszczeniach, szafach, skrzynkach), co reguluje stosowny regulamin PBI.
20. Sprzątanie pomieszczeń i obsługa środków technicznych SIODO musi odbywać się pod kontrolą osób odpowiedzialnych za dane pomieszczenia i środki techniczne, eliminując możliwości nieautoryzowanego dostępu do DO, nośników informacji, oprogramowania i technicznych środków przetwarzania, transmisji oraz ochrony informacji SIODO.
21. Do obowiązków administratorów SIODO należy nadzór nad kontami użytkowników, utrzymanie normalnej pracy SIODO, w tym oprogramowania do tworzenia kopii zapasowych danych, a także instalacja i konfiguracja sprzętu i oprogramowania SIODO, niezwiązanego z zapewnieniem bezpieczeństwa DO gromadzonych i przetwarzanych w SIODO. Ponadto, do obowiązków administratorów SIODO wchodzi zapewnienie zgodności sposobu przetwarzania i bezpieczeństwa DO w SIODO z wymaganiami w zakresie poufności, integralności i dostępności DO przypisywanych do konkretnego SIODO i ogólnych wymagań bezpieczeństwa DO określonych przez prawo Rzeczpospolitej Polskiej.
22. W zakres obowiązków administratorów SIODO wchodzi również instalacja, konfiguracja i administracja sprzętu i oprogramowania do ochrony danych, ewidencjonowanie i przechowywanie maszynowych nośników DO, okresowe audyty rejestrów bezpieczeństwa i analiza bezpieczeństwa SIODO, a także udział w wewnętrznych dochodzeń dotyczących naruszenia ustalonego porządku przetwarzania i bezpieczeństwa DO.

23. W celu zapewnienia skutecznej dystrybucji pełnomocnictw, realizacji wzajemnej kontroli i niedopuszczenia do koncentracji funkcji krytycznych dla bezpieczeństwa DO, łączenie uprawnień użytkownika i administratora SIODO jest niezalecane.
24. Kwalifikacje zawodowe oraz szczegółowy wykaz praw i obowiązków administratorów SIODO powinny być zdefiniowane w odpowiednich regulaminach wewnętrznych, z którymi mianowani na stanowiska pracownicy są zaznajamiani, potwierdzając to podpisem.
25. Wewnętrzna kontrola procesu przetwarzania DO u Administratora ma na celu ocenę stanu faktycznego bezpieczeństwa DO, szybkie reagowanie na naruszenia ustalonego porządku ich przetwarzania, a także jego poprawę.
26. Wewnętrzne kontrole przetwarzania i bezpieczeństwa DO ukierunkowane są na rozwiązanie następujących zadań:
    a. Zapewnienie przestrzegania przez pracowników Administratora wymogów niniejszego regulaminu i aktów prawnych regulujących sferę DO;
    b. Ocena kompetencji pracowników, zaangażowanych w przetwarzanie DO;
    c. Zapewnienie sprawności i skuteczności środków technicznych SIODO i środków ochrony DO, ich zgodności z wymaganiami właściwych organów władzy wykonawczej, odpowiedzialnej za sprawy bezpieczeństwa DO;
    d. Wykrycie naruszenia ustalonego porządku przetwarzania DO i terminowe zapobieganie negatywnym skutkom takich naruszeń;
    e. Podejmowanie działań naprawczych mających na celu usunięcie stwierdzonych naruszeń, dotyczących przetwarzania DO oraz funkcjonowania urządzeń technicznych SIODO;
    f. Opracowanie zaleceń dotyczących poprawy sposobu przetwarzania i bezpieczeństwa DO na podstawie wyników działań kontrolnych;
    g. Realizacja kontroli wewnętrznej przestrzeganiem zaleceń i wskazówek dotyczących pojawiających się naruszeń bezpieczeństwa DO.
27. Wyniki działań kontrolnych są opracowywane w postaci oficjalnych dokumentów i stanowią podstawę do opracowania zaleceń dotyczących poprawy sposobu przetwarzania i bezpieczeństwa DO, modernizacji środków technicznych SIODO i środków ochrony DO, uczenia się i doskonalenia kompetencji pracowników zaangażowanych w przetwarzanie DO.

XII. Zarządzanie danymi osobowymi pracowników

1. Niniejszy rozdział Polityki definiuje dodatkowe prawa i obowiązki Administratora i jego pracowników w zakresie przetwarzania DO swoich pracowników.
2. DO pracownika to informacja dotycząca konkretnego pracownika, niezbędna Administratorowi w związku z wiążącym ich stosunkiem pracy.
3. Przetwarzanie DO pracownika może odbywać się wyłącznie w celu zapewnienia przestrzegania ustaw i innych aktów normatywnych oraz prawnych, wspierania

pracowników w zakresie zatrudnienia, szkolenia i awansu, w celu zapewnienia ich osobistego bezpieczeństwa, kontroli ilości i jakości wykonywanej pracy i zabezpieczenia mienia.

4. Administrator nie ma prawa uzyskiwać i przetwarzać DO pracownika dotyczących jego członkostwa w stowarzyszeniach społecznych lub jego działalności związkowej, za wyjątkiem przypadków przewidzianych prawem Rzeczpospolitej Polskiej.
5. Podczas podejmowania decyzji dotyczących interesów pracowników, Administrator nie ma prawa opierać się na DO pracownika, uzyskanych wyłącznie w wyniku ich automatycznego przetwarzania lub pozyskanych drogą elektroniczną.
6. Pracownicy nie muszą rezygnować ze swoich praw w celu zachowania i ochrony tajemnicy.
7. Administrator zobowiązuje się nie ujawniać DO pracownika w celach komercyjnych bez jego pisemnej zgody.
8. Administrator jest zobowiązany poinformować swoich pracowników, osoby trzecie, otrzymujące za zgodą pracownika jego DO o tym, że dane te mogą być wykorzystywane wyłącznie w celach, dla których zostały zgłoszone oraz wymagać od tych osób potwierdzenia, że zasada ta jest przestrzegana. Osoby, które otrzymują DO pracownika są zobowiązane do przestrzegania tajemnicy. Przestrzeganie tajemnicy jest zapewniane podpisaniem stosownej umowy, będącej załącznikiem do niniejsze Polityki. Przepis ten nie ma zastosowania do wymiany DO pracowników przewidzianej przez ustawodawstwo Rzeczpospolitej Polskiej.
9. Dostęp do DO pracowników odbywa się na podstawie rozporządzeń i przepisów zatwierdzonych przez Administratora.
10. Administrator zobowiązuje się nie żądać informacji o stanie zdrowia pracownika, z wyjątkiem tych, które odnoszą się bezpośrednio do możliwości wykonywania przez niego pracy przewidzianej zakresem jego obowiązków.
11. Administrator zobowiązuje się przekazywać DO pracownika jego przedstawicielowi (pełnomocnikowi), zgodnie z ustawodawstwem Rzeczpospolitej Polskiej i ograniczać te informacje tylko do tych DO pracownika, które są niezbędne do wykonania przewidzianych dla przedstawicielami lub pełnomocnika funkcji.
12. Pracownik ma prawo wskazać swojego przedstawiciela lub pełnomocnika w celu ochrony swoich DO.

XIII. Odpowiedzialność za naruszenia Polityki

1. Kadra kierownicza Administratora ponosi odpowiedzialność za niezapewnienie prywatności DO, a także nieprzestrzeganie praw i wolności podmiotów DO w odniesieniu do ich danych, w tym prawa do prywatności, tajemnicy osobistej i rodzinnej.

2. Pracownicy Administratora ponoszą osobistą odpowiedzialność za przestrzeganie wymagań w zakresie przetwarzania i bezpieczeństwa DO, określonych niniejszą Polityką, zgodnie z ustawodawstwem Rzeczpospolitej Polskiej.
3. Pracownik Administratora może być pociągnięty do odpowiedzialności w następujących przypadkach:
    a. Umyślne lub lekkomyślne ujawnienie DO;
    b. Utraty materialnych nośników DO;
    c. Naruszenia niniejszej Polityki oraz innych dokumentów normatywnych Administratora w zakresie dostępu i pracy z DO.
4. W przypadku naruszenia ustalonego trybu przetwarzania i bezpieczeństwa DO, nieautoryzowanego dostępu do DO, ujawnienia DO i spowodowania Administratorowi, jego pracownikom, klientom i kontrahentom materialnej lub innej szkody, sprawcy ponoszą cywilną, karną, administracyjną, dyscyplinarną oraz inną odpowiedzialność, przewidzianą prawem Rzeczpospolitej Polskiej.

Bibliografia

[1] J. Krawiec i G. Ożarek, Certyfikacja w informatyce, Wydanie drugie red., Warszawa: Polski Komitet Normalizacyjny, 2014.

[2] P. K. Normalizacyjny, *PN-EN ISO/IEC 27001:2017-06 - wersja polska,* 2017.

[3] P. K. Normalizacyjny, *PN-ISO/IEC 27000-1:2014-01 - wersja polska,* 2014.

[4] P. K. Normalizacyjny, *PN-ISO/IEC 27013:2014-01 - wersja polska,* 2014.

[5] A. Gawrońska-Baran i A. Smerd, RODO w zamówieniach publicznych, Warszawa: Wiedza i Praktyka, 2018.

[6] A. Sagan-Jeżowska, Klauzule RODO Wzory klauzul z praktycznym komentarzem, Warszawa: C.H. Beck , 2018.

[7] B. Pióro, RODO Ochrona danych osobowych, Warszawa: Infor, 2018.

[8] K. Czajkowska-Motosiuk , RODO dla samorządu i administracji, Warszawa: Infor, 2018.

[9] K. Gałaj-Emilańczyk, Wdrożenie RODO w małych i średnich organizacjach. Praktyczny poradnik(eBook), Warszawa: ODDK, 2018.

[10] K. Gałaj-Emiliańczyk , Dokumentacja ochrony danych osobowych, Warszawa: Difin, 2016.

[11] M. Gawroński, Rodo Przewodnik ze wzoram, Warszawa: Wolters Kluwer, 2018.

[12] M. Mędrala, RODO dla kadrowych i HR, Warszawa: Infor, 2018.

[13] P. zbiorowa, RODO – prawo unijne i krajowe, Warszawa: ODDK, 2018.

[14] P. zbiorowa, RODO w 15 krokach, Warszawa: C.H. Beck.

[15] S. Greengard, „The new face of war," *Communications of the ACM,* tom 53, nr 12, pp. 20-22, 2010.

[16] Y. Elayat, E. Zananiri, M.-L. Wong, A. Porter i J. George, „Zero Days VR," w *Proceeding SIGGRAPH '17 ACM SIGGRAPH 2017 Computer Animation Festival*, Los Angeles, 2017.

[17] T. R. Peltier, Information security policies, procedures, and standards: guidelines for effective information security management, Boca Raton: CRC Press, 2002.

[18] J. S. T. R. O'Hanley, Information Security Management Handbook, Boba Raton: CRC Press, 2014.

[19] D. W. Straub, S. Goodman and R. L. Baskerville, Information Security. Policy, Process and Practices, London: M.E. Sharpe, 2008.

[20] W. Stallings, Cryptography and Network Security: Principles and Practice, VI red., Boston: Pearson, 2014.

[21] D. R. Stinsom i M. B. Paterson, Cryptography : theory and practice, IV red., Boca Raton: CRC Press, 2019.

[22] A. S. Tanenbaum i A. S. Woodhull, Operating Systems Design and Implementation, 3 red., New Jersey: Prentice Hall, 2006.

[23] S. E. Donaldson, S. G. Siegel, C. K. Wiliams i A. Aslam, Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against, New York: Apress, 2018.

[24] G. Tomsho, Guide to Operating Systems, Boston: Cengage Learning, 2017.

[25] S. Shivani, S. Agarwal i J. S. Suri, Handbook of Image-Based Security Techniques, Boca Raton: CRC Press Taylor & Francis Group, 2018.

[26] F. Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, II red., Boca Raton Taylor & Francis Group: CRC Press, 2017.

[27] A. Yahya, Steganography Techniques for Digital Images, Cham, Switzerland: Springer International Publishing AG, 2019.

[28] Polski Komitet Normalizacyjny, *PN-ISO/IEC 27000 - Technika informatyczna. Techniki bezpieczeństwa. System zarządzania bezpieczeństwem informacji. Przegląd i terminologia,* Warszawa: Polski Komitet Normalizacyjny, 2014.

[29] R. Lehtinen and G. Gangemi Sr., Computer Security Basics, 2 ed., T. Apandi, Ed., Sebastopol, CA: O'Reilly Media, Inc., 2011.

[30] M. Vatsa, R. Singh and A. Majundar, Deep Learning in Biometrics, Boca Ratton, FL: CRC Press, Taylor & Francis Group, 2018.

[31] R. Jiang, S. Al-maadeed, A. Bouridane and D. Crookes, Biometric Security and Privacy. Opportunities & Challenges in The Big Data Era, A. Beghdadi, Ed., Baton Rouge, Louisiana: Springer International Publishing, 2017.

[32] R. Das, The Science of Biometrics, New York, NY: Routledge, 2019.

[33] "Is facial recognition technology the future of retail security?," 19 09 2018. [Online]. Available: https://www.get-licensed.co.uk/get-daily/is-facial-recognition-technology-the-future-of-retail-security/. [Accessed 07 12 2018].

[34] Flir, "Image Comparison - Face," [Online]. Available: http://shop.flir.com/science/display/?id=60838. [Accessed 19 09 2018].

[35] J. L. Hennessy and D. A. Patterson, Computer Architecture a Quantitative Approach, I ed., San Francisco: Morgan Kaufmann, 2002, p. 1143.

[36] A. Yardin, Computer systems architecture, Boca Raton: CRC Press, 2016.

[37] H. F. Tipton and M. Krause, Information Security Management Handbook, 6 ed., Boca Raton: CRC Press, 2012.

[38] D. Cannon, B. T. O'Hara i A. Keele, CISA®: Certified Information Systems Auditor. Study Guide, IV red., Indianapolis, Indiana: John Wiley & Sons, 2016.

[39] A. Otero, Information Technology Control and Audit, V ed., Boca Raton: CRC Press, Taylor & Francis Group, 2019.

[40] W. Allsopp, Advanced Penetration Testing. Hacking the World's Most Secure Networks, Hoboken, New Jersey: John Wiley & Sons, 2018.

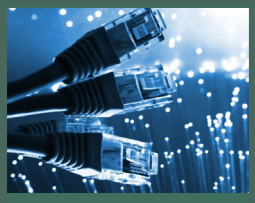
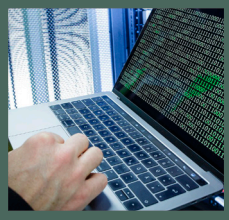
[41] V. K. Velu, Mastering Kali Linux for Advanced Penetration Testing, II red., Birmingham: Packt, 2018.

[42] P. Bramwell, Hands-On Penetration Testing on Windows, Birmingham, UK: Packt Publishing, 2018.

[43] S. Rahalkar, Quick Start Guide to Penetration Testing, New York, USA: Apress, 2019.

[44] „Oficjalna Strona Polskiego Komitetu Normalizacyjnego," Polski Komitet Normalizacyjny, [Online]. Available: https://www.pkn.pl/. [Data uzyskania dostępu: 01 09 2018].



Nie tak dawno, regiony naszego kraju wybrały inteligentne specjalizacje, w których upatrują swoich szans zrównoważonego rozwoju. Jedną z najbardziej obiecujących, a zarazem niedocenionych jest produkcja informacyjna, którą nazywamy proces oddziaływania na informację wykorzystujący narzędzia informatyczne. Jego celem jest uzyskanie nowej wiedzy, niezbędnej do tworzenia dóbr materialnych i duchowych, zapewniających istnienie i rozwój człowieka oraz społeczeństwa. Produkty i usługi informacyjne, obok produktów i usług materialnych są podstawowymi składnikami produktu krajowego większości państw. Podkarpacie spełnia wszelkie wymagania, niezbędne do uczynienia produkcji informacyjnej podstawą zrównoważonego rozwoju.

Aby produkcja informacyjna przynosiła odpowiednie efekty, niezbędne jest wytworzenie kapitału informacyjnego, będącego specyficzną formą kapitału transakcyjnego, urzeczywistnionego w postaci dóbr niedostępnych w gotowej formie w przyrodzie, będących rezultatem działalności człowieka. Wchłania on nowe informacje, pozostając jednocześnie źródłem wiedzy niezbędnej do tworzenia nowych i rozwijania starych produktów. Podstawą tworzenia kapitału informacyjnego jest masowa edukacja.

WYŻSZA SZKOŁA
INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie