POLITECHNIKA CZĘSTOCHOWSKA

Wydział Inżynierii Produkcji i Technologii Materiałów

ROZPRAWA DOKTORSKA

mgr inż. Estera Pietras

Zarządzanie bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej

Promotor: dr hab. inż. Marcin Knapiński, prof. PCz.

Częstochowa, 2021r.

SPIS TREŚCI

WSTĘP

Rozwój technologiczny niesie za sobą pozytywne skutki związane m.in.: z poszerzeniem metod i kanałów komunikacji, obszernym dostępem do wiedzy, jak również udoskonaleniem gromadzenia i przetwarzania informacji. Świat bez technologii informatycznych, wykorzystujących oczywiście internet, nie mógłby osiągnąć tak wysokiego rozwoju cywilizacyjnego. Rozwój globalnego rynku automatyzuje procesy produkcyjne, finansowo-księgowe, kadrowe, projektowe itp., które z kolei umożliwiają szybką komunikację, chociażby w postaci zawierania np. umów na odległość. Tego typu działania, zwłaszcza oparte są o przetwarzanie informacji. Jest to w szczególności ważne, w coraz bardziej zintegrowanym środowisku biznesowym.

Informacja w przedsiębiorstwach może być wyrażona w różnych formach: ustnej, podczas rozmowy, drukowanej lub przechowywanej w sposób elektroniczny. Jednak niezależnie od tego, w jakiej postaci występuje i za pomocą, jakich środków jest udostępniona lub utrwalona, to zawsze powinna być w należyty sposób chroniona.

W tym kontekście celowym jest wskazanie działań polegających na przygotowaniu się na zagrożenie wywołane brakiem odpowiedniej ochrony informacji, niewłaściwego sposobu zarządzania personelem, niezadawalającego dystrybuowania sprzedaży produktu gotowego itp. Nieprzemyślane postępowanie może zostać wykorzystane przez konkurencję, obniżając efektywność pracy jednostki gospodarczej. Stanowi to punkt wyjścia dla przedsiębiorców, którzy powinni czynić starania o zapewnienie należytego stanu bezpieczeństwa w organizacji, bowiem pomyłki w przechowywaniu, przetwarzaniu, udostępnianiu informacji mogą pozbawić przedsiębiorcę poczucia stabilizacji, a w konsekwencji prowadzić do strat finansowych, operacyjnych, czy konsekwencji prawnych. Nie wprowadzenie działań zapobiegających powstawaniu zagrożeń wiąże się z nie zapewnieniem ciągłości działań obejmujących ludzi, procesy i systemy informacyjne oraz brakiem możliwości ograniczenia ryzyka do poziomu akceptowalnego [1,2]. Zatem, organizacje i ich systemy narażone są na naruszenia bezpieczeństwa informacji, pochodzące z wielu źródeł w postaci przestępstw, fałszerstw komputerowych, sabotażu komputerowego, szpiegostwa gospodarczego, manipulowania urządzeniami, phishingu, kradzieży urządzeń służbowych, podsłuchowi, szantażu, podszywania się pod inną osobę, strategii wyrafinowanych metod ataku, działalności grup świadomie manipulujących przekazem informacji, czy nieuprawnionego ujawnienia informacji. Wirusy, makrowirusy, szkodliwe oprogramowanie, bomby logiczne, czasowe, robaki, koń trojański, aplikacje

szpiegujące, włamania komputerowe, dialery, tylne drzwi i wiele innych niebezpiecznych praktyk są powszechnym zagrożeniem. Zważywszy na łatwość pozyskiwania, przetwarzania, gromadzenia oraz przechowywania informacji należy zwrócić uwagę na stale rosnącą liczbę zagrożeń oraz ich podatności.

W nawiązaniu do omawianych zagrożeń amerykańska firma Dark Reading powołuje się w raporcie na badania Ponemon Institute, gdzie można zauważyć, że ataki te są najczęściej internetowe wywołane złośliwym kodem lub też niefrasobliwym działaniem użytkowników systemu, czy też innych pracowników. Fakt, że 90% kosztów wywołanych praktykami i atakami cyberprzestępców, w odniesieniu do jednej organizacji pokazuje powagę problemu bezpieczeństwa informacji. Jak podaje raport straty wywołane atakiem internetowym kosztują przedsiębiorstwo 124 083$. Tymczasem dla porównania straty związane z celowym działaniem pracowników wynoszą 100300 $ [3].

W związku z występującymi problemami niedostatecznej ochrony systemu bezpieczeństwa informacji oraz tym, że temat ten jest nadal ważny i aktualny podjęto próbę poszerzenia wiedzy w zakresie sposobu ochrony informacji oraz zaproponowano system zarządzania bezpieczeństwem informacji, zmniejszający ryzyko utraty informacji.

Niniejsze opracowanie składa się z sześciu rozdziałów. Pierwsza część zawiera dwa rozdziały, które podejmują problematykę bezpieczeństwa i ochrony informacji, wskazując na system zarządzania redukujący ryzyko w przedsiębiorstwie. W omawianych rozdziałach zaprezentowano klasyfikacje, rodzaje i ich źródła oraz skutki zagrożeń. Ponadto zaprezentowano pogląd rozporządzeń, aktów prawnych, które regulują temat należytej ochrony informacji. Dodatkowo przedstawiono pogląd autorów, którzy zajmują się tematem systemu zarządzania bezpieczeństwem informacji w artykułach naukowych, książkach, rozprawach doktorskich wskazując, na praktyczną wartość dobrych praktyk rozpatrywanych, w kontekście systemowym i procesowym.

Natomiast druga część pracy obejmuje cztery rozdziały, podejmujące temat bieżącego stanu w organizacjach, gdzie wykorzystano metody, techniki w celu ochrony przed powstającymi zagrożeniami. Przeprowadzone badania ujawniły jasny obraz ciągłej potrzeby analizy poziomu bezpieczeństwa informacji oraz opracowania systemu związanego z zarządzaniem ryzykiem. Na podstawie badań zdiagnozowano luki występujące w systemie bezpieczeństwa oraz podano propozycje ich zmian. W efekcie końcowym opracowano projekt systemu ZBI. W projekcie określono założenia

i przedstawiono budowę systemu ZBI. Zatem przedstawiono gotowe do wprowadzenia narzędzie, reagujące na wektor wejściowy, czyli pojawiające, się zagrożenia. Za wektor wyjściowy uznano zabezpieczenia, które jako zbiór procedur z zakresu obowiązków minimalizowania wpływu zagrożeń, będzie można powielić pod kątem, tych samych działań. Stworzone procedury wykazują charakter uniwersalności i z powodzeniem mogą być stosowane w różnych obszarach organizacji.

Ideą pracy jest przedstawienie znaczenia wpływu analizy poziomu bezpieczeństwa informacji, jako narzędzia do diagnozowania oraz ulepszania działań w procesie zarządzania BI. Chcąc scharakteryzować faktyczny stan bezpieczeństwa w organizacjach przeprowadzono badania w dziewięciu przedsiębiorstwach z branży motoryzacyjnej, w celu określenia poziomu bezpieczeństwa w badanych jednostkach. Otrzymane wyniki pozwoliły, na podjęcie działań w kierunku oszacowania poziomu ryzyka utraty informacji. Dzięki takiemu postępowaniu opracowano katalog zagrożeń. Zawarta w nim klasyfikacja zagrożeń pozwoli na określenie kierunków funkcjonowania SZBI oraz jego uwarunkowań. W związku z tym, nadrzędnym celem pracy jest wykazanie, że utrzymanie wymaganego poziomu atrybutów bezpieczeństwa informacji, jako trzonu SZBI zapewni ochronę strategicznym zasobom posiadanym, przez organizacje.

Całość rozprawy doktorskiej zamknięto w podsumowaniu opartym o wnioski wynikające z przeprowadzonej analizy poziomu bezpieczeństwa informacji w przedsiębiorstwach, bibliografię, spis tabel, rysunków. Natomiast w załącznikach zamieszczono kwestionariusz ankiety, wywiadu i obserwacji oraz przykładową Politykę Bezpieczeństwa Informacji, którą mogą zaadoptować przedsiębiorcy dla potrzeb swoich organizacji. W załącznikach zamieszczono przykładowe procedury wyselekcjonowanego działania systemu, pomocnego w identyfikacji pojawiającego się zagrożenia, klasyfikowaniu go oraz sposobu postępowania podczas wdrożenia nowych środków naprawczo doskonalących.

Autorka pracy składa podziękowania zarządom i wszystkim pracownikom, którzy wzięli udział w badaniu i poświęcili swój czas i udzielili merytorycznych odpowiedzi, na pytania w kwestionariuszu ankiety oraz dyskusji na temat bezpieczeństwa informacji.

1. TEORETYCZNE UJĘCIE PROBLEMATYKI BEZPIECZEŃSTWA I OCHRONY INFORMACJI W PRZEDSIĘBIORSTWIE

1.1. Pojęcie ochrony i bezpieczeństwa informacji

Ludzie starają się od dawna zapewnić sobie bezpieczeństwo szukając różnych sposobów mogących zabezpieczyć życie jednostki i społeczeństwa. Ponadto poszukują i tych, które pozwalają na bezpieczną egzystencję, rozwój i ochronę danego państwa. Tak, więc z tego wynika teza, że cyt. ”*Bezpieczeństwo nie jest wszystkim, lecz bez bezpieczeństwa, wszystko jest niczym” Klaus Neuman.* Przyjrzyjmy się co na temat definicji bezpieczeństwa myślą inni.

Słownik języka polskiego definiuje bezpieczeństwo, jako stan pewności, niezagrożenia. To pierwsze znaczy, że można ufnie być przekonanym i przeświadczonym o bezpieczeństwie, natomiast drugi element pozwala na to by nie czuć niebezpieczeństwa.

Wielu uczonych dokonuje różnego podziału bezpieczeństwa w zależności np. od zasięgu na: globalne, regionalne, narodowe (wewnętrzne, zewnętrzne) itp. lub też np. w ujęciu podmiotowym (gdzie podmiotem jest człowiek, grupa społeczna), czy też przedmiotowym dzieląc je na: polityczne, militarne, energetyczne, społeczne, ekologiczne itp.

Wydaje się, że problematyka bezpieczeństwa ogólnie jest zrozumiała dla przeciętnego człowieka, jednak sprecyzowanie jej definicji nie należy do najłatwiejszych zadań. Wynika to z wieloznaczności i jej wpływu na różne dziedziny życia człowieka.

P. Bączek przedstawia w swojej książce, że pomimo tylu odniesień i znaczeń można wyróżnić wspólny mianownik, który „*bezpieczeństwo wiąże z poczuciem stabilności i trwałości określonego stanu rzeczy, z odczuciem braku zagrożenia wewnętrznego a także zewnętrznego, a ponadto także z doznawaniem pewności i spokoju w codziennym bytowaniu, ufności”* [4].

Bezpieczeństwo jest ważną wartością nie tylko dla jednostek czy grup społecznych, ale też dla całych państw i systemów międzynarodowych. Jest nadrzędną potrzebą człowieka, całych grup społecznych, państwa czy też przedsiębiorstwa, a jego

brak wywołuje skrajnie negatywne emocje. W roku 1943 Abraham Harold Maslow stworzył teorie hierarchii potrzeb człowieka skatalogowanych od potrzeb podstawowych do potrzeb wyższego rzędu. Piramida Maslowa oddaje istotność potrzeb, zaspakajanie tych z niższego poziomu umożliwia człowiekowi podjęcie działań w celu zaspokojenia potrzeb znajdujących się na wyższym poziomie [5]. Zauważa się, że istotną potrzebą człowieka jest właśnie bezpieczeństwo. Zajmuje ono drugie miejsce, od razu po potrzebach fizjologicznych. Bezpieczeństwo gwarantuje, więc stabilność.

Jednak bezpieczeństwo nierozerwalnie wiąże się z zagrożeniami. Są to dwa stany przeciwstawne sobie, a jednak występujące w społeczeństwie. Poczucie bezpieczeństwa determinowane jest brakiem zagrożenia.

W kontekście ogólnie znanych definicji chociażby Daniela Frei, który uważa, „że *stan bezpieczeństwa pojawia się, gdy zagrożenie jest nieznaczne, a jego postrzeganie jest słuszne”* utożsamia się bezpieczeństwo ze stanem braku zagrożenia [5].

Natomiast bezpieczeństwo informacji rozumiane jest, jako całokształt działań skoncentrowanych na zabezpieczeniu zasobów informacyjnych przed zagrożeniem dostępu do informacji, przechowywania jej i transmisji. Chodzi o niedopuszczenie do ujawnienia jej w żadnej postaci, czy to w formie dokumentów papierowych, czy też plików danych. Bezpieczeństwem informacji oznacza działanie, metody, czy też system, który zabezpiecza zasoby informacyjne.

W kontekście głównego tematu rozważań niniejszej pracy warto zwrócić uwagę na spostrzeżenia innych znawców literatury, którzy w swoich publikacjach wypowiadają się na temat bezpieczeństwa informacji.

P. Tyrała uważa, że bezpieczeństwo informacji to działanie ukierunkowane na zabezpieczeniu aktywów informacyjnych w pamięciach komputerów oraz w sieciach teleinformatycznych. Ponadto zauważył on, że jest to całokształt procesów, podczas których dochodzi do generowania oraz przetwarzania informacji [6].

Również E. Nowak i M. Nowak w swoim podręczniku naukowym [7] zauważają, że bezpieczeństwo informacji to stan warunków wewnętrznych i zewnętrznych, który pozwala na posiadanie, przetwarzanie i swobodę rozwoju społeczeństwa informacyjnego.

Z brytyjskiego standardu zarządzania bezpieczeństwem informacji możemy się dowiedzieć, że bezpieczeństwo informacji należy rozumieć, jako proces zarządzania

bezpieczeństwem na wszystkich obszarach występowania informacji w działalności organizacji [8].

Natomiast norma ISO/IEC 27002: 2017 określa bezpieczeństwo informacji, jako zachowanie następujących trzech cech informacji: dostępności, poufności oraz integralności. W porównaniu z poprzednią edycją normy (ukazała się w 2005r.) norma z 2017r. zwraca uwagę na zachowanie jeszcze innych cech takich jak: autentyczność, rozliczalność, niezawodność, niezaprzeczalność [19]. Poniższa tabela opisuje szerzej omawiane cechy.

Tabela 1. Charakterystyka poszczególnych atrybutów bezpieczeństwa

Poufność-zapewnienie, że informacja nie jest udostępniana bądź ujawniana osobom podmiotom i procesom nieuprawnionym	**Integralność**-zapewnienie integralności danych i systemu **Integralność danych**- zapewnienie, że dane nie zostały zamienione w sposób nieautoryzowany, zapewnienie dokładności i kompletności aktywów, czyli wszystkiego, co ma wartość dla organizacji **Integralność systemu**-zapewnienie, że system realizuje swoje funkcje w sposób nienaruszony
Rozliczalność-wiąże się z jednoznacznym przypisaniem określonego zakresu działań jednego podmiotu	**Dostępność**-zakłada możliwość autoryzowanego wykorzystania danych i informacji w pożądanym czasie, właściwość bycia dostępnym
Autentyczność –zapewnienie, że tożsamość podmiotu bądź zasobu jest zgodną z zdeklarowaną (dotyczy to użytkowników procesów, systemów)	**Niezawodność**-oznacza stałe spójne zamierzone zachowania oraz skutki

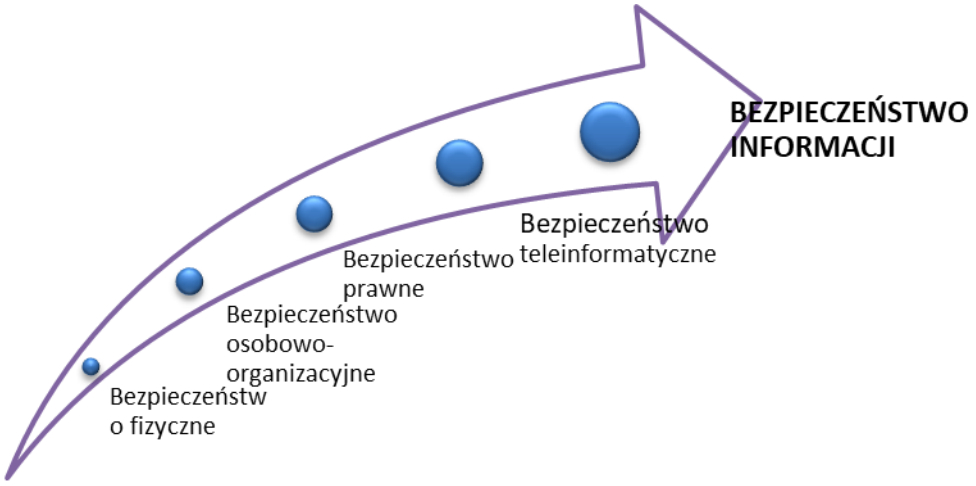
Źródło: Opracowanie na podstawie [9,19]

Dodatkowo wspomniany standard wskazuje na rolę jeszcze innych cech, jakimi są: funkcjonalność, czytelność przedstawienia, zdolność przetwarzania oraz zrozumiałość. Niemniej jednak trzy pierwsze atrybuty przedstawiają fundament istoty bezpieczeństwa informacji. To, która z tych cech będzie kluczowa, zależy od okoliczności. Dla instytucji rządowych, konsultingowych, czy bankowych niezwykle ważna jest poufność, gdyż ujawnienie informacji osobom nieuprawnionym podważa reputację organizacji. Natomiast dla innych najważniejsza będzie integralność w procesie przetwarzania danych. Z kolei dostępność będzie najistotniejszym czynnikiem funkcjonowania wszystkich organizacji z sektora usług, gdzie krótka przerwa w działaniu biznesowym powoduje lawinowe straty finansowe.

Dokonując dalszej interpretacji pojęcia bezpieczeństwa informacji można, zatem ustalić, że jest to zapewnienie spójności, niezawodności i tajności podczas gromadzenia informacji i udostępniania jej jedynie osobom do tego upoważnionym.

Poza tym zdaniem autorki bezpieczeństwo informacji znacznie wykracza poza zapis w formie papierowej czy w systemach informatycznych. W tym wypadku należy również pamiętać o zapisie w pamięci ludzkiej.

Podstawową determinantą zaaplikowania do organizacji idei bezpieczeństwa informacji są cztery obszary, o jakie powinna zadbać firma, która w pełni chce zarządzać bezpieczeństwem informacji. Prezentuje to rysunek nr.1.



Rysunek 1. Definicja bezpieczeństwa informacji
Źródło: opracowanie własne na podstawie [10]

Szerzej wpływ składowych na bezpieczeństwo informacji został omówiony w rozdziale 2.2. Cele i zadania SZBI.

Bezpieczeństwo fizyczne

Kluczową ochroną przed zagrożeniem stanowi zbiór konwencjonalnych środków ochronnych stosowanych w jednostkach gospodarczych [1]. Pojęcie to obejmuje wszelkie rozwiązania dotyczące kontroli ruchu osób, pojazdów, towarów w obszarze przedsiębiorstwa i jego otoczeniu. Te zabezpieczenia pełnią funkcję związaną z wykrywaniem włamań (umożliwia wykrycie obecności osób w określonych strefach), kontrolą dostępu (pozwala na ograniczenie ruchu osób, pojazdów oraz identyfikację osób i uwierzytelnienie ich dostępu) oraz nadzorem telewizyjnym (pomocny w wyjaśnianiu wątpliwości w przypadku ewentualnego włamania sygnalizowanego przez system detekcji).

Bezpieczeństwo osobowo-organizacyjne

Wiąże się z przygotowaniem i doskonaleniem procedur istotnie wpływających na zapewnienie bezpieczeństwa zasobów. Dotyczy to edukowania za pomocą szkoleń z dziedziny bezpieczeństwa informacji, których celem jest podniesienie świadomości

personelu. Odpowiedni poziom wiedzy może wpłynąć na zmniejszenie wystąpienia zagrożeń z winy pracowników oraz sposób przeciwdziałania im. Tylko świadomy pracownik jest w stanie odpowiednio skutecznie zareagować na ataki wyłudzenia informacji.

W rozważaniach dotyczących aspektu bezpieczeństwa osobowego należy pamiętać o bezpieczeństwie informacji firmy. Informacje dotyczące baz danych dostawców, klientów, patentów, metod rywalizacji, wiedzy o konkurencji są znane zatrudnionej kadrze. Zasoby ludzkie przepływające do konkurencji zabierają właśnie o wiedzę i mogą w znacznym stopniu przyczynić się do osłabienia sytuacji przedsiębiorstwa. Dlatego utrata doświadczonej kadry jest nieocenioną stratą i w znacznym stopniu może przyczynić się do osłabienia konkurencyjności firmy [11].

Istotną kwestią jest **bezpieczeństwo prawne**, które interpretuje się, jako zgodność z obowiązującym prawem w obszarze danego państwa. Ponadto zabezpieczenia muszą być dostosowane dla ochrony danych osobowych i informacji niejawnych w rozumieniu ustawy.

Do działań w sferze bezpieczeństwa prawnego w organizacji można zaliczyć, następujące: [12].

Bezpieczne składowanie dokumentacji medycznej pracowników, jeżeli jest to zgodne z prawem prowadzenia działalności.
Uruchomienie systemów ochrony danych osobowych klientów.
Audyt dotyczący zgodności funkcjonowania przedsiębiorstwa z obowiązującym prawem państwowym.
Edukowanie na szkoleniach mające na celu uświadomienie o stosowanych zasadach i procedurach w jednostce.
Używanie w przedsiębiorstwie wyłącznie licencjonowanych systemów i oprogramowania.

Podstawą funkcjonowania przedsiębiorstwa na rynku powinno być prowadzenie działalności zgodnie z wymaganiami prawnymi, minimalizuje się wówczas sankcje w postaci kar. Duża świadomość pracowników w przedsiębiorstwie jest równoznaczna z znacznie większą ochroną przedsiębiorstwa przed zagrożeniami, co wiąże się z kolei z doskonaleniem systemów wspomagających zarządzanie organizacją.

Bezpieczeństwo teleinformatyczne

Zgodnie z definicją J. Jańczaka i A. Nowaka oznacza „*poziom uzasadnionego zaufania i pewności, że potencjalne stany wynikające z przypadkowego czy świadomego ujawnienia, modyfikacji, zniszczenia czy ujawnienia przetwarzania danych przechowywanych lub przesyłanych za pomocą systemów teleinformatycznych nie zastaną poniesione*” [39]. Z tą też definicją utożsamia się K. Liderman, który uważa omawiany rodzaj bezpieczeństwa za możliwość przetwarzania informacji

przechowywanej w systemie teleinformatycznym w wyniku, czego przedsiębiorstwo nie poniesie strat [13].

Z kolei Ustawa z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną, wskazuje, że bezpieczeństwo teleinformatyczne „*to bezpieczeństwo systemu teleinformatycznego"* [14]

Pojęcie bezpieczeństwa teleinformatycznego stosuje się zamiennie z takimi określeniami jak: bezpieczeństwo danych, bezpieczeństwo komputerowe, bezpieczeństwo komunikacyjne, bezpieczeństwo sieciowe.

Na bezpieczeństwo teleinformatyczne składają się zagadnienia telekomunikacji z uwagi na formę komunikowania się z innymi, jak również elementy informatyki, które pomagają w przepływie informacji.

Ponieważ z założenia systemy informatyczne mają na celu gromadzenie, przetwarzanie oraz szybkie udostępnianie danych, to stanowią one źródło zainteresowania służb specjalnych lub też innych instytucji będących potencjalnym przeciwnikiem, np. organizacji o charakterze terrorystycznym oraz pojedynczych organizacji.

Reasumując można stwierdzić, że systemy informatyczne są bezpośrednio zagrożone ze strony każdego, kto ma większy zasób wiedzy, czy też umiejętności [15].

1.2. Rola i znaczenie informacji

Truizmem byłoby stwierdzenie, że bez wymiany informacji niemożliwe jest nie tylko istnienie życia społecznego czy też gospodarczego, lecz także funkcjonowanie nawet najbardziej prymitywnych form życia. Nic, więc dziwnego, że problematyka informacji wywołuje emocje u specjalistów z wielu dziedzin [16].

Informacja zawsze była i jest jedną z najcenniejszych wartości człowieka, instytucji, państwa, gospodarki czy całego społeczeństwa, mimo iż człowiek nie zawsze był tego świadomy. Osoby, które dysponowały informacją, we właściwym czasie potrafiły osiągnąć pokaźne sukcesy rynkowe. Od niepamiętnych czasów ludzkość w zdobywaniu informacji upatrywała skutecznego narzędzia do objęcia władzy. Tymczasem, zdobywanie informacji jest przejściem od traktowania jej, jako wiedzy do informacji powiązanej z działaniem lub powzięciem decyzji. Stąd też w naszym otoczeniu obserwuje się pewien rodzaj ambiwalencji. Z jednej strony informacje staramy się chronić, z drugiej zaś strony występują działania zakrojone na dużą skalę, związane z udostepnieniem jej szerokiemu gronu [17].

Bez wątpienia, więc najbardziej poszukiwanym zasobem w dzisiejszych czasach jest informacja. Wprowadzenie technologii informatycznych i komputerowych wpłynęły na wymianę jej pomiędzy oddalonymi od siebie przedsiębiorstwami i przestały się już liczyć logistyczne uwarunkowania. Technika umożliwiła gromadzenie, przechowywanie, przetwarzanie i przekazywanie informacji w wielu dotychczas nieosiągalnych płaszczyznach [17].

Obserwując zachowania inwestorów na giełdzie można zauważyć, że rynek nie reaguje na konkretne zdarzenie, lecz na informację o tych właśnie zdarzeniach np. informacja sprawia, że akcje podlegają różnym wahaniom.

Często słyszymy określenie „gospodarka oparta na wiedzy" czy podobne temu „zarządzanie wiedzą", wskazuje to jak wysoko cenimy informację, upatrując w niej klucz do sukcesu. Dotyczy to społeczeństw czy cywilizacji jak również przedsiębiorstw. Tak, więc informacja to mądrość, która jest potrzebna do sformułowania i spełnienie wymagań, co do zdobycia przez przedsiębiorstwo określonych zadań [17].

W oparciu o dostępne źródła literatury można znaleźć wiele definicji informacji. Niektóre z nich przedstawiają źródła [18,19, 20, 21].

Jednak niezależnie od tego, jaką formę przybiera lub za pomocą, jakich środków jest udostępniana czy też przechowywana zawsze powinna być w odpowiedni sposób chroniona.

W kontekście omawianego tematu pracy, roli, jaką odgrywa informacja w przedsiębiorstwie, została zdefiniowana przez T. Kifnera, jako *„element wiedzy, faktu, wiadomości, komunikatu lub wskazówką gromadzenia, komunikowania, i przekazywania komuś za pomocą jakiegoś kodu lub języka"* [22]. Ponadto autor podzielił informacje na trzy grupy: decydujące o istnieniu organizacji (dokumentację wewnętrzną, dane personalne pracowników, opis zdarzeń gospodarczych), decydujące o konkurencyjności na rynku (szczegóły o używanych technologiach) oraz związane z kontrolą dostępu do informacji (klucze kryptograficzne, karty magnetyczne, hasła do firmowych komputerów, hasła do poczty elektronicznej).

Na jakość informacji składają się różne cechy charakterystyczne tj. aktualność, zrozumiałość, dokładność, precyzyjność, pochodzenie z pewnego źródła. Dlatego też informacja powinna być klarowna, czytelna aktualna, zrozumiała, dokładna, precyzyjna. W literaturze przedmiotu można znaleźć stwierdzenie, że wartość informacji jest dodatnia wówczas, gdy jej otrzymanie zwiększa prawdopodobieństwo osiągnięcia celu, a ujemna, gdy prawdopodobieństwo osiągnięcia zamierzonego celu zmniejsza się po

otrzymaniu informacji- wówczas mówimy o dezinformacji. Polega ona na wysyłaniu komunikatów niezgodnych ze stanem faktycznym [23].

W dalszych rozważaniach warto zwrócić uwagę na definicję informacji używaną w socjotechnice. Informacja jest przekazywana o określonej treści przez nadawcę do odbiorcy za pośrednictwem środków przekazywania informacji. Może posiadać cechy rzeczywiste lub niezgodności. Służą one wywołaniu pożądanych przemian w postawach społecznych.

Informacja jest, więc czymś więcej niż wiadomością, znakiem czy formą komunikowania. Jest zarówno opisem rzeczywistości, jak i odzwierciedleniem stanu systemu oraz jej elementów, które mogą być przetwarzane, gromadzone czy też dystrybuowane.

Obecnie zauważa się różnicę między informacją, która była przekazywana kilka czy też kilkadziesiąt lat temu a tą, która jest przekazywana dzisiaj i polega na zwiększonym dostępie do różnych jej form tak, aby stała się potężną bronią [24].
Również w zarzadzaniu jednostkami gospodarczymi informacja odgrywa ważną rolę. Spełnia ona cel edukacyjny dostosowując wiedzę do stale zmieniającego się otoczenia zewnętrznego.

Umiejętność pozyskiwania informacji jest kluczowym elementem warunkującymi sukces w prowadzeniu biznesu i utrzymaniu poziomu konkurencyjności na rynku. Informacje stanowią o istocie i realizacji kluczowych funkcji w zarządzaniu przedsiębiorstwem. Mowa tutaj o planowaniu, organizowaniu, motywowaniu, czy kontroli.

Zatem informacja jest niematerialnym zasobem organizacji, choć jest zaliczana do aktywów biznesowych. Wartość i przydatność informacji można ocenić podsumowując decyzje zarządu i co za tym idzie efekty kadry zarządzającej. Posiadanie odpowiednich informacji skutkuje zazwyczaj podjęciem decyzji racjonalnych, podejmowanych w optymalnych warunkach. Decyzje zarządcze są równoznaczne z generowaniem zysków dla przedsiębiorstwa [25]. Szerzej temat informacji zarządczych i ich podział podejmuje Marek Strzoda w swojej publikacji [25].

W praktyce, podstawą funkcjonowania przedsiębiorstwa na rynku jest posiadanie odpowiednich, wiarygodnych informacji. Zależność tą, można zauważyć w rozwoju nowoczesnych technologii, która sprawia, że informacja stała się towarem, czyli wartością, która nie różni się od innych pod tym względem i podlega wycenie, posiada konkretną wartość rynkową. Jest to szczególny rodzaj towaru o znaczeniu

strategicznym dla istnienia całych państw, w tym i również dla przedsiębiorstw. Właściwy obieg informacji warunkuje wręcz poprawne funkcjonowanie jednostek [26].

Gwarantując stan bezpieczeństwa informacja winna być chroniona w aspektach: przechowywania informacji, dostępu do informacji, transmisji informacji, tak, aby dane były chronione przed ujawnieniem, modyfikacją czy też zniszczeniem. Poza tym ochrona odnosi się do zapewnienia poufności, integralności, dostępności, autentyczności, rozliczalności czy niezawodności zarówno w przedsiębiorstwie wewnątrz jak i na zewnątrz. W przeciwnym razie można stracić ważne informacje tj. niejawne czy dane osobowe, które z kolei powodują kary finansowe za nieprzestrzeganie wymogów prawnych lub też utratę wiarygodnego wizerunku zarówno w oczach potencjalnych kontrahentów, jak i stałych klientów.

Informacje, o których mowa w tym rozdziale, mogą być przechowywane w systemach informatycznych tzn. programach, aplikacjach, sprzęcie komputerowym tzn. nośniki danych, komputerach, i w archiwach oczywiście w formie papierowej. Alternatywą dla tradycyjnej formy jest przechowywanie danych w sposób elektroniczny (zdecydowanie trudniej taką informacje zmodyfikować a próby naniesienia zmian pozostaje trwale w systemie. Do dokumentacji w formie elektronicznej zaliczamy: pliki edytorów tekstu, pocztę elektroniczną, dokumenty dostępne w internecie.

Jednakże, niezależnie od stosowanych w przedsiębiorstwie form przechowywania informacji, zawsze znajduje się ona w umysłach pracowników i współpracowników. Jak donoszą naukowcy pamięć ludzka jest bardzo pojemna. Okazuje się, że możemy dobrze pamiętać informacje, do których mieliśmy dostęp przez ułamek sekundy, nawet po kilku latach. Dlatego też w kontekście ochrony informacji nie zaleca się, aby ujawniać informacje jednemu człowiekowi w całości, lecz je dzielić. Podział informacji jest szeroko stosowany np., gdy mówimy o kluczu kryptograficznym lub o hasłach [22].

Według badań przeprowadzonych w Stanach Zjednoczonych aż 70% spółek odnotowało przypadki ujawnienia poufnych informacji na zewnątrz organizacji. Amerykańskie Stowarzyszenie Certyfikowanych Ekspertów od Wykrywania Oszustw oszacowało, że gospodarka amerykańska wskutek dopuszczenia do utraty, modyfikacji, czy ujawnienia informacji traci rocznie 6% dochodu [16].

Organizacja chcąc mieć nieprzerwany dostęp do wiarygodnych informacji ponosi znaczne koszty, w wyniku, których otrzymuje informacje mające dla niej wartość. Istota funkcjonowania przedsiębiorstwa zakłada, że pozyskane informacje

umożliwią osiągnięcie większych dochodów, w stosunku do poniesionych nakładów. Jednak dokonanie takiej analizy nie jest łatwe i zazwyczaj wraz z wzrostem ilości informacji, wzrasta koszt ich uzyskania.

1.3. Elementy bezpieczeństwa informacji

Elementami, na których opiera się zarządzanie bezpieczeństwem informacji zgodnie z treściami zawartymi w normie PN-I-13335-1 będą: zasoby, zagrożenia, podatność, następstwo, ryzyko, zabezpieczenia, ryzyko szczątkowe. Nadrzędnym celem zarządzania jest proces minimalizowania ryzyka wystąpienia zagrożenia i wprowadzenia skutecznych zabezpieczeń.

- **Zasoby**

Prawidłowe zarządzanie zasobami jest niezbędnym czynnikiem w celu osiągnięcia odpowiedniego działania w obszarze jednostki i jest obowiązkiem kierownictwa instytucji na wszystkich poziomach.

Patrząc na bezpieczeństwo informacji do najważniejszych zasobów zaliczamy:

1. Oprogramowanie komputerowe
2. Informacje/dane- dokumenty, bazy danych
3. Zasoby fizyczne- sprzęt komputerowy, bazy danych
4. Ludzie-kadra zarządzająca i wykonawcza
5. Dobra niematerialne- obejmujące reputacje przedsiębiorstwa, wizerunek
6. Zdolność produkowania czy też świadczenia usług

Jak na to wskazuje norma PN-I-13335-1 większość lub prawie wszystkie zasoby uważane są za wartościowe na tyle, aby zagwarantować odpowiedni stopień ochrony, i poziom bezpieczeństwa informacji.

Niezbędne staje się, więc zidentyfikowanie zasobów przedsiębiorstwa i wymagań w zakresie ich ochrony. Jest to niezbędna czynność zapewniająca określenie wymaganego poziomu bezpieczeństwa oraz sformułowanie określonego poziomu ryzyka.

Przy identyfikacji zasobów należy również wziąć pod uwagę atrybuty zasobów takie jak: ich wartość, wrażliwość oraz podatność na określone zagrożenie.

Z perspektywy bezpieczeństwa i ochrony informacji należy pamiętać, że na zasoby i ich atrybuty wpływa środowisko zewnętrzne oraz jego otoczenie, w którym funkcjonuje organizacja.

- **Zagrożenia**

Podstawową determinantą pomocną w podjęciu rozważań identyfikacji, analizy i oceny zagrożeń jest poznanie znaczenia słowa zagrożenie.

W Wielkim słowniku poprawnej polszczyzny określa się zagrożenie, jako „*sytuację będącą sygnałem czegoś, co może nastąpić, zwykle złego, niepożądanego"* [27]. Z kolei zdaniem Lidwy W. „ *zagrożenie to zdarzenie powstające losowo lub wywołane losowo, i wywiera negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa, na warunkach bytowania ludności oraz stan środowiska naturalnego"* [28]. Zgadza się to z poglądami Ficona K., który uważa, że zagrożenie *to „zdarzenie spowodowane losowo z przyczyn naturalnych lub celowo z przyczyn nielosowych, które wywierają negatywny wpływ na funkcjonowanie całego systemu lub powodują niekorzystne, niebezpieczne zmiany w otoczeniu wewnętrznym i zewnętrznym"* [29].

Kaczmarek T.T. z kolei w swojej definicji prezentuje pogląd, *że „zagrożenie należy rozumieć, jako potencjalne negatywne zdarzenie, które pochodzi z zewnątrz i które może spowodować szkody w systemie"* [30]. Do podstawowych zagrożeń należą wg Kaczmarka T. utrata zaufania, integralności systemu, ograniczenie swobody dysponowania i autentyczności oraz utrata zdolności wykonywania zobowiązań.

Natomiast norma PN-ISO 31000: 2018-08 wskazuje, że zagrożenie winno być uszczegółowione przez podanie jego pochodzenia np. zagrożenie mechaniczne, albo powinna być podana potencjalna szkoda np. ujawnienie poufnych danych [31].
Z analizy treści dostępnych publikacji wynika, iż zagrożenie odnosi się do potencjalnej przyczyny niepożądanego incydentu, który na pewno wyrządzi szkodę w systemie lub instytucji.

Można wyciągnąć wniosek, iż zagrożenie wymaga podejmowania działań z uwagi na jego negatywny wpływ destabilizujący równowagę poziomu bezpieczeństwa. Należy zaznaczyć, że nie podjęcie działań naprawczych może spowodować powstanie łańcuchowo następnych zagrożeń, które kolejno naruszają poczucie bezpieczeństwa [32].

W rezultacie prowadzenie działalności gospodarczej zawsze obarczone jest określonym ryzykiem i z całą pewnością im szybciej będzie się rozwijał podmiot, tym skala i rozmiary ryzyka będą wzrastały. W skondensowanej postaci pojawia się, jako

zagrożenie w różnej formie np. wewnętrznej (awarii sprzętu komputerowego) czy też w formie zewnętrznej (użycie sił zbrojnych przez państwa ościenne).

Nowe możliwości prowadzenia działalności gospodarczej, zawieranie umów na odległość, spowodował prowadzenie działalności w oparciu o technologię teleinformatyczną, która rzecz jasna niesie ze sobą oczywisty zysk, ale i równie wysoki poziom zagrożeń [10].

Najczęściej spotykanym zagrożeniem jest utrata informacji, w wyniku, czego może zostać ona ujawniona, zmodyfikowana, uszkodzona, zniekształcona, itp. Ataki stanowią realne zagrożenie dla funkcjonowania firmy, obciążając systemy informatyczne tak, iż dokonywanie transakcji jest uniemożliwione lub co gorsze doprowadzenie do całkowitego zatrzymania systemów i braku odstępności.
Szczegółowe informacje dotyczące zagrożeń bezpieczeństwa informacji zostaną przedstawione w podrozdziale 1.4.

- **Podatność**

Autor książki „Jak chronić informacje", podaje, że podatność jest *„związana z zasobami, i oznacza pewną słabość fizyczną, organizacyjną proceduralną, osobową, zarządzania, administracji, sprzętu komputerowego, oprogramowania i informacji"*[33]. Podatność może wykorzystać zagrożenie i konsekwencji spowodować szkodę. Aby uniknąć takich sytuacji zaleca się przeprowadzenie analizy podatności, która pokaże słabość systemu.

Natomiast norma PN-EN ISO/IEC 27000: 2017 definiuje podatność, jako *"wady i luki w strukturze fizycznej organizacji, procedurach zarządzania, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone lub niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika"* [23].

Tak, więc istnienie tego rodzaju wad i luk w w/w. strukturach może być użyte do spowodowania szkód dla realizacji procesu informacyjnego lub też bezpośrednio dla samej instytucji. Samo istnienie podatności nie wywoła szkody, lecz korespondując już choćby z jednym lub wieloma zagrożeniami stanowi bardzo realne niebezpieczeństwo wystąpienia incydentu i stwarza pewną okazję do ich wyrządzania [34,21,22].

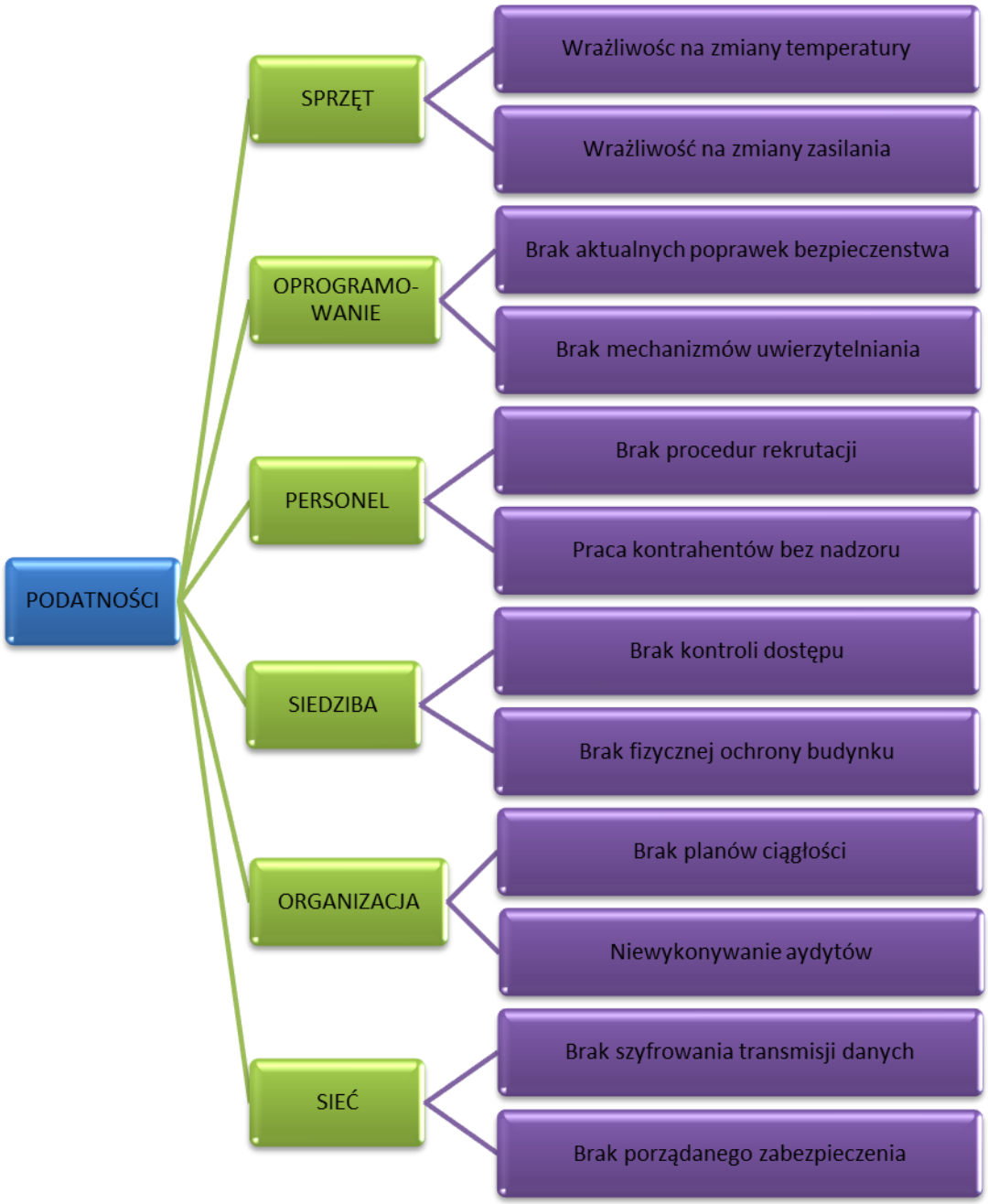
Norma PN-I-13335-1 wskazuje, że należy rozważyć podatności pochodzące z różnych źródeł, na przykład wewnętrzne względem zasobu. Podatność może istnieć dopóty, dopóki same zasoby nie zmieniają się tak, że podatność nie będzie się do nich odnosić [35]. Stanowią one okazję, która może pozwolić zagrożeniu wyrządzić szkodę.

Podatności, czyli słabości, mogą mieć następujący charakter:

- Dotyczący informacji np.: brak kontroli dostępu, brak kryptograficznej ochrony informacji,
- Dotyczący oprogramowania np.: źle skonfigurowany lub też niewłaściwie dobrany system operacyjny,
- Związany z administracją np.: dostęp administratorów systemu do jakiejkolwiek poczty zarządu,
- Fizyczny np.: skutki zalania serwerowni podczas powodzi,
- Proceduralny np.: brak regulaminu odnośnie stosowania haseł, brak regulaminu dostępu do określonych dokumentów
- Organizacyjny np.: dopuszczenie osób obcych do poufnych informacji przetrzymywanych na dyskach,
- Personalny np.: niewystarczająca wiedza, brak odpowiednio przeszkolonych pracowników do określonych działań
- Związany ze sprzętem komputerowym np.: brak wystarczającego obszaru na dysku lub pamięci operacyjnej, nielegalne połączenie modemowe z Internetem poza zabezpieczeniami systemu teleinformatycznego instytucji.

W instytucji nie wszystkie podatności podlegają zagrożeniom. Ważne są te, z którymi związane są realne zagrożenia. Z uwagi na to, iż wszystko, co nas otacza podlega zmianie to prawdziwe będzie również stwierdzenie, że zagrożenia i środowisko też się zmieniają. Dlatego też niezwykle ważną sprawą staje się monitorowanie podatności aktualnie występujących, ale i też branie pod uwagę dynamicznie powstających nowych zagrożeń.

Z urzeczywistnieniem zagrożeń ściśle powiązane są podatności, odnoszące się do poszczególnych zasobów. Zagrożenia wpływają negatywnie na zasoby, które charakteryzują się podatnością.



Rysunek 2. Przykładowe podatności zgodne z normą PN-ISO/IEC 27005:2014-01
Źródło: Opracowanie na podstawie [34].

- **Następstwo**

Następstwo można określić, jako konsekwencje niepożądanego incydentu, który może być spowodowany rozmyślnie lub też przypadkowo, i znacząco wpłynąć na zasoby. Nie bez znaczenia jest fakt, że konsekwencją następstwa może być utrata poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności chronionej informacji. Dalszymi skutkami takiej sytuacji może być zniszczenie

pewnych zasobów, części lub też całości systemu informatycznego oraz straty finansowe, utrata udziału w rynku lub też pozytywnego wizerunku firmy [33, 34, 35].
Określając wielkość następstw mamy do czynienia z kontrolą nad utrzymaniem równowagi pomiędzy skutkami niechcianego incydentu, a kosztami zastosowanych do ochrony zabezpieczeń.

- **Ryzyko**

Ustawa z 15 marca 2019 roku o ochronie informacji niejawnych definiuje ryzyko, jako: *„kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji* [36].
W podobnym kontekście, wyraża się również K. Ficoń, który określa ryzyko, jako oszacowanie prawdopodobieństwa wystąpienia określonego rodzaju zagrożenia lub straty, a także zysku i korzyści [29].
Również Wielki słownik wyrazów obcych podaje definicję ryzyka, jako *„możliwość, prawdopodobieństwo, że coś się nie uda, że sprawy przybiorą zły obrót”* [37].

Natomiast jak podaje norma PN-I-13335-1, scenariusz ryzyka opisuje, w jaki sposób dane zagrożenie lub grupa zagrożeń może wykorzystać konkretną podatność lub grupę podatności, narażając zasoby na szkodę [38].

Z uwagi na to, że ryzyko nie jest pojęciem jednoznacznym(jego istota wskazuje na szeroki zakres znaczenia słowa), istnieje wiele definicji znaczeniowych. Autorka pracy przytoczyła zaledwie kilka z nich. W niniejszym opracowaniu rozważania nad problematyką ryzyka rozpoczęto od konceptualizacji pojęcia ryzyka.

Literatura przedmiotu wskazuje, iż ryzyko jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty lub zniszczenia zasobu lub też grupy zasobów. Taka sytuacja w znaczymy stopniu odbije się negatywnie na każdej jednostce gospodarczej. Na gruncie nauki ryzyko właściwe określone jest przez dwa czynniki tj. prawdopodobieństwo wystąpienia zdarzenia oraz jego skutek, który może zostać wywołany tym zdarzeniem. Już dowolna zmiana w zasobach, zagrożeniach, podatnościach oraz zabezpieczeniach może mieć bezpośrednio wpływ na ryzyko. Zatem, ryzyko nie stanowi zagrożenia, ale określa, że może się ono wydarzyć. Natomiast rozpoznanie i określenie pojedynczego ryzyka oraz całkowitego ryzyka znacząco pomoże redukować i wyeliminować negatywne oddziaływanie na gospodarkę przedsiębiorstwa [34].

Szerzej interpretacja pojęcia ryzyka została omówiona w publikacjach [39] [24].

- **Zabezpieczenia**

Z uwagi na to, że zasoby podlegają wielu zagrożeniom zasadne jest poznanie znaczenia pojęcia zabezpieczenia.

Otóż zgodnie z treściami zawartymi w normie PN-EN ISO/IEC 27000: 2020-07 zabezpieczenie to „ *środek służący zarządzaniu ryzykiem, włączając polityki, procedury, zalecenia, praktyki lub struktury organizacyjne, które mogą mieć naturę administracyjną, techniczną lub też zarządczą lub prawną"* [23].
Z kolei Wielki Słownik Wyrazów Obcych definiuje zabezpieczenia, które „*zapewniają ochronę przed czymś niebezpiecznym lub szkodliwym, zapewniając utrzymanie się czegoś w dotychczasowym stanie"* [37].

Dokonując dalszej interpretacji pojęcia zabezpieczenia warto odnieść się do definicji prezentowanej przez normę PN-I-13335-1: 1999 która mówi o tym, że *„to praktyka, procedura lub mechanizm redukujący ryzyko"* [35].

Zatem zgodnie z normą można podzielić zabezpieczenia na następujące:

1. Zabezpieczenia administracyjne: administrowanie uprawnień do zasobów i systemów teleinformatycznych (wiąże się to ściśle z nadawaniem uprawnień, zmianą ich lub też dobieraniem ich w razie potrzeby).
2. Zabezpieczenia techniczne: wprowadzenie systemu kontroli dostępu do wybranych pomieszczeń.
3. Zabezpieczenia o naturze zarządczej: koordynacja bezpieczeństwa informacji przez Pełnomocnika ds. SZBI, podpisywanie przez pracowników przedsiębiorstwa umów o zachowaniu poufności.
4. Zabezpieczenia o naturze prawnej: wynikają one zazwyczaj z ustanowionych regulacji prawnych np. z Rozporządzenia RODO i krajowych przepisów [23].

Literatura przedmiotu wskazuje na praktyki, procedury i mechanizmy, które mogą chronić przed zagrożeniem, redukując tym samym podatność, a ograniczając następstwa oraz wykrywając niepożądane incydenty. Aby zabezpieczenia były efektywne i poprawnie dobrane wymagają kombinacji różnych rozwiązań w celu utworzenia warstw ochronnych dla chronionych zasobów. Na przykład mechanizmy kontroli dostępu stosowane dla komputerów powinny być wspomagane przez narzędzia audytu, procedury postępowania dla personelu, szkolenia czy zabezpieczenia fizyczne.

Można, zatem stwierdzić, że dzięki dobraniu odpowiednich zabezpieczeń należycie można wdrożyć politykę bezpieczeństwa informacji. Dzięki temu z kolei można właściwie redukować ryzyko. Przy tej okazji stosownym będzie wskazanie, iż wprowadzenie zabezpieczeń nie wyeliminuje ryzyka, jedynie, co jest istotne pozwoli zdecydowanie obniżyć jego poziom.

Wiele zabezpieczeń może służyć różnym funkcjom, dlatego też korzystny wybór zabezpieczeń to taki, który będzie spełniał wiele funkcji.

Podstawowe zastosowanie zabezpieczeń prezentuje się następująco:

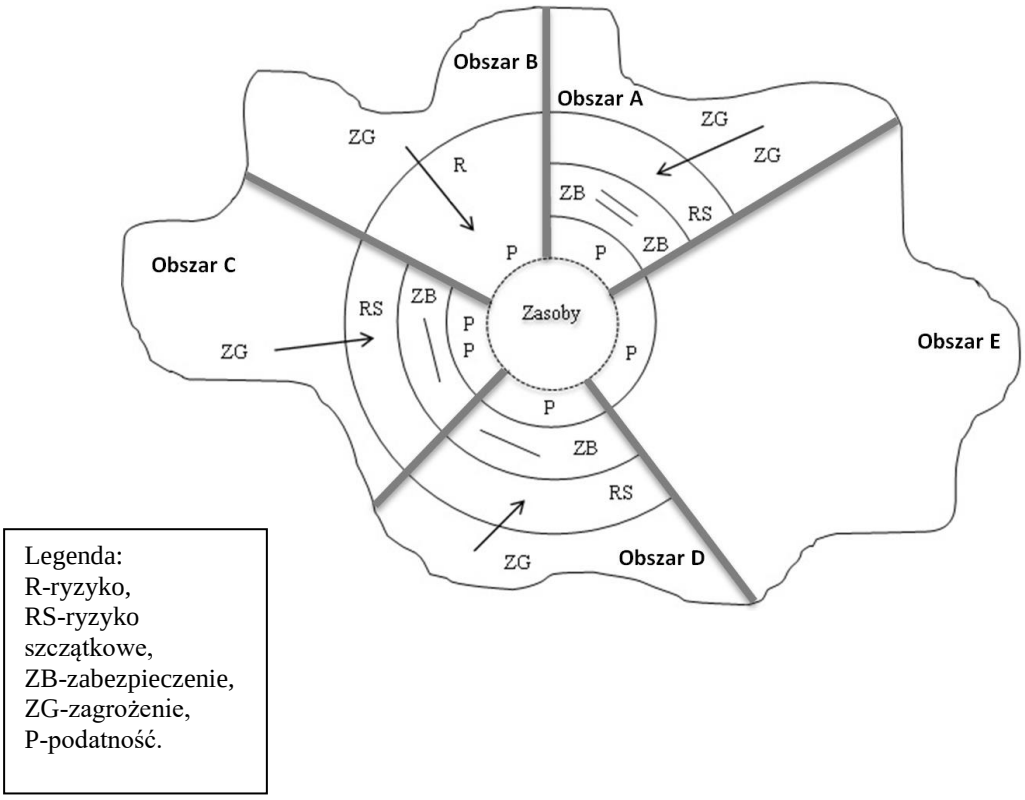
- ochrona przed zagrożeniami;
- redukcja podatności;
- odtwarzanie zasobów po incydentach;
- wykrywanie niepożądanych zagrożeń;
- ograniczenie następstw [40].

W tym aspekcie należy mieć na uwadze zarówno efektywność, jak i ograniczenia przedsiębiorstwa w obszarze organizacyjnym, finansowym, prawnym, czy technicznym. Na uwagę zasługuje fakt, że zabezpieczenia mają przeznaczenie, jako: zapora sieciowa, narzędzia do monitoringu, analizy sieci, kryptografia, podpisy cyfrowe, oprogramowanie antywirusowe, polityka tworzenia kopii bezpieczeństwa, zasilanie rezerwowe, mechanizmy kontroli dostępu oraz tworzenie wysokiej świadomości w obszarze bezpieczeństwa informacji wśród etatowców w jednostce gospodarczej [34]. Jednak warto o taką ochroną zabiegać, gdyż odpowiednio dobrane zabezpieczenia to wielki sukces dla firmy.

- **Ryzyko szczątkowe**

Ryzyko można zredukować jedynie częściowo poprzez zastosowanie zabezpieczeń. Jednak zawsze pozostaje ryzyko szczątkowe, które należy zaakceptować. Wskazuje na to norma cyt. *„elementem podejmowania decyzji o adekwatności zabezpieczeń do potrzeb instytucji jest akceptacja ryzyka szczątkowego”* [44]. Zarządzający przedsiębiorstwem powinni być w posiadaniu wiedzy o istnieniu ryzyka szczątkowego w kontekście następstw oraz prawdopodobieństwie zajścia określonego zdarzenia wywołanego zagrożeniem. Poza tym kierujący przedsiębiorstwem powinni liczyć się z konsekwencjami ewentualnych skutków incydentu.

Relacje pomiędzy poszczególnymi składowymi bezpieczeństwa informacji przedstawiono w sposób graficzny na rysunku 3.



Rysunek 3. Zależności pomiędzy elementami bezpieczeństwa wg. normy PN-I-13335-1:1999

Źródło [35] [9]

Rysunek 3. przedstawia, w jaki sposób zasoby, są narażone na różnego rodzaju zagrożenia. Katalog zagrożeń ulega ciągłym zmianom w czasie i jest systematyczne poszerzany o coraz to nowo powstające zagrożenia [35].

Zaprezentowany rysunek wskazuje na środowisko, zasoby instytucji, podatności tych zasobów, określone zabezpieczenia wybrane dla ochrony zasobów i redukcję konsekwencji utraty zasobów, oraz ryzyko szczątkowe, akceptowane przez organizację.

Biorąc pod uwagę wybrane zabezpieczenia można powiedzieć, że niektóre z nich mogą być bardziej skuteczne, niż inne i redukcja ryzyka związanego z wieloma zagrożeniami i podatnościami będzie mniejsza. Na rysunku w obszarze A zwielokrotniono zabezpieczenia w wyniku, czego zmniejszyła się podatność na zagrożenie i zredukowano ryzyko szczątkowe do poziomu akceptowalnego. w aspekcie akceptacji ryzyka w wybranych sytuacjach nie wdraża się zabezpieczeń, mimo iż obecne są zagrożenia (obszar B). Z kolei w innych sytuacjach gdzie widać podatności nie zauważa się znanych zagrożeń, które te podatności mogłyby wykorzystać (obszar E). Warto zaznaczyć, że zaleca się pełną kontrolę poprzez monitorowanie środowiska zabezpieczeń, które z całą pewnością zapewnią ochronę przed zagrożeniami, i mogą wykorzystać podatności (obszar C,D) [14].

Konkludując, osoby, które przetwarzają, przechowują i tworzą informacje zobowiązane są do znajomości istoty zasobu, podatności, zagrożenia, następstwa oraz zabezpieczenia. Bowiem dość często jesteśmy świadkami poglądów, iż wystarczy zabezpieczyć system poprzez zainstalowanie zapory ogniowej, czy też udoskonalenie metody uwierzytelniania i to powinno wystarczyć.

Jednak obserwując kłopoty i ciągłe problemy w przedsiębiorstwach związane z zachowaniem bezpieczeństwa ochrony informacji, należy być świadomym, że żadne z tych zabezpieczeń nie stanowi całościowego rozwiązania problemu poprawy bezpieczeństwa w organizacjach.

1.4. Identyfikacja zagrożeń bezpieczeństwa informacji przedsiębiorstwa

W świecie, w którym informacja jest nadrzędną wartością przedsiębiorstwa szczególnego znaczenia nabiera problem zagrożeń bezpieczeństwa informacji.

Modernizując procesy produkcyjno-finansowe, księgowe, kadrowe, szybką komunikację międzynarodową umożliwiającą podpisywanie umów na odległość można dojść do wniosku, że korzyści wynikające z funkcjonowania teleinformatyki znacznie przeważają nad powstałymi zagrożeniami. Jednak mimo wszystko rozwój sieci komputerowych, nowe technologie, zarządzanie sieciami, czy korzystanie z sieci publicznych takie jak Reuters czy Internet, niosą ze sobą niezliczoną liczbę zagrożeń [41].

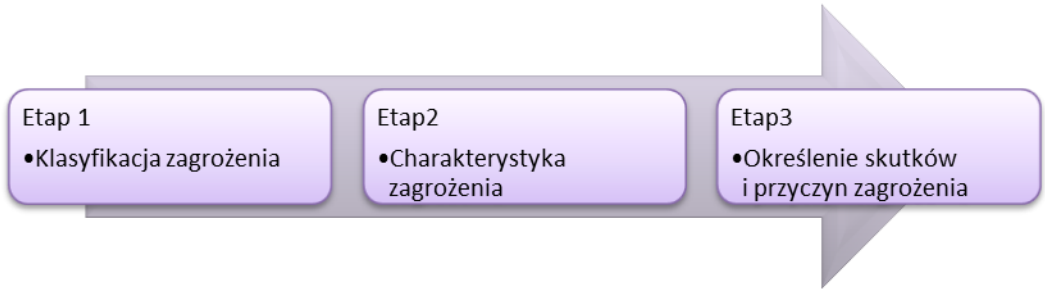
Uzupełnieniem powyższych rozważań będzie przedstawienie roli człowieka, jako źródła powodującego zagrożenia. Okazuje się, bowiem że człowiek jest w stanie dzięki antycypacji poradzić sobie z zagrożeniami, oprócz tych naturalnych. Istotnie może on wpływać na zagrożenie i znacznie wcześniej przewidzieć wystąpienie określonego zagrożenia. Jest to możliwe dzięki znajomości taksonomii zagrożeń, progresu technicznego, czy też technologicznego oraz zasobów informacyjnych, dzięki którym zdobywa się świadomość odnośnie nadchodzących zdarzeń. Aby przedstawić taką prognozę nieodzowne jest wcześniejsze zgromadzenie danych, aby później przewidzieć skutki i przyczyny zagrożeń lub też złagodzić następstwa zaistniałych zdarzeń. Postępowanie takie jest możliwe poprzez zidentyfikowanie zagrożeń, dzięki którym można dowiedzieć się jak zakwalifikować dane zagrożenie, do jakiego typu i grupy według dostępnych kryteriów. Później warto skorzystać z opisu zagrożenia

z uwzględnieniem przyczyn powstania i skutków następstw jego wystąpienia. Tak rozumiane zagrożenie poddaje się odpowiedniej analizie i ocenie ryzyka.

Współczesna jednostka gospodarcza obfituje w różnorodną liczbę zagrożeń o szerokim prawdopodobieństwie wystąpienia i co jest z tym związane trudne do przewidzenia i określenia przypuszczalnych skutków. W rezultacie żadna działalność jednostki gospodarczej nie może być realizowana w pełni bezpiecznie wolna, od ryzyka szczątkowego.

Liczba zagrożeń dla bezpieczeństwa danych wzrasta proporcjonalnie do rozwoju technologii informacyjno–komunikacyjnej i upowszechniania rozmaitych rozwiązań informatycznych wykorzystywanych w przedsiębiorstwach. Zagrożenia dla bezpieczeństwa danych tworzą zjawiska i czynności powodujące stratę w zasobach informacyjnych danego obiektu gospodarczego.

Etapy identyfikacji zagrożeń przedstawia w następujący sposób rysunek 4.



Rysunek 4. Stopniowa identyfikacja zagrożeń
Opracowanie własne na podstawie [42].

Wobec powyższego, zapewnienie odpowiedniego poziomu ochrony związane jest z identyfikacją i klasyfikacją zagrożeń. Zapoznanie się z tymi informacjami daje wiedzę gwarantującą odpowiednie postępowanie podczas doboru odpowiednich środków naprawczych i określenia zasad bezpieczeństwa. Ponadto, należy dodać, że aby podjąć się starań na rzecz kierowania poziomem bezpieczeństwa danego obszaru nieodłączna jest znajomość metod klasyfikowania zagrożeń oraz poznania ich taksonomii. Umożliwi to określenie potencjalnych przyczyn i skutków zaistniałego zagrożenia. Analiza literatury przedmiotu wskazuje na system klasyfikacji zagrożeń uwzględniając poniższe warunki.

Tabela 2. Wymagania klasyfikacji zagrożeń

Użyteczność	**Oczekuje się żeby klasyfikacja wnosiła do systemu bezpieczeństwa określoną wartość**
Wyłączność	Zagrożenie winno być zakwalifikowane do jednej grupy
Powtarzalność	Proces klasyfikacji powinien być porównywalny, bez względu na to, kto go będzie

Użyteczność	**Oczekuje się żeby klasyfikacja wnosiła do systemu bezpieczeństwa określoną wartość**
	dokonywał
Akceptowalność	Procedury klasyfikacji powinny być czytelne i proste tak, aby proces był ogólnie rozumiany
Jednoznaczność	Kryteria klasyfikacji winny być jasne, czytelne i oczywiste dla wszystkich identyfikujących zagrożenie, tak, aby osoba dokonująca klasyfikacji nie miała wątpliwości, co do sposobu zaklasyfikowania zagrożenia
Kompletność	Klasyfikacja obejmująca szeroki zakres wszystkich zagrożeń

Źródło [43].

Literatura przedmiotu wyróżnia wiele systemów podziału zagrożeń. Można je podzielić w następujący sposób:

1. cywilizacyjne, naturalne,
2. wewnętrzne, zewnętrzne,
3. techniczne, i inne,
4. pierwotne, wtórne,
5. przedmiotowe, podmiotowe,
6. militarne i niemilitarne

Warto zaznaczyć, że przedstawiony system klasyfikacji zagrożeń jest jednym z wielu możliwych podziałów. Wnikając głębiej w temat zagrożeń bezpieczeństwa informacji możemy dokonać szerszego podziału zaprezentowanego w normie PN-ISO/IEC 27005:2014-01. Zagrożenia mogą być rozmyślne, przypadkowe lub środowiskowe. Jednakże wszystkie one mogą skutkować uszkodzeniem bądź utratą informacji. Tabela 3. prezentuje rodzaj oraz źródło pochodzenia zagrożeń.

Tabela 3. Typowe grupy zagrożeń

RODZAJ	*ZAGROŻENIA*	*ŹRÓDŁO*
Zniszczenia fizyczne	pył, korozja, wychłodzenie, zniszczenie	przypadkowe, umyślne, naturalne
	pożar	umyślne, naturalne, przypadkowe
	poważny wypadek	umyślne, naturalne, przypadkowe
	zniszczenie urządzeń lub nośników	umyślne, naturalne, przypadkowe
Naruszenie bezpieczeństwa informacji	manipulowanie urządzeniem	umyślne
	szpiegostwo zdalne	umyślne
	kradzież urządzenia	umyślne
	Ujawnienie, podsłuch	umyślne, przypadkowe
	przechwycenie sygnałów na skutek zjawiska interferencji	umyślne
	kradzież nośników lub dokumentów	umyślne
	dane z niewiarygodnych źródeł	umyślne, przypadkowe
	sfałszowanie oprogramowania	umyślne, przypadkowe
	detekcja umiejscowienia	umyślne
	odtworzenie z powtórnie wykorzystanych i wyrzuconych nośników	umyślne
	promieniowanie elektromagnetyczne	przypadkowe, naturalne, umyślne

RODZAJ	*ZAGROŻENIA*	*ŹRÓDŁO*
	(cieplne, elektromagnetyczne)	
Utrata podstawowych usług	awaria urządzeń telekomunikacyjnych	umyślne przypadkowe
	utrata dostawy prądu	przypadkowe, naturalne, umyślne
	awaria systemu klimatyzacji i dostawy wody	umyślne, przypadkowe
Awarie techniczne	niewłaściwe funkcjonowanie oprogramowania	przypadkowe
	przeciążenie systemu informacyjnego	umyślne, przypadkowe
	naruszenie zdolności utrzymania systemu informacyjnego	umyślne, przypadkowe
	niewłaściwe używanie urządzeń	przypadkowe
	awaria urządzeń	przypadkowe
Nieautoryzowane działania	zniekształcenie danych	umyślne
	nielegalne przekształcanie danych	umyślne
	nielegalne przetwarzanie danych	umyślne
	używanie fałszywego lub skopiowanego oprogramowania	umyślne, przypadkowe
	nieautoryzowane używanie urządzeń	umyślne
Naruszenia bezpieczeństwa funkcji	naruszenie dostępności personelu	przypadkowe, naturalne, umyślne
	odmowa działania	umyślne
	naruszenie praw	umyślne, przypadkowe
	fałszowanie praw	umyślne
	błąd użytkowania	przypadkowe
Zjawiska naturalne	zjawiska klimatyczne	naturalne
	powódź	naturalne
	zjawiska pogodowe	naturalne
	zjawiska wulkaniczne	naturalne
	zjawiska sejsmiczne	naturalne

Źródło [44]

W tabeli 4. przedstawiono podział zagrożeń w oparciu o źródło pochodzenia.

Tabela 4. Podział zagrożeń w oparciu o źródło pochodzenia

NATURALNE	**LUDZKIE**	
	PRZYPADKOWE DZIAŁANIA	**CELOWE UMYŚLNE DZIAŁANIA**
Wyładowania atmosferyczne	Nieprawidłowe użycie	Złośliwe kody
Powódź	Skanowanie pliku	Kradzież
Trzęsienie ziemi	Wypadki fizyczne	Włamania do systemu
Pożar	Pomyłki	Celowa modyfikacja informacji

Źródło: Opracowanie na podstawie [35]*[14]*.

W związku ze zwróceniem szczególnej uwagi na zagrożenia spowodowane błędem ludzkim zdefiniowano kolejną grupę zagrożeń. Zestawiono je w tabeli nr.5

Tabela 5. Zagrożenia osobowe

ŹRÓDŁA ZAGROŻEŃ	MOTYWACJA	MOŻLIWE NASTĘPSTWA
PRZESTĘPCA KOMPUTEROWY	Nielegalne ujawnienie informacji Zniszczenie informacji Korzyść finansowa Nieautoryzowana zmiana danych	Przestępstwo komputerowe (cybernetyczne prześladowanie-cyberstalking) Wtargnięcie do systemu. Atak sieciowy polegający na fałszowaniu adresu źródłowego (spoofing). Przekupstwo informacyjne. Czyn przestępczy (powtórne podszycie się i przechwycenie informacji)
TERRORYSTA	Szantaż Zniszczenie Wykorzystanie Korzyść polityczna Rozgłos medialny	Bomba Wojna informacyjna Ataki na system, rozproszona odmowa usługi. Naruszenie bezpieczeństwa systemu
HACKER, CRACKER	Pieniądze Wyzwanie Status Ego	Haking Inżynieria społeczna Wtargnięcie do systemu Nieautoryzowany dostęp do systemu
SZPIEDZY PRZEMYSŁOWI	Szpiegostwo gospodarcze Przewaga konkurencyjna	Penetracja systemu Naruszenie prywatności Kradzież informacji Wykorzystanie informacji Nieautoryzowany dostęp do systemu (dostęp innych osób do informacji klasyfikowanej wewnętrznej lub związaną z technologią produktu)
OSOBY z WNĘTRZA PRZEDSIĘBIORSTWA	Niezamierzone błędy lub pomyłki (błąd programisty, błąd wprowadzania danych) Wywiad Zemsta Ciekawość Ego	Błędy w systemie Wtargnięcie do systemu Sabotaż systemu Nieautoryzowany dostęp do systemu Złośliwy kod-wirus, bomba logiczna, koń trojański Przechwycenie Wprowadzenie fałszywych, zniekształconych danych Przekupstwo informacyjne Oszustwo i kradzież Nadużycie komputerowe Przeszukiwanie informacji stanowiącej czyjąś własność Szantaż Napaść na pracownika

Źródło: Opracowanie na podstawie [44].

Zaistnienie zagrożeń bezpieczeństwa informacji wywołuje kolejny podział.

Tabela 6. Rodzaje zagrożeń bezpieczeństwa informacji

KATEGORIA ZAGROŻENIA	PRZYKŁADY ZAGROŻEŃ
Technologiczne starzenie się	Korzystanie z przestarzałych technologii
Naruszenie własności intelektualnej	Piractwo, naruszenie praw autorskich
Zamierzone działanie o charakterze szpiegowskim	Nieautoryzowany dostęp i gromadzenie danych
Siły natury	Pożar, powódź, trzęsienia ziemi, błyskawice, wyładowania atmosferyczne

KATEGORIA ZAGROŻENIA	PRZYKŁADY ZAGROŻEŃ
Zamierzone ataki na oprogramowanie	Wirusy, robaki, makra, odmowa wykonania usługi
Odchylenie, w jakości usług	ISP, zasilanie lub usługi WAN od dostawców usług
Błędy i pomyłki ludzkie	Wypadki, błędy pracowników
Kradzież	Nielegalne skonfiskowanie sprzętu jak również informacji
Zamierzone działania w kierunku sabotażu lub wandalizmu	Zniszczenie systemów bądź informacji
Techniczne błędy	Awarie sprzętu
Techniczne błędy i awarie oprogramowania	Pluskwy, nieznane luki, problemy z kodowaniem
Zamierzone działania w celu wyłudzenia informacji	Szantaż, ujawnianie informacji
Awarie infrastruktury usługowej (zasilanie, klimatyzacja, woda, ogrzewanie)	Utrata możliwości przetwarzania danych. Możliwe zniszczenie danych. Zniszczenie sprzętu komputerowego, urządzeń sieciowych czy łączy. Zniszczenie infrastruktury usługowej.

Źródło: Opracowanie na podstawie [17].

W nawiązaniu do tematu pracy ważnym elementem są skutki wykorzystania podatności na zagrożenie.

Tabela 7. Skutki zagrożeń bezpieczeństwa informacji

Rodzaj zagrożenia	**Skutki/Straty**
Podszywanie się pod inną osobę	Przejęcie danych o umowach związanych z klientami Utrata przewagi konkurencyjności na rynku
Włamanie do systemu komputerowego	Udana próba zemsty zwolnionego pracownika, który umieszcza bombą logiczną lub wirusa uaktywnioną po określonym czasie. Straty finansowe, unieruchomienie systemu
Podejrzenie informacji	Satysfakcja firm konkurencyjnych, które są w posiadaniu ważnych informacji badanego przedsiębiorstwa. Brak konkurencyjności.
Awaria zasilania	W wyniku braku prądu, przestoje a w następnej kolejności straty finansowe Brak wymiany informacji
Oszustwa komputerowe	Wyciek kluczowych informacji z przedsiębiorstwa Restrykcje prawne i finansowe. Kompromitacja przedsiębiorstwa.
Fałszerstwo komputerowe	Problemy z poprawnym zapisem informacji.
Niszczenie danych lub programów komputerowych	Utrata reputacji i wiarygodności dobrego imienia firmy. Brak wiarygodności w oczach klientów. Zacofanie technologiczne względem konkurencji. Utrata lub zniszczenie sprzętu komputerowego.
Utrata poufności danych	Skutkiem utraty danych jest ujawnienie nieupoważnionym osobom określonych informacji, co zazwyczaj jest związane z wyciekiem do konkurencji
Utrata integralności	W wyniku utraty integralności, wirusy komputerowe zmieniają, niszczą również i inne programy oraz ich dane. Utrata danych informacji
Utrata dyspozycyjności systemu	Dyspozycyjność systemu zostaje zniszczona przez robaki internetowe, które uniemożliwiają prawidłowe funkcjonowanie komputerów.
Utrata autentyczności	Utrata autentyczności najczęściej prowadzi do utraty integralności. Podejmowanie decyzji w oparciu o nieprawdziwe informacje będzie miało odzwierciedlenie w zakłóceniu realizacji procesów.

Rodzaj zagrożenia	Skutki/Straty
Podsłuchanie i przechwycenie danych	Niepowołana osoba zapoznaje się z przesyłanym informacjami. Pozyskane dane zostają ujawnione. Straty finansowe, utrata konkurencyjności.
Sabotaż komputerowy	Przestępcy zostają niezauważeni, co umożliwia całkowity nadzór nad sprzętem i możliwość ataku w dowolnym momencie. Straty finansowe.
Szpiegostwo gospodarcze	Włamywacz posiada dostęp do wszystkich informacji, kradzież danych, straty finansowe, utrata badań nad technologią, utrata konkurencyjności na rynku.
Ataki na systemy komputerowe	Poniesienie kosztów ataku komputerowego. Unieruchomienie pracy systemu komputerowego. Sankcje wynikające z RODO. Uzyskanie rozgłosu wśród towarzystwa hackerskiego.
Awaria sprzętu komputerowego	Dezorganizacja, ograniczony dostęp do danych lub w ogóle jego brak. Zakłócenia realizacji procesów Zakłócenia komunikacji w przedsiębiorstwie.
Kradzież sprzętu, dokumentów firmowych	Utrata technologii, dzięki której przedsiębiorstwo dominuje na rynku. Pośrednie straty finansowe np.: koszty sądowe Przerwa w funkcjonowaniu przedsiębiorstwa, przestój. Wyciek informacji do konkurencji.

Źródło: Opracowanie na podstawie [45][16].

Aby odpowiednio usystematyzować powstałe zagrożenia wymaga się rozróżniania w nich takich cech jak:

1. dotkliwość określona poprzez zakres szkodliwości;
2. motywacja;
3. częstotliwość pojawienia się;
4. rodzaj szkody, np. czasowa spowoduje tylko przerwę w dostępie do zasobu, ale może być też stała, która może zniszczyć całkowicie zasoby;
5. źródło występowania [17][15].

Przyglądając się zagrożeniom środowiskowym możemy skorzystać z danych statystycznych, które uwzględnia się podczas określania zagrożeń w instytucji. Uwarunkowania kulturowe i środowiskowe, w których funkcjonuje dana jednostka organizacyjna, mogą znacząco wpływać na sposób postępowania z zagrożeniem. W pewnych wyjątkowych przypadkach, ze względu na specyficzne uwarunkowania kulturowe, pewne zagrożenia mogą nie być określane, jako szkodliwe a w innych mogą zostać uznane, jako zagrażające bezpieczeństwu informacji w organizacji [17, 35].

Wobec przedstawionych powyżej, różnego rodzaju zagrożeń to środowisko i często koniunktura, otoczenie, w której obraca się organizacja decydują o czynniku szkodliwości powstania zagrożeń i warunkują zasady postępowania w organizacji.

Dlatego też powinno się zwracać uwagę na wszystkie źródła pochodzenia zagrożenia (wewnętrzne, zewnętrzne, naturalne, techniczne, pierwotne przedmiotowe, podmiotowe itd.)

Zagrożenia mogą mieć bardzo różnorodne pochodzenie, co zaprezentowano w tabelach 3-6. Wynika z tego, że problem jest złożony i faktem jest, że ryzyko zagrożenia ma wpływ na wszystkie obszary prowadzenia działalności gospodarczej. i tak począwszy od fizycznego zniszczenia informacji, po ataki na systemy informatyczne, używanie nielegalnego oprogramowania, czynnik ludzkiej słabości oraz inne należy traktować wszystkie je priorytetowo i uważać, jako ważne. Rozwój technologiczny, używanie nowych technik powoduje powstawanie coraz to nowych niezidentyfikowanych dotychczas źródeł zagrożeń.

Takie niebezpieczeństwo niosą ze są przestępstwa komputerowe, gdzie zagrożone są sieci podmiotów komunikujących się nawzajem ze sobą. Bez względu jednak na to skąd one pochodzą, instytucje gospodarcze powinny być wyczulone na ich negatywny wpływ.

W ramach Agencji Bezpieczeństwa Wewnętrznego, której zadaniem jest ochrona bezpieczeństwa wewnętrznego państwa, funkcjonuje Departament Bezpieczeństwa Teleinformatycznego, w skład, którego wchodzi Rządowy Zespół Reagowania na Incydenty Komputerowe tzw. CERT.GOV.PL. Pełni on rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym, publikując *Raport o stanie bezpieczeństwa cyberprzestrzeni RP, w którym* przedstawiono katalog zagrożeń (tab.8). Wg. dostępnych danych skorzystano z takich informacji prezentując zidentyfikowane zagrożenia.

Tabela 8. Katalog zagrożeń wg.CERT.GOV.Pl.

	RODZAJ ZAGROŻENIA	TYP ZAGROŻENIA-PODATNOŚĆ
Działania celowe	Publikacje w sieci Internet	Szkodliwe, obraźliwe treści Publikacja danych wrażliwych, dezinformacja, pomawianie, zniesławienie
	Przełamanie zabezpieczeń	Włamanie na konto, włamanie do systemu, włamanie do infrastruktury, nieuprawnione kopiowanie
	Oprogramowanie złośliwe	Wirus, ransomware, klient botnetu, koń trojański, robak sieciowy
	Sabotaż komputerowy	Atak odmowy dostępu np; DDoS, DOS Zniszczenie całkowite zasobu Wykorzystanie podatności w urządzeniach czy aplikacji Skanowanie danych Nieuprawniona zmiana informacji, nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji
	Czynnik ludzki	Prace techniczne, awaria , zaniedbanie,

	RODZAJ ZAGROŻENIA	TYP ZAGROŻENIA-PODATNOŚĆ
		naruszenie polityki bezpieczeństwa, naruszenie obowiązujących przepisów prawnych
	Podatności	Ujawnienie podatności, błędna konfiguracja
	Cyberterroryzm	Zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni
Działania niecelowe	Wypadki i zdarzenia losowe	Awarie sprzętowe, awarie łącza, awarie-błędy oprogramowania
	Czynnik ludzki	Brak wiedzy, błędna konfiguracja urządzenia, naruszenie procedur, praw autorskich

Źródło: Opracowanie na podstawie [46].

Z uwagi na to, że działalność organizacji gospodarczych oparta jest, o zasoby informacyjne o charakterze operacyjnym, strategicznym, taktycznym to należy, je w odpowiedni sposób ochraniać przed zniszczeniem, ujawnieniem oraz modyfikacją, utratą czy dostępnością. Do sytuacji, w których informacja jest szczególnie narażona, należy przesyłanie danych, dostęp do informacji oraz jej przechowywanie.

Urzeczywistnienie się zagrożenia doprowadza do incydentu, który w następstwie może doprowadzić do wywołania szkód w systemie oraz całym przedsiębiorstwie.

Przytoczone zagrożenia szczególnie wskazały na przestępczość komputerową, jako na zagrożenie dla przedsiębiorstw komunikujących się ze sobą. Nie bez wpływu są również włamania komputerowe, co znajduje potwierdzenie w raportach CERT. Ponadto odnotowano metody phishingowe, oszustwa, kradzieże, szpiegostwo gospodarcze, wyłudzenie informacji, błędy pracowników kończąc na awariach technicznych, złośliwym oprogramowaniu czy klęskach żywiołowych itp. Zagrożenia mogą mieć charakter środowiskowy (tabela 3), ludzki (tabela 5), przypadkowy i rozmyślny (tabela 4,8).

Zagrożenia połączone z lukami w systemie tworzą niebezpieczeństwo dla systemu komputerowego w skutek bezpośredniego lub pośredniego ataku na aktywa organizacji. Zatem, zagrożenia i ryzyko utraty informacji wzajemnie na siebie oddziałują.

Patrząc na pochodzenie zagrożeń oraz ich różnorodność i miejsca, w których mogą się pojawić profilaktyka działań zapobiegających powstaniu zagrożeń, również powinna być bardzo szeroka stosowana obejmując zabezpieczenia techniczne, teleinformatyczne, fizyczne, administracyjne, organizacyjne, sprzętowe- programowe i inne szerzej omówione w niniejszej pracy.

1.5. Wpływ zagrożeń socjotechnicznych na BI firmy

Jak podaje Hadnagy Christopher w swojej książce [47] „*socjotechnika nie różni się wyraźnie od przekrętu czy pospolitego oszustwa, jednak termin ten jest zwykle stosowany na określenie sztuczek lub podstępów stosowanych w celu gromadzenia informacji, dokonywania oszustw lub uzyskiwania dostępu do systemów komputerowych"* [47]. Dokonując interpretacji pojęcia socjotechnika można stwierdzić, że jest to sterowanie zachowaniami ludzkimi skierowanymi na podjęcie określonych działań (w domyśle ułatwiających ujawnienie informacji). Socjotechnika stała się wręcz wszechobecna. Występuje w mediach, biznesie, polityce, miejscach pracy, życiu publicznym i społecznym oraz zawodowym. Zdecydowana część wpływu społecznego, pod jakim się znajdujemy i pułapki socjotechniczne, w które wpadamy zazwyczaj odbywają się na poziomie nieświadomym. Z tego też względu możemy myśleć, że te tematy nas nie dotyczą. Jednak nie ma takiego człowieka, który by oparł się manipulacji w swoim życiu [48].

Nie można w tym miejscu pominąć zdania i uwag zespół CERT, który w swoich raportach rocznych 2011/2012 poinformował o użyciu socjotechniki na systemy informatyczne administracji publicznej, posługując się pocztą elektroniczną. Od roku 2011 zaobserwowano wzrost ilości dedykowanych ataków socjotechnicznych skierowanych przeciwko pracownikom administracji publicznej [49].

W socjotechnice informacja to przekazywanie danej treści przez nadawcę do odbiorcy poprzez kanał łączności tzn. środek przekazania informacji. Ze względu na jej charakter można nadać jej różne cechy prawdziwości lub też niezgodności ze stanem rzeczywistym. Socjotechnika zakłada wykorzystanie naiwności oraz niewiedzy ludzi w celu zdobycia informacji mających znaczny wpływ na prawidłowe funkcjonowanie jednostki. Ponadto, służy wywołaniu pożądanych przemian w postawach i zrachowaniach społecznych. Dlatego też uważana jest, za ogromne zagrożenie. w socjotechnice obowiązuje ogólna zasada zgodnie, z którą im więcej gromadzisz informacji, tym większa szansa na sukces.

Słownik Webster′s Dictionary definiuje słowo *społeczny*, jako „*dotyczący życia, dobrobytu oraz wzajemnych relacji ludzi żyjących w społeczności*". Natomiast Inżynierię definiuje się jako „*naukę lub sztukę znajdowania praktycznych zastosowań teoretycznej myśli naukowej.*.". Połącznie tych dwóch definicji dopiero pozwala spojrzeć na inżynierię społeczną, jako na socjotechnikę, czyli próby manipulowania

ludźmi w taki sposób, aby podjęli określone działania. Może chodzić tutaj o pozyskiwanie informacji, uzyskanie dostępu do czegoś lub nakłonienie ofiary do podjęcia konkretnych działań. Okazuje się, bowiem, iż wiele możemy nauczyć się od stróżów prawa, polityków, psychologów, aby móc skuteczniej ocenić poziom bezpieczeństwa. Podczas gdy psycholog formułuje pytania, wprowadza w stan rozluźnienia, i uspakaja ludzi. Stróż prawa prowadzi efektywne przesłuchanie, uzyskując potrzebne informacje od ofiary. Politycy i przedstawiciele władz, najskuteczniejsi sprzedawcy świata formułują tak zdania, aby osiągnąć najlepszy możliwy efekt. Socjotechnika występuje w trzech formach:

Działania perswazyjne, system sterujący może znacznie wpłynąć na zmianę postawy i poglądów jednostki manipulowanej
Działania manipulacyjne, które zmieniają poglądy, zachowania wobec jednostki sterowanej lub też dzieją się zupełnie bez jej wiedzy
Działania facylitacyjne, tworzą realne sytuacje, które mogą ułatwić kształtowanie postaw ludzi

Współczesne postrzeganie socjotechniki skłania się ku wykorzystaniu znajomości ludzkiej psychiki, tak by podporządkować sobie ofiarę. Doświadczeni socjotechnicy opanowali do perfekcji tworzenie sytuacji stymulujących emocje typu strach, poczucie winy, czy podekscytowanie. Dzięki tym umiejętnościom skutecznie nakłaniają ludzi do mówienia, i oto jest ten czynnik, od którego zależy sukces lub też porażka socjotechnika. z chwilą, kiedy socjotechnik poznaje zasady rządzące w firmie, może z powodzeniem nawiązać kontakt z pracownikiem i go zastraszyć. z kolei zastraszenie powoduje obawę przed karą, co zwiększa chęć współdziałania ofiary. Ponadto zastraszenie może również wywoływać obawę przed ośmieszeniem przed innymi pracownikami lub też stratę szansy na awans.

Zadziwiający jest fakt, że socjotechnicy są w posiadaniu szczegółowych działań takich instytucji jak: policja, prokuratura, praktyk firm telekomunikacyjnych itp. Dodatkowo posiadają dane dotyczące obszarów przydatnych podczas ataków, czyli telekomunikacji czy komputerów [50] [51].

Socjotechnikę również można dostrzec w wydarzeniach politycznych. Np.: w roku 2010 po katastrofie rządowego samolotu pod Smoleńskiem odnotowano e-maile z kondolencjami, które trafiły do Sejmu RP, rzekomo wysłanych przez Ambasadę Kazachstanu. Jednak e-mail zawierał załącznik ze złośliwym oprogramowaniem, którego otwarcie mogło doprowadzić do utraty istotnych informacji lub co gorsze przejęcia kontroli nad użytkowaniem komputera. Opisana sytuacja sugeruje, iż sposoby

i pomysły na ataki socjotechniczne są nieograniczone i w znacznym stopniu zależą od pomysłowości atakującego oraz celu, jaki obrał sobie intruz [5]. Zatem należy bardzo uważać na załączniki wiadomości poczty e-mailowych oraz darmowe oprogramowanie. Przebiegły napastnik postara się użyć możliwych środków, aby włamać się do firmowej sieci komputerowej, łącznie z wykorzystaniem naszych skłonności do otrzymania darmowych prezentów. Czasem przyciąga nasz wzrok oferta i otwieramy załącznik, by zobaczyć poradę inwestycyjną, rabaty na komputer, telewizor, czy telefon. Klikamy na załącznik, który przenosi nas na stronę, o której nigdy wcześniej nie słyszeliśmy. Pewnie w większości przypadków to, co zobaczymy, będzie tym, czego się spodziewaliśmy, aczkolwiek czasami mogło to zostać nam celowo wysłane. Przesłanie niebezpiecznego programu na nasz komputer to tylko jeden z elementów ataku.

Działanie destrukcyjnych wirusów opiera się na socjotechnicznej manipulacji, która wykorzystuje nasze pragnienie otrzymania czegoś za darmo. Dzięki temu mogły swobodnie poruszać się wirusy o nazwie Anna Kurnikova, SirCam, Love Letter. Wirus pojawia się w załączniku do poczty e-mail, który przykuwa uwagę czymś intersującym. Może to być informacja poufna, czy też darmowa pornografia lub też wiadomość, że załącznik zawiera rachunek za jakąś rzecz, którą domniemająco kupiliśmy. Wszystkie te formy ataku działają. Na przykład w ostatnim przypadku otwieramy załącznik, powodowani strachem, że nasza karta kredytowa została obciążona, mimo, że wiemy, iż nic nie kupowaliśmy. Okazuje się, że metoda ta jest bardzo skuteczna i mimo, że znamy niebezpieczeństwa związane z otwieraniem załączników i tak je otwieramy [52].

Rozróżniamy dwie metody związane z atakami socjotechnicznymi na systemy informatyczne: wykorzystujące technologię informatyczną oraz wykorzystujące techniki komputerowe. Niezwykle efektywnym działaniem socjotechnicznym jest wysłanie e-maila z załącznikiem ze wskazaniem nadawcy, jako osoby dobrze znanej adresatowi. W takim wypadku większość adresatów nie zastanawia się czy otworzyć załącznik z poczty uznając to za działanie bezpieczne. Każda z tych osób otrzymuje wiadomość od kogoś, kogo zna i komu ufa, jednak wiadomość zawiera wirusa. Ofiara niczego nie podejrzewa z uwagi na identyfikator nadawcy, który jednoznacznie sugeruje, od kogo pochodzi wiadomość.

Kolejnym typem niebezpiecznych programów to te, które po uruchomieniu na komputerze pracują bez naszej wiedzy i zgody albo, co gorsza wykonują działania, których w ogóle nie jesteśmy świadomi. Mogą to być dokumenty Worda, prezentacje PowerPoint lub pliki każdego z programów, które potajemnie instaluje

nieautoryzowany program. Mowa tutaj o wersji konia trojańskiego. Z chwilą, kiedy program zainstaluje się na naszym urządzeniu, może przesłać napastnikowi wszystko, co wpisujemy na klawiaturze, łącznie z hasłami i numerami kart kredytowych [52].

Istnieją jeszcze dwa rodzaje niebezpiecznego oprogramowania. Jeden z nich jest w stanie przesłać każde słowo, jakie wypowiemy w zasięgu komputerowego mikrofonu (nawet wtedy, gdy jesteśmy w oddaleniu od komputera i wydaje się, że jest on wyłączony). z kolei drugi rodzaj dotyczy komputera wyposażonego w kamerę sieciową, gdzie napastnik może za pomocą tej techniki widzieć wszystko, co się dzieje wokół naszego komputera, (mimo iż wydaje się, że kamera jest wyłączona) [52].

W przypadku wykorzystania komputerów do ataków możliwe jest wykrycie takich działań w cyberprzestrzeni oraz zareagowanie poprzez zwalczanie zagrożeń. Takimi narzędziami są antyspam, czy też programy antywirusowe. Dużo trudniejsze do wykrycia są metody kontaktu bezpośredniego. Z uwagi na to, że człowiek jest najsłabszym ogniwem w systemie bezpieczeństwa, nie jest jednak łatwe wcześniejsze monitorowanie, wykrycie i opracowanie sposobów zwalczania tego typu zagrożeń [5]. Złośliwi hakerzy nie znikają z firmy tylko, dlatego że jej nie lubią. Socjotechnika manipulowania pracownikami i oszustwa internetowe to zabiegi, które stosuje się wszechobecnie. Współczesne przedsiębiorstwa programistyczne uczą się jak najskuteczniej zabezpieczać swoje aplikacje, więc hakerzy i złośliwi socjotechnicy skierowali swoją uwagę na najsłabszy element systemu, czyli na człowieka. Kierują się przy tym zwrotem z inwestycji, ponieważ żaden dobry haker nie poświęci wielu godzin i dni na uzyskanie tych samych wyników, które może osiągnąć podczas prostego ataku, przeprowadzonego w ciągu niespełna godziny [47].

Złośliwe działania pracowników zdecydowanie świadczą o tym, że firmy powinny zwrócić szczególną uwagę na zagrożenia związane ze stosowaniem socjotechniki. Wielu ataków z pewnością można by uniknąć gdyby, ludzie byli bardziej ostrożni, co do przekazywanej wiedzy innym konkurencyjnym podmiotom czy osobom.

Świadomość bezpieczeństwa oznacza edukację wszystkich pracowników, znajomość polityki i procedur bezpieczeństwa stosowanych w jednostce organizacyjnej. Okazuje się że polityka ta jest niezbędna, jako wyznacznik stosowania reguł w celu ochrony systemów informatycznych i przekazywania poufnych danych. Zatem, jeśli pracownik nie jest wyszkolony, czujny i nie postępuje zgodnie z procedurami to utrata informacji na korzyść socjotechnika jest tylko kwestią dni. Firma powinna nie tylko

zdefiniować zasady w formie pisemnej, ale i poczynić dodatkowy wysiłek, aby pracownicy mający do czynienia z informacją lub systemami komputerowymi zapoznali się i zapamiętali zasady oraz zgodnie z nimi postępowali. Dobrze jest się również upewnić, że wszyscy rozumieją zasadność wprowadzonych ograniczeń i aby nie próbowali ich omijać choćby z wygody. Zatem, niewiedza zawsze będzie dla pracownika dobrym wytłumaczeniem, jednak dla socjotechnika stanie się słabą stroną, którą, chętnie wykorzysta. Mądrym zachowaniem, więc będzie nie czekanie aż coś się wydarzy, ponieważ straty finansowe dla przedsiębiorstwa mogą okazać się niepowetowane [35,36,77]. „*Nawet najbardziej bezpieczny system świata da się złamać. Często to właśnie pierwiastek ludzki tych systemów okazuje się najprostszy do zmanipulowania i oszukania. Wywoływanie paniki, wywieranie wpływu, stosowanie technik manipulacyjnych i wzbudzanie zaufania to wszystko metody stosowane w celu uśpienia czujności ofiary"* [47]. Christopher Hadnagy podaje w swojej książce motto, które brzmi następująco" *bezpieczeństwo przez wiedzę*". Znaczenie wiedzy daje pewne podstawy, aby móc mówić o zabezpieczeniu przed coraz częstymi przypadkami stosowania socjotechniki czy kradzieży tożsamości. Poza tym skutecznym sposobem minimalizacji skutków tego rodzaju ataków jest właśnie wiedza, o tym jak do nich dochodzi, w jaki sposób się je prowadzi oraz jak myślą ludzie odpowiedzialni za te działania.

Jak oszacowała firma Kaspersky Labs, która jest wiodącym producentem oprogramowania antywirusowego na świecie, w 2009 roku w serwisach społecznościowych rozpowszechniono ponad 100 tysięcy próbek złośliwego oprogramowania. Przedstawiciele firmy Kasperski stwierdzają, iż „ *ataki skierowane przeciw sieciom społecznościowym są dziesięciokrotnie bardziej skuteczne niż ataki innego rodzaju*" [47]. Uzyskanie informacji na potrzeby ataków socjotechnicznych wcale nie jest takie ciężkie. W tym celu wykorzystuje się portale społecznościowe tj. Facebook, Twitter czy też wyszukiwarki internetowe tj. Google, Bing lub portale z zawartościami multimedialnymi tj.Youtube, Google Maps, Google Images. Nieocenionym źródłem wiedzy okazują się również Wikipedia, NetCraft, Whois oraz strony atakowanych organizacji, dzięki którym możliwe jest uzyskanie informacji o celu ataku, mogących uwiarygodnić cyberprzestępcę w oczach pracowników przedsiębiorstwa. Takie strony internetowe, gromadzące różnego rodzaju informacje wrażliwe (data urodzenia, hasło do konta) powstają każdego dnia. Atakujący socjotechnik, który posiada już wiedzę, uwiarygadnia swoją osobę przed pracownikami

organizacji, tym samym uzyskuje coraz istotniejsze informacje, co w rezultacie pomaga w dalszej fazie ataku. Przedstawienie się innym, za pracownika firmy zdecydowanie ułatwia zdobycie wiedzy o jednostce organizacyjnej [5, 53].

Kelvin Mitnick, jeden z najbardziej znanych włamywaczy komputerowych na świecie, wykorzystał właśnie socjotechnikę, aby wyłudzić informację, która z kolei umożliwiła mu przełamanie zabezpieczeń systemów informatycznych wielu znanych i prestiżowych firm m.in.: SCO, Pacific Bell, Nowel, agendy rządowe FBI oraz Pentagon. Jak bardzo może być groźna socjotechnika z wykorzystaniem informatyki świadczy uzasadnienie sądu, że Kevin Mitnicka po zakończeniu odbywania kary otrzymał zakaz zatrudnienia w firmach informatycznych i telekomunikacyjnych [5]. Wydaje się, więc oczywistym, że od manipulacji nie da się uchronić. Jest również niemożliwe opanowanie czy poznanie wszystkich stosowanych technik manipulacji i wywierania nimi wpływu na innego człowieka. Nowe metody i techniki wpływu oraz różne kombinacje powstają na każdym kroku. Można natomiast nauczyć się podstawowych reguł i zasad, które rządzą socjotechniką oraz poznać najważniejsze narzędzia wpływu stosowane przez manipulantów. W świetle przytoczonych faktów, skuteczna ochrona przed manipulacją nie istnieje.

Reasumując dociekania o socjotechnice w zakresie systemów informatycznych można zamknąć je następującą konkluzją Kevina Minicka: „*W miarę wymyślania coraz to nowych technologii zabezpieczających, utrudniających znalezienie technicznych luk w systemie, napastnicy będą zwracać się w stroną ludzkich słabości. Złamanie ludzkiej bariery jest o wiele prostsze i często wymaga jedynie inwestycji rzędu kosztu rozmowy telefonicznej*…” [52].

1.6. Bezpieczeństwo teleinformatyczne i jego znaczenie w XXI wieku

1.6.1. Istota bezpieczeństwa teleinformatycznego

Obecnie świat bez technologii informatycznych, wykorzystujących globalną sieć Internet, nie byłby w stanie osiągnąć tak spektakularnego rozwoju cywilizacyjnego. Poprzez Internet, jako medium komunikacji znacznie ułatwione jest prowadzenie działalności poza granicami państwa. Ale i również anonimowo i nieskrępowanie poza granicami państwa można prowadzić działalność niszczenia danych w postaci cyfrowej,

doprowadzenia do nieprawidłowego funkcjonowania infrastruktury, kradzieży czy zastraszania użytkowników internetu.

Współczesne prowadzenie działalności gospodarczej wymusza korzystanie z przeróżnych rozwiązań technologicznych. Skutkiem wprowadzenia technologii jest przekształcenie systemów informacyjnych biznesu na systemy informatyczne biznesu. Na żywo można zobaczyć postępującą transformację coraz większej liczby dokumentów papierowych na elektroniczne odpowiedniki. Znacznym zmianom uległy również techniki gromadzenia, przetwarzania i przesyłania danych. Dokumenty elektroniczne zaczęto gromadzić na nośnikach danych np.: na dyskach twardych, serwerach, komputerach osobistych, czy dyskach DVD, CV w postaci plików oraz baz danych. Zaczęto przetwarzać dane poprzez programy komputerowe, które odznaczają się dużą prędkością przeprowadzania operacji. Operacje przesyłania danych elektronicznych wewnątrz jednostki gospodarczej, jak i na zewnątrz wykonywane są za pośrednictwem lokalnych i rozległych sieci teleinformatycznych. W związku z powyższym, zauważono, że wraz ze wzrostem nasycenia środkami technicznymi informatyki w większości obszarów organizacji, znaczącym problemem okazał się dobór odpowiednich zabezpieczeń dla gromadzonych, przetwarzanych i przesyłanych danych. Dostęp do sieci Internet daje liczne korzyści, tj. nieograniczony dostęp do wszelkiej informacji, szybkie sposoby komunikowania się a zarazem niskie koszty działania. Każdy z nas, zauważa o wiele więcej walorów i zalet internetu. Jednak niewielu zastanawia się nad niebezpieczeństwami czyhającymi na nieostrożnych użytkowników. Systemy komputerowe narażone są na zagrożenia, bez względu na to czy podłączone są do Internetu czy też nie [5, 45, 54].

Na przełomie XX/XXI wieku, świat obiegła informacja dotycząca wystąpienia szczególnie ważnych zagrożeń dla bezpieczeństwa teleinformatycznego. Przykłady ofiar cyberataku zostały szczegółowo opisane w pozycjach [55, 56, 36].

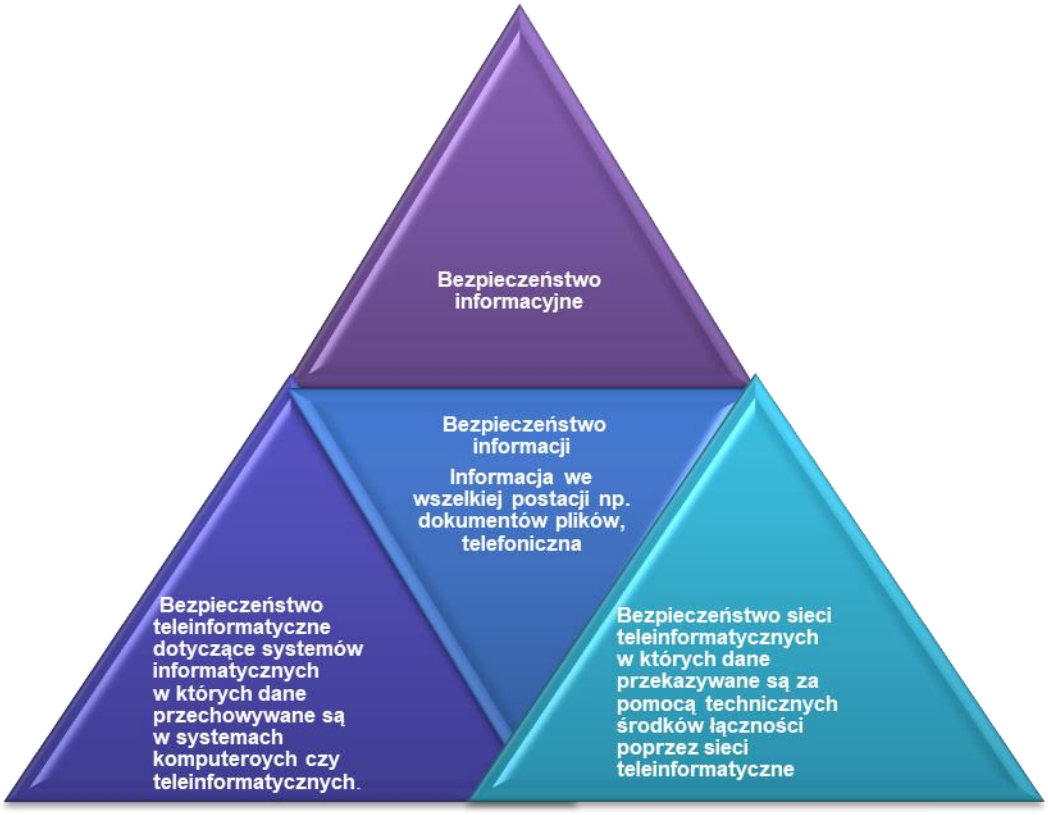
Każda z tych sytuacji jest inna, jednakże wszystkie odznaczają się wspólnym mianownikiem, tj.: deficytem informacji, dezinformacją, paniką, przerwaniem pracy w wyniku zaistnienia zagrożenia, destabilizacją, utratą kontroli, przerwaniem procesów decyzyjnych. Przyglądając się tym sytuacjom można wyciągnąć wniosek, że bezpieczeństwo nie jest stanem, lecz ciągle zmieniającym się procesem.

W kontekście tematu rozważań niniejszej pracy, warto zwrócić najpierw uwagę na termin bezpieczeństwa informacyjnego, w skład, którego wchodzi bezpieczeństwo teleinformatyczne.

Ponieważ informacje są celem ataku, więc zakłócenie ich może powodować zakłócenie w prawidłowym funkcjonowaniu systemu teleinformatycznego.

Andrzej Białas opracował definicję bezpieczeństwa informacyjnego, które definiuje je, jako: „*zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymania poziomu poufności, integralności, dostępności, rozliczalności, autentyczności* ” [40]. A. Białas skupia się na procesowym ujęciu bezpieczeństwa, choć wskazuje atrybuty, które pozwalają określić, czy bezpieczeństwo zostało osiągnięte czy też nie.

Zatem, bezpieczeństwo informacyjne jest pojęciem bardzo obszernym, dotyczącym dwóch rodzajów bezpieczeństw, co graficznie prezentuje rysunek 5.



Rysunek 5. Rodzaje bezpieczeństwa informacyjnego
Źródło [58].

Bezpieczeństwo procesu informacyjnego będzie zapewnione, jeśli zapewnione zostanie sprawne i poufne gromadzenie informacji oraz ich przetwarzanie, przetrzymywanie i przesyłanie w systemach teleinformatycznych. Prowadząc dyskusję

na temat bezpieczeństwa informacyjnego nie sposób pominąć obszaru dotyczącego teleinformatyki.

Technologie teleinformatyczne są spotykane coraz częściej i w coraz bardziej odpowiedzialnych zastosowaniach, dlatego też szczególnego znaczenia nabiera ich bezpieczeństwo. Wspomnieć tutaj należy o potrzebie obrony krajowych infrastruktur teleinformatycznych, służących obronności, łączności, energetyce, czy bankowości oraz o rozwoju technologii teleinformatycznych społeczeństwa informacyjnego.

Ponadto autorka pracy zgadza się z poglądami J. Jańczaka oraz A. Nowaka [58], którzy rozumieją bezpieczeństwo teleinformatyczne, jako całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych. Dotyczy to ochrony danych wytwarzanych, przetwarzanych przechowywanych, w systemach i sieciach przed przypadkowym bądź celowym ujawnieniem, modyfikacją czy zniszczeniem w wyniku, czego uniemożliwione jest ich przetwarzanie poprzez zastosowanie technicznych, programowych czy kryptograficznych i organizacyjnych środków i metod zapobiegających ujawnieniu.

Mamy, więc do czynienia ze zbiorem zagadnień z dziedziny telekomunikacji i informatyki bezpośrednio związanych z monitorowaniem ryzyka, wynikającego z korzystania komputerów, sieci teleinformatycznych czy przesyłania danych. To całokształt działalności zmierzającej do uniemożliwienia przypadkowego lub też celowego ujawnienia informacji chronionej, która może być przesyłana za pomocą technicznych środków teleinformatycznych.

1.6.2. Rodzaje zagrożeń bezpieczeństwa teleinformatycznego

Ze względu na wieloaspektowość bezpieczeństwa i bogatą literaturę z tego obszaru oraz uwzględniając tematykę niniejszej pracy, zasadne jest dokonanie dalszej percepcji zagrożeń oraz wynikających z nich typologii bezpieczeństwa. Istota ochrony oraz bezpieczeństwa informacji została przedstawiona już w rozdziale 1.1. dla zachowania logicznej struktury oraz zbudowania podstaw do omówienia typologii bezpieczeństwa informacji w kontekście zagrożeń.

Istnieje szereg zidentyfikowanych zagrożeń, opisanych przez naukowców, jednak w kontekście tematu należy zwrócić również uwagę na zagrożenia związane z ujawnieniem danych.

Punktem wyjścia dla rozpatrywania omawianego zagadnienia bezpieczeństwa danych jest identyfikacja zasobów, które należycie powinny być chronione. Zasoby te mogą być materialne lub niematerialne, i nie zawsze stanowią własność danej jednostki gospodarczej, chociaż są potrzebne do odpowiedniego jej funkcjonowania. W zależności od indywidualności organizacji, zasoby podlegające ochronie są zlokalizowane w różnych miejscach tzn. mogą być gromadzone w systemach komputerowych, pisane, drukowane, przesyłane w sieciach teleinformatycznych, przekazywane ustnie między pracownikami. Do zasobów podlegających ochronie należą dane lub obiekty realizujące całość lub część funkcji związanych z tworzeniem, przechowywaniem, przekazywaniem i wykorzystaniem danych. Do wspomnianych zasobów można zaliczyć:

- Zasoby ludzkie –kadrowe, tworzone przez personel mający dostęp do danych (administratorzy, analitycy, programiści, wdrożeniowcy, konsultanci, pracownicy ochrony) oraz zgromadzoną w ich umysłach wiedzę.
- Zbiory dokumentów- zestawy danych w postaci papierowej czy elektronicznej (tekstowej, liczbowej, graficznej, multimedialnej).
- Zasoby programowe- niematerialne dotyczące oprogramowania wykorzystywanego w jednostce organizacyjnej (oprogramowanie systemowe, kody źródłowe).
- Zasoby infrastrukturalne- fizyczne przedmioty, które są pomocne do uzyskania dostępu do danych i ich użytkowania (sprzęt komputerowy, urządzenia sieciowe i telekomunikacyjne, urządzenia do wprowadzania i wyprowadzania danych) [45][16].

Z uwagi na fakt, że rodzaj, jakość i sposób wykorzystania opisanych zasobów przesądzają o wartości rynkowej przedsiębiorstwa, należy zwrócić szczególną uwagę na pojawianie się zagrożeń dla danego podmiotu gospodarczego, które wzrastają wraz z rozwojem technologii teleinformatycznych. Niebezpieczeństwa dla bezpieczeństwa danych stanowią zjawiska oraz czynności, których działanie może spowodować poważną stratę w zasobach informacyjnych organizacji.

Tabela 9. Klasyfikacja zagrożeń i ich skutki

Kryterium	Podział zagrożeń	Przykłady zagrożeń i ich skutki
Rola człowieka	**Zagrożenie zależne od człowieka**	Bezprawna modyfikacja oprogramowania lub danych w związku z tym ujawnienie danych lub ich usunięcie, nielegalne kopiowanie, instalowanie programów komputerowych, skanowanie

Kryterium	Podział zagrożeń	Przykłady zagrożeń i ich skutki
		oprogramowania lub danych, kradzież sprzętu komputerowego lub wyposażenia, przechowywanie zabronionych prawem zbiorów, błędy powstające wskutek braku wiedzy lub przemęczenia czy roztargnienia, zaniedbanie obowiązków służbowych, których skutkiem jest niezamierzone zagubienie, zniszczenie czy skasowanie czy tez rozpowszechnienie danych innym niepowołanym osobom.
	Zagrożenie niezależne od człowieka	Wyładowania atmosferyczne, powódź, pożar, wilgoć.
Obiekt oddziały-wania	**Zagrożenia związane z ludźmi**	Nieprzestrzeganie tajemnicy służbowej i handlowej przez personel podmiotu gospodarczego, udostępnienie współpracownikom lub osobom obcym informacji o systemach zabezpieczeń stosowanych w danym podmiocie gospodarczym, nagła utrata lub rezygnacja z pracy pracowników np. inspektora ochrony danych, programistów lub przejście do grupy osób mających dostęp do tajnych danych do konkurencji.
	Zagrożenia sieci teleinformatyczch	Celowe bądź niezamierzone poczynania ludzkie np. kradzież elementów sieci, uszkodzenie fizyczne sieci, zła konfiguracja, całkowite blokowanie działanie sieci, podsłuch lub nieuprawnione korzystanie z sieci, awarie sieci teleinformatycznych wywołanych czynnikami zewnętrznymi np. wyładowania atmosferyczne, pożar.
	Zagrożenia dotyczące danych	Nieuprawnione przeglądanie danych, nieupoważniona modyfikacja danych (zmiana treści, usunięcie) bezprawne kopiowanie danych, monitorowanie(podsłuch) danych, wprowadzenie nieprawdziwych danych, zaprzeczenie nadania/odbioru danych.
	Zagrożenia dotyczące oprogramowania	Takim zagrożeniem może być błąd popełniony przez producenta oprogramowania lub na skutek świadomego lub nieświadomego działania pracowników lub też osób trzecich np. zła instalacja, konfiguracja, wdrożenie lub administracja, skasowanie lub modyfikacja oprogramowania, celowe wprowadzenie złośliwych programów, blokowanie poprawnie funkcjonujących aplikacji, nielegalny dostęp, bezprawne użytkowanie.
	Zagrożenia dotyczące sprzętu komputerowego	Spowodowane przerwami w dostawie energii elektrycznej lub też wywołane zamierzonym lub niezamierzonym działaniem ludzkim np. kradzieżą, mechanicznym uszkodzeniem, błędem konfiguracji, niewłaściwym użytkowaniem lub konserwacją, niespodziewane awarie elementów mechanicznych lub elektrycznych sprzętu komputerowego.
	Zagrożenia niepowodujące straty, ale niefinansowe	Utrata pozytywnego wizerunku firmy, prestiżu i dobrego imienia, spadek wiarygodności jednostki gospodarczej, spadek wydajności, narażenia zdrowia lub życia ludzkiego, w wyniku sfałszowania i niepełnych danych , podjęcie błędnych decyzji
	Zagrożenia powodujące straty finansowe	Strata kontrahentów, utrata technologii, brak możliwości zachowania ciągłości działania przedsiębiorstwa, niezwłoczna konieczność wymiany oferowanych produktów, utrata bądź zniszczenie sprzętu i oprogramowania, finansowe konsekwencje wynikające z nieprzestrzegania norm prawnych, wzrost składek ubezpieczeniowych, konieczność zatrudnienia nowych pracowników, koszty sądowe, kryzys w prowadzeniu działalności gospodarczej lub w konsekwencji jej zamknięcie.

Źródło: Opracowanie na podstawie [45, 59].

Zagrożenia dla bezpieczeństwa danych składają się na podział wg. różnych kryteriów. Tymi kryteriami są miedzy innymi: rola człowieka, obiekt oddziaływania oraz skutek oddziaływania. Poszczególne zagrożenia mają różny stopień wystąpienia

i najczęściej największy procentowy udział pochodzi z wnętrza podmiotu gospodarczego oraz skierowany jest na nieświadome działania personelu, czy też współpracowników przedsiębiorstwa. Zupełnie inaczej wygląda sytuacja z zagrożeniami powodującymi starty w zasobach jednostek gospodarczych, do których zaliczyć można np. pożar i związane z tym skutki [59].

Zespół CERT Polska pracuje w obszarze Państwowego Instytutu Badawczego, który prowadzi działalność naukową, krajowy rejestr domen.pl i świadczy usługi teleinformatyczne. CERT Polska istnieje od 1996 roku i jest pierwszym w Polsce zespołem reagowania na incydenty, rozpoznaje i mierzy zagrożenia, które dokuczają przedsiębiorcom. Ponadto razem z innymi instytucjami krajowego systemu cyberbezpieczeństwa analizuje skuteczność metod zapobiegania, wykrywania i znoszenia zagrożeń. W raportach znajdują się dane liczbowe na temat zgłoszeń od użytkowników oraz wskazuje wnioski z obserwacji, co do nowych podatności na zagrożenia [60].

W 2020 roku operatorzy z zespołu CERT Polska przyjęli **10420** zgłoszeń incydentów cyberbezpieczeństwa**,** które przeanalizowano i odpowiednio sklasyfikowano. Liczba zgłoszeń stanowi 60,7% w porównaniu do 2019 roku. Więcej informacji zawartych w raporcie odnoszących się do rodzajów ataków wg. typów oraz liczby incydentów w ostatnich latach znajduje się w pozycji [60].

W związku z opanowaniem sektora gospodarczego przez internet, należy stwierdzić, że ataki na systemy komputerowe są jedną z najłatwiejszych źródeł pozyskiwania informacji. Ze względu na charakter zagrożeń oraz ich duże zróżnicowanie w pracy nie skupiono się na wszystkich zagrożeniach występujących w podmiotach gospodarczych, gdyż nie były poddawane szczegółowej analizie w obszarze badań. Opis stosowanych ataków typu: wirusy komputerowe, makrowirusy, konie trojańskie, wrogi „aplet Javy", pfishing, aplikacje szpiegujące (apyware), złośliwe podzespoły (chipping), podszywanie się pod inną osobę (spoofing), przechwycenie transmisji, podsłuchiwanie, backdoor, wiadomości spam, bomby logiczne, zalewanie, broń częstotliwości radiowej, DoS DDoS, receptor van Eycka, bakterie, robaki, pozorowanie identyczności, fałszywy alarm, dialery, uzyskanie informacji metodmi socjal-engineering oraz bezprawne wejście do obiektów chronionych znajdują się szerzej opisane w następującej literaturze [10, 30, 33, 34, 41, 54, 59, 61].

We wszystkich dziedzinach zarządzania nie da się zrezygnować z komputera. To ważne narzędzie narażone jest jednak na ataki ze strony przestępców komputerowych. Mowa tutaj o Joyriderach, wandalach, szpiegach przemysłowych czy szantażystach. Gromadzone informacje, z racji ich ogromnej wartości, stały się ostrym celem ze stronu konkurencji. Niezbędnym jest, zatem aby zarządy spółek poświęcały szczególną uwagę na zabezpieczenia baz danych w komputerach przed nieuprawnionym dostępem, czy też włamaniem.

1.7. Analiza wybranych aktów prawnych regulujących problematykę bezpieczeństwa informacji

Obecnie obowiązujące w polskim prawie regulacje spełniają pośrednią funkcje, ponieważ nie niema jednej zbiorczej ustawy czy rozporządzenia, które obejmowałoby całościowo obowiązki związane z bezpieczeństwem informacji tzn. objaśnienie wymagań, wytycznych, obowiązkowych zabezpieczeń sprzętowych, zabezpieczeń programów i całości organizacji. W wyniku obecnego stanu rzeczy, wdrażając system zarządzania bezpieczeństwem informacji, należy z całą uwagą przeanalizować pogląd ustawodawców, wyrażony w wielu rozporządzeniach, ustaw, standardach normatywnych na podstawie, których opiera się funkcjonowanie organizacji [17]. W niniejszej pracy zostaną określone i przedstawione regulacje prawne związane bezpośrednio lub pośrednio z ochroną informacji. Polskie prawodawstwo reguluje temat dotyczący ochrony informacji następującymi aktami prawnymi: [14, 38, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79]. Są to zaledwie wybrane ustawy, które ściśle w swojej treści zajmują się i podejmują temat bezpieczeństwa informacji. Autorka pracy zwróci uwagę tylko na niektóre z nich.

Konstytucja Rzeczypospolitej Polskiej

- Konstytucja RP, jako najważniejszy akt polski stanowiący podstawę polskiego państwa, gwarantuje prawo do wolności obywatelskiej, przedstawia wzajemne stosunki między władzą ustawodawczą, wykonawczą oraz sądowniczą. W jej treści można odnaleźć artykuły dotyczące bezpieczeństwa informacji. Między innymi w Art. 47, 49 oraz 51 znajdują się odniesienia do bezpieczeństwa informacji. Art.47 wskazuje na prawo do ochrony prawnej życia prywatnego i swobody decydowania o swoim życiu osobistym. Art.49 wskazuje na rolę ochrony tajemnicy komunikowania się i ograniczenia w określonych przypadkach. Natomiast Art.51 mówi, że ujawnić dane może tylko

osoba, której te dane dotyczą, proces gromadzenia i udostępniania informacji określa ustawa a ponadto każdy z nas ma prawo do „*sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą". Nie bez znaczenia jest fakt, że „władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym"* [68].

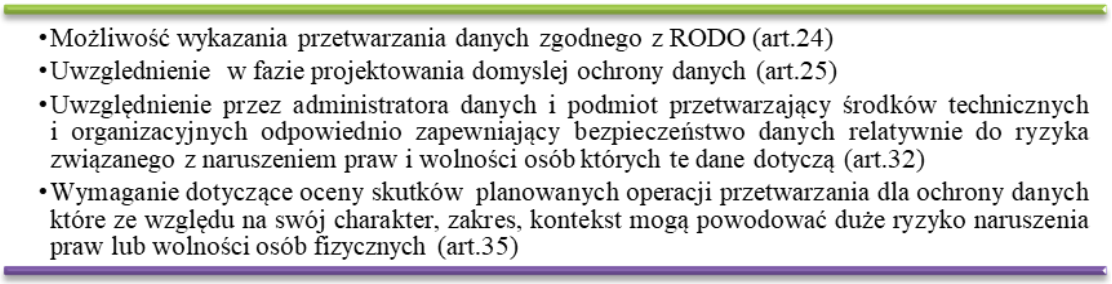
RODO

Mówiąc o RODO mamy na myśli Rozporządzenie Parlamentu Europejskiego i rady UE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, swobodnego przepływu danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych), ściśle zobowiązującego do podjęcia szeregu działań. Szczególnie mowa tutaj o działaniach technicznych i organizacyjnych dla zapewnienia ochrony danych osobowych zgodnie z istniejącymi przepisami. Aktualne przepisy RODO mają zastosowanie od 25 maja 2018r. a uzupełnieniem jest Polska Ustawa o Ochronie Danych Osobowych z dnia 10 maja 2018 roku.

Głównym zadaniem RODO jest utwierdzenie, że ochrona danych osobowych jest podstawowym prawem każdego obywatela. W rozporządzeniu można znaleźć szczegółowe uprawnienia przeznaczone dla osób prywatnych oraz obowiązki przedsiębiorców i instytucji przetwarzających dane osobowe. RODO ma zastosowanie w operacjach przetwarzania danych osobowych, które rozumiemy w świetle ustawy, jako wykonywanie następujących czynności: zbieranie, utrwalanie, organizowanie, podporządkowanie, przechowywanie, adaptowanie, pobieranie przeglądanie, wykorzystanie, ujawnienie poprzez przesłanie, rozpowszechnienie, niszczenie.
Są to czynności, których przedmiot stanowią dane osobowe i nie chodzi tylko o usługi archiwizowania dokumentów, lecz wszystkie operacje dotyczące zbierania do archiwizacji i usunięcia włącznie, wraz z czynnościami wykonywanymi w systemach informatycznych [80].

Przetwarzanie danych osobowych może być realizowane przez Administratora danych, podmiot przetwarzający dane, inne podmioty przetwarzające dane i osoby upoważnione do przetwarzania danych.

RODO zawiera obowiązki administratora danych związanych z zapewnieniem przetwarzania danych zgodnie z obowiązującymi przepisami. Należą do nich następująco:



Rysunek 6. Główne wymagania zapewniające zgodne przetwarzanie danych z RODO
Źródło: Opracowanie własne na podstawie [81].

Dla zrealizowania części zadań administrator danych osobowych może wyznaczyć inną osobę, która będzie nadzorować przestrzeganie zasad ochrony informacji. RODO oprócz roli administratora, którym może być organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych wskazuje na funkcję Inspektora Danych Osobowych. Takiego Inspektora wyznacza Administrator w celu wspomagania oraz nadzorowania systemu ochrony danych osobowych. Natomiast grupa informatyków odpowiedzialna za należyte funkcjonowanie systemu informatycznego i wszystkiego, co się z tym wiąże tzn.: programów, sprzętu i jego okresowe przeglądy, pracuje pod nadzorem Inspektora Ochrony Danych.

Ustawa o ochronie danych osobowych

Ustawa z 10 maja 2018 roku (Dz.U.2019, pozycja 1000) o ochronie danych osobowych nakłada obowiązek podjęcia wielu działań podczas tworzenia, przechowywania danych, gwarantując tym samym prawo do zachowania prywatności osób, które te dane dotyczą, miedzy innymi organizacyjnych oraz technicznych w zakresie ochrony przetwarzanych informacji i danych osobowych. W świecie cyfryzacji coraz większego znaczenia nabiera bezpieczeństwo i ochrona informacji, więc znalazło i to swój wyraz w przepisach dotyczących ochrony danych osobowych [66].

Omawiana ustawa ma zastosowanie w organach państwowych, samorządach terytorialnych, czy też innych państwowych i komunalnych organizacjach oraz w podmiotach niepaństwowych, ale realizujących zadania publiczne. Ustawa ma również zastosowanie wśród osób fizycznych i prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, a przetwarzających dane osobowe. Dodatkowo, dotyczy podmiotów, których siedziba lub miejsce zamieszkania są poza

terytorium Rzeczypospolitej Polskiej, a przetwarzają one dane dotyczące osób fizycznych zamieszkujących na terytorium Polski [82].

Ustawa o rachunkowości

Ustawa z dnia 17 stycznia 2019r. o rachunkowości (DZ.U.2019, poz.351) określa wymagania i obowiązki w zakresie bezpieczeństwa informacji osób prowadzących księgi rachunkowe, przy użyciu systemów informatycznych. Ustawa szczególny nacisk kładzie na bezpieczeństwo danych podczas zapisu elektronicznego oraz dotychczas obowiązującego zapisu tradycyjnego.

Art. 71.1. w/w ustawy wskazuje, iż dokumenty powinny być przechowywane w należyty sposób, tzn. z uwzględnieniem ochrony przed niedozwolonymi zmianami, uszkodzeniem, rozpowszechnieniem czy też zniszczeniem. Określa szczegółowe zasady przechowywania, prowadzenia i udostępniania osobom trzecim ksiąg rachunkowych, sprawozdań finansowych oraz dokumentów inwentaryzacyjnych.

Z kolei Art.72.2. wskazuje na formy zapewniające ochronę danych w księgach rachunkowych, przy użyciu sprzętu informatycznego, które powinny wykorzystywać przedsiębiorstwa. Mowa tutaj o:

- ✓ Wykorzystaniu środków ochrony zewnętrznej
- ✓ Użyciu odpornych na zagrożenia nośników danych
- ✓ Regularnym tworzeniu kopii zapasowych danych zapisanych na nośnikach, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości
- ✓ Zapewnieniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości, stosując odpowiednie rozwiązania programowe i organizacyjne [62].

Ustawa reguluje również sposób przechowywania dokumentów inwetaryzacyjnych, mianowicie:

- ✓ W macierzystej jednostce organizacyjnej, w formie oryginalnej w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych
- ✓ Poza jednostką macierzystą, gdy dokumenty zostaną przekazane innej jednostce, która świadczy usługi w zakresie przechowywania dokumentów [62].

Ustawa o informacjach niejawnych

Dnia 15 marca 2019r. została znowelizowana ustawa o ochronie informacji niejawnych z przeznaczeniem ograniczenia dostępu do pewnych kategorii informacji i objęcia ich specjalnym systemem bezpieczeństwa. Mowa tutaj o podmiotach, które mogłyby wykorzystać informację w sposób zagrażający podstawowym interesom

państwa, interesom obronności czy bezpieczeństwa obywateli. Tabela 10 określa następujące podmioty, które zobowiązane do przestrzegania ustawy.

Tabela 10. Podmioty, zobowiązane do przestrzegania w/w ustawy

Organy władzy publicznej
Jednostki organizacyjne podlegające Ministrowi Obrony Narodowej
Narodowe Banki Polskie
Jednostki organizacyjne podlegające organom władzy publicznej
Przedsiębiorcy mający dostęp do informacji niejawnych lub mogących mieć w przyszłości zadania związane z dostępem do informacji niejawnych

Źródło: Opracowanie własne na podstawie [23]

Do sytemu ochrony informacji niejawnych zaliczamy:

- ✓ Bezpieczeństwo osobowe
- ✓ Bezpieczeństwo fizyczne
- ✓ Bezpieczeństwo obiegu dokumentów
- ✓ Bezpieczeństwo przemysłowe
- ✓ Bezpieczeństwo teleinformatyczne

Ustawa o informacjach niejawnych ma szczególne znaczenie dla przedsiębiorców, którzy mają dostęp do informacji niejawnych z związku z wykonywaniem umów lub też zadań wynikających z przepisów prawa. Omawiane podmioty muszą posiadać zdolność do ochrony takich informacji. Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne" jest świadectwo bezpieczeństwa przemysłowego wydana przez ABW lub też SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego. Świadectwa te obejmują również podwykonawców umów, gdy ich wykonywanie wiąże się z dostępem do informacji niejawnych [82].

Ustawa o zwalczaniu nieuczciwej konkurencji

Częstym zjawiskiem przy podpisywaniu umów, postępowaniu ofertowym, negocjacjach, współpracy handlowej czy opracowywaniu klauzuli poufności jest powoływanie się przedsiębiorców na zapisy Ustawy z 16 maja 2019 (Dz.U.2019 poz.1010) o zwalczaniu nieuczciwej konkurencji. Na gruncie Ustawy wskazano znaczenie tajemnicy przedsiębiorstwa i co będzie ją stanowić. Przez tajemnicę przedsiębiorstwa rozumianą, jako: *„wiadomości trwale użytkowane w przedsiębiorstwie, tzn. kolekcje wzorów, modele wytworów, rysunki krawieckie lub inne, tajna lista klientów, zbiór adresów dostawców, znajomość pewnej korzystnej metody produkcji, nowe pomysły czy wynalazki"* [82].

Jednak w rozważaniach na temat regulacji prawnych służących ochronie tajemnicy przedsiębiorstwa warto zwrócić uwagę na aktualnie obowiązującą ustawę, która traktuje je następująco: *„(...) nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe, organizacyjne lub inne informacje posiadające wartość gospodarczą, co, do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności”* Dz. U. z 2019r., poz.1010 [63].

Natomiast w literaturze przedmiotu [11, 25, 82, 58] przyjmuje się, że tajemnicę przedsiębiorstwa mogą stanowić informacje techniczne, wewnętrzne przedsiębiorstwa, technologiczne, handlowe, które przedsiębiorstwa objęły szczególną ochroną w celu zachowania poufności [58]. Zatem, zaliczamy do nich:

- ✓ strategie przedsiębiorstwa, treść umów, metody kontroli, jakości, wynalazki w tym nieopatentowane, wzory użytkowe, lista klientów, informacje dotyczące planów wydawniczych przedsiębiorstwa, dane zawarte w PIT-05 i F-01 sprawozdania finansowe o aktywach i pasywach oferentów, zysk, koszty działalności, dochód, plany finansowe, straty, dane związane z wielkością produkcji i sprzedaży, źródła zaopatrzenia i zbytu [25, 82].

Nie zastosowanie się do należytego potraktowania tajemnicy przedsiębiorstwa może doprowadzić nawet do zlikwidowania organizacji gospodarczej.

Według W.J. Katnera tajemnica przedsiębiorcy to *„informacje o działalności gospodarczej, których się nie ujawnia w trosce przed konkurencją, natomiast tajemnica przedsiębiorstwa koncentruje się na samej działalności firmy”* [43]. Aby informacja została zaliczona do kategorii tajemnicy przedsiębiorstwa musi spełniać następujące warunki:

- powiązanie z danymi technicznymi, technologicznymi, handlowymi, organizacyjnymi przedsiębiorstwa
- informacji o charakterze poufnym, które nie zostały i nie będę podane do wiadomości publicznej innym osobom
- wynalazki, również te nieopatentowane, wzory użytkowe, zasady organizacji pracy, listy klientów
- dysponowanie przez zarząd organizacji prawami do dóbr materialnych tzn. prawa do programu utworzonego przez pracownika [16].

Niniejsza ustawa wskazuje na odpowiednie zabezpieczenia informacji poufnej przez przedsiębiorcę. Należy również wziąć pod uwagę fizyczne środki ochrony,

nadawanie dokumentom o klauzuli „niejawne", uwarunkowanym wewnątrz zakładowym powiązaniem dokumentów w organizacji (stosowanie klauzuli do zawartych już umów czy porozumień) [83].

Konkludując należy stwierdzić, że uzyskanie informacji przez określoną grupę osób w organizacji nie powoduje utraty poufności informacji gdyż, w orzeczeniu Sądu Najwyższego z dnia 5 września 2001 można znaleźć zapis *"Tajemnica nie traci zaś swego charakteru przez to, że wie o niej pewne ograniczone koło osób, zobowiązanych do dyskrecji w tej sprawie, jak pracownicy przedsiębiorstwa lub inne osoby, które przedsiębiorca wtajemnicza w proponowany im interes"* [82].

Jeśli przedsiębiorca uznał pewne informacje za tajemnicę przedsiębiorstwa, zobowiązany jest podjąć określone działania w celu zachowania poufności tych informacji np.: zanim pracownik zacznie pracować powinien podpisać potwierdzenie zapoznania się z zakresem informacji objętych tajemnicą przedsiębiorstwa. Powyższy obowiązek wiąże pracownika nie tylko przez okres pracy, ale i po ustaniu stosunku pracy do trzech lat, chyba, że umowa stanowi inaczej. To w interesie pracodawcy jak i pracownika jest dokonanie określonych ustaleń w obszarze ochrony tajemnicy przedsiębiorstwa.

Znaczenie tego elementu podkreśla również S. Sołtysiński, [84] który twierdzi, że posługiwanie się klauzulami poufności przez dysponenta tajemnicy stanowi dowód przedsiębrania niezbędnych działań, które mają wpływ na zachowanie tajemnicy.

Kodeks karny

Katalog aktów prawnych regulujących obszar nadużyć podlegających karze jest dość obszerny jednak w pracy przytoczono tylko wybrane z nich. Dz. U. 2020 poz. 1444 Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 lipca 2020 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks karny oraz niektórych ustaw formułuje zasady odpowiedzialności karnej za nadużycie, jakim jest ujawnienie informacji. Zidentyfikowano następujące nadużycia karne za:

- ✓ hacking komputerowy –Art.267
- ✓ nieuprawnione przechwycenie informacji podczas podsłuchu komputerowego- Art.267
- ✓ niszczenie informacji-Art.268
- ✓ fałszerstwo dokumentów-Art.270
- ✓ nielegalne uzyskanie programu komputerowego-Art.278

- ✓ oszustwa telekomunikacyjne-Art.285
- ✓ oszustwa komputerowe -Art. 287
- ✓ paserstwo programu komputerowego –Art.291 [85].

Podstawową determinantą zaaplikowania do przedsiębiorstwa idei ochrony informacji jest przypis kodeksu karnego zawartego w Art. 267 stanowiący, że korespondencje są tajne i kto bez stosownego uprawnienia *„uzyska dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególnie jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Podobna kara grozi również za uzyskanie nieuprawnionego dostępu do całości lub części systemu informatycznego lub też posługiwanie się urządzeniami do podsłuchu* [65].

Kodeks karny zawiera, więc kanony, jakimi powinien się kierować każdy, kto ma dostęp do informacji niejawnych o klauzuli „tajne" bądź „ściśle tajne", „zastrzeżone" lub też „poufne" oraz pozostałych informacji.

Kodeks Pracy

W Obwieszczeniu Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 18 czerwca 2020 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks pracy można znaleźć obszar związany z bezpieczeństwa informacji. Mianowicie kodeks pracy reguluje zapisy związane z ochroną danych osobowych, jakich pracodawca może żądać od kandydata na stanowisku pracy np.: imię, imiona rodziców, data urodzenia, miejsce zamieszkania, wykształcenie. Pracodawca może zażądać również przebiegu dotychczasowego zatrudnienia, numeru pesel, daty urodzin dzieci pracownika, fotografii, świadectw pracy z poprzednich miejsc pracy lub innych dokumentów potwierdzających czas zatrudnienia. Ponadto pracodawca ma również prawo zażądać dokumentów potwierdzających kwalifikacje zawodowe wymagane do oferowanej pracy, orzeczenia lekarskiego stwierdzającego brak przeciwskazań do wykonywania pracy na określonym stanowisku. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą i pracodawca ma pełne prawo poprosić o zweryfikowanie z oryginałem danych osobowych.

Zasady postępowań pracownika wobec przedsiębiorstwa w kontekście ochrony informacji oraz sposobu ochrony tajemnicy reguluje kodeks pracy w Art. 100δ1 [63].

1.8. Ocena zaleceń zawartych w normach z zakresu bezpieczeństwa informacji

Obszerność zagadnień związanych z ochroną informacji w jednostkach biznesowych doprowadziła do usystematyzowania i sformułowania wymagań w postaci międzynarodowych norm. Proces ten rozpoczął się pod koniec lat 80-tych XX wieku. z tego też względu obecne opracowania zawierają praktyczne wskazówki, co do dobrych praktyk, czy też oceny zabezpieczeń systemów teleinformatycznych.

Obszar standardów z zakresu systemowego zarządzania bezpieczeństwem informacji ze szczególnym uwzględnieniem rodziny norm ISO/IEC 27000, jest tematem niniejszego podrozdziału.

Wykorzystanie norm ISO/IEC w ochronie danych osobowych

Podczas przetwarzania danych osobowych zgodnie z RODO można skorzystać z następujących norm [21, 23, 29, 31,82].

Zarządzanie bezpieczeństwem informacji

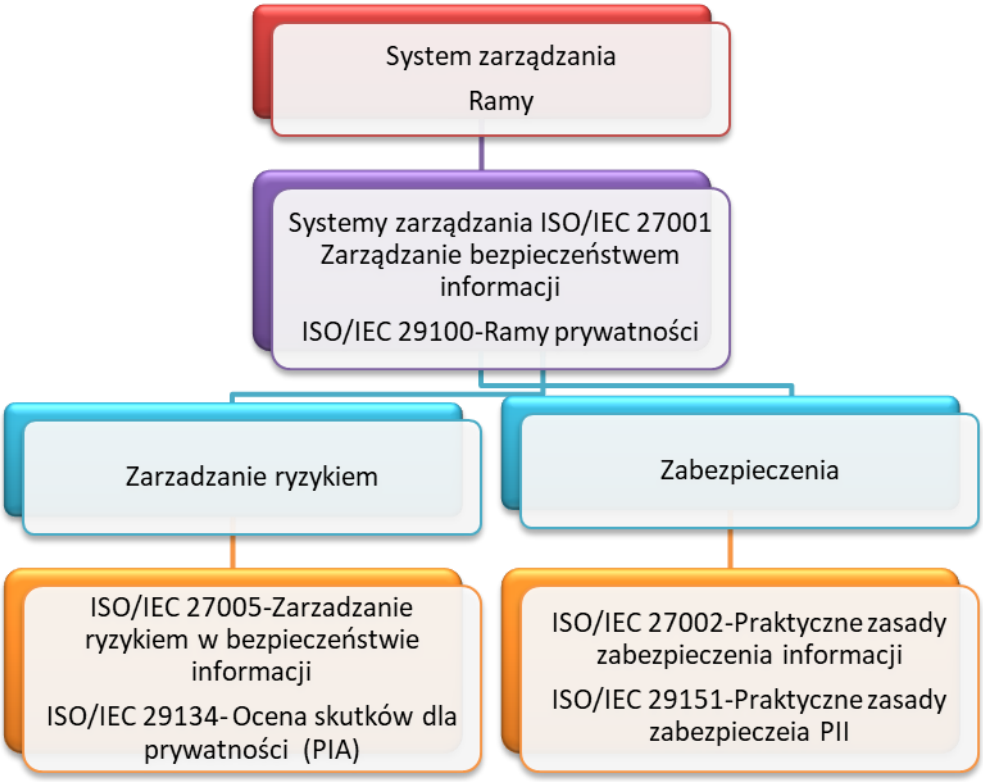
Problematyką związaną z bezpieczeństwem informacji i mechanizmami, które powinny być zastosowane w organizacji a odnoszących się do zarządzania bezpieczeństwem informacji zawierają normy [13, 21, 23, 44, 52, 82, 86, 87, 103, 104].

Szczególnie praktyczne wskazówki dla organizacji dotyczące skutecznego zarządzania ryzykiem związanym z bezpieczeństwem informacji znajdują się w normach [44]. Jak można przeczytać na stronie Polskiego Komitetu Normalizacyjnego ISO/IEC 27005 *jest jedną z kilkunastu norm z rodziny ISO/IEC 27000 stanowiących zestaw narzędzi dotyczących cyberryzyka. Pozostałe normy z tego zakresu obejmują ochronę informacji w chmurze, bezpieczeństwo informacji w telekomunikacji i sektorach użyteczności publicznej, cyberbezpieczeństwo, audyt SZBI i inne* [88].

Normy ISO miejące związek z zarządzaniem ryzykiem.

Standardy przedstawiające wskazówki dotyczące wyboru i stosowania technik oceny ryzyka w różnych sytuacjach oraz wytyczne związane z zarządzaniem ryzykiem, na które narażone są organizacje zawarte zostały w normach [31, 89, 105, 106]. Z wytycznych może skorzystać każda organizacja bez względu na jej kontekst.

Normy z serii 29100 są ściśle połączone z rodziną norm z serii 27000. Na reguły dotyczące zarządzania bezpieczeństwem informacji nakładają się kanony dotyczące wymagań prywatności, w tym ochrony danych osobowych (PII).



Rysunek 7. System zarządzania - Ramy prywatności
Źródło: Opracowanie własne na podstawie [81].

Ramy prywatności

Standardy [90, 91, 92, 107,109] określają proces zarządzania ryzykiem prywatności i wskazują, że jednym z jej wyników może być ocena wpływu na prywatność, która jest składnikiem zarządzania ryzykiem, skierowanym na gwarantowanie zgodności z wymogami prawa odnośnie ochrony prywatności i danych. Norma określa następujące ramy prywatności.

- definjują wspólne nazewnictwo dotyczące prywatności
- opisują wymogi w zakresie ochrony prywatności
- opisują wymogi dla tworzenia polityki prywatności oraz zasad i obowiązków dla ochrony danych
- wskazują na mechanizmy kontroli prywatności
- identyfikują wymogi szacowania ryzyka, ocenę skutków, dla danych podmiotów
- zapobiegają przetwarzaniu nieadekwantynych danych w stosunku do celu ich przetwarzania
- określają metody ograniczenia możliwości identyfikacji osób
- wskazują podstawowe zasady prywatności-11 pryncypiów
- definjują uczestników przetwarzania danych identyfikujących osoby PII
- określają uczestników przetwarzania i ich role tzn. podmiot danych, administrator danych, podmiot przetwarzający

Rysunek 8. Ramy prywatności ISO/IEC 29100

Opisane ramy prywatności mają zastosowanie w technologiach informatycznych wykorzystywanych, do przetwarzania danych oraz rozwoju systemów zarządzania prywatnością. Norma jest przeznaczona dla organizacji uczestniczących w projektowaniu, opracowywaniu i testowaniu oraz administrowaniu systemów i usług informatycznych, które wymagają stosowania mechanizmów kontroli prywatności do przetwarzania PII.

Zarządzanie ryzykiem

Sposób postępowania w celu zapewnienia bezpieczeństwa informacji przedstawiają standardy [13,31,44, 102].

Norma [31] przedstawia schemat procesu zarządzania ryzykiem w poszczególnych etapach. Należą do nich: ustanowienie kontekstu, szacowanie ryzyka (tzn. identyfikowanie ryzyka, analiza ryzyka ocena ryzyka), postępowanie z ryzykiem, monitorowanie ryzyka, informowanie i konsultowanie ryzyka.

Na fundamencie tego standardu zostały przyjęte wytyczne odnośnie zarządzania ryzykiem tak, aby zapewnić należyty poziom bezpieczeństwa informacji. Szerzej zostały one zawarte w standardzie normatywnym [44]. Norma nie wskazuje żadnej konkretnej metody szacowania ryzyka, dlatego też wybór należy do organizacji i zależy od zakresu SZBI (systemu zarządzania bezpieczeństwem informacji), w tym rodzaju przetwarzanych informacji (aktywa informacyjne). Innym ważnym czynnikiem może okazać się rodzaj prowadzonej działalności.

Opisane zasady z całą pewnością mogą być stosowane przy wymaganiach dotyczących szacowania ryzyka naruszenia praw i wolności osób, których dane dotyczą (PIA), a które, z kolei są zawarte w art. 24, 25, 32 i 35 RODO.

Standard [44] określa metodyki szacowania ryzyka, które w większości przypadków dedykowane są przedmiotowi szacowania ryzyka, jakim jest ocena skutków w organizacji w nawiązaniu do przetwarzania różnych informacji, i danych osobowych.

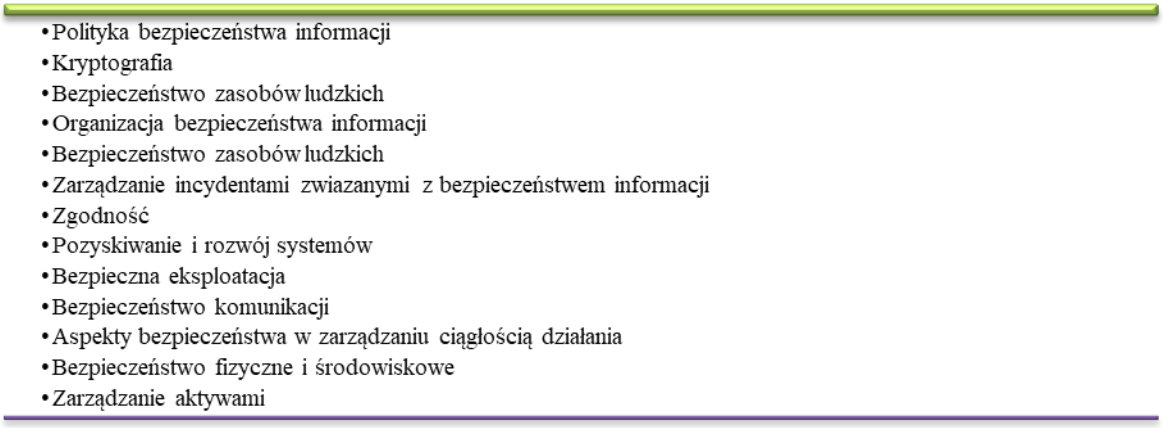
Wytyczne dla szacowania ryzyka

- Problematyka związana z bezpieczeństwem informacji i szacowaniem ryzyka w organizacji w zawierają normy [93]. Zawierają one wytyczne dla szacowania ryzyka w odniesieniu do PIA oraz wskazówki do przeprowadzenia procesu szacowania skutków dla prywatności osoby, której dane dotyczą oraz zawartość raportu PIA.

- ISO/IEC TR 13335-1 (PN-I-13335-1: 1999) uwzględnia wytyczne zarządzania bezpieczeństwem systemów informatycznych, omawiając przy tym terminologię i związki pomiędzy pojęciami, jak i podstawowe modele zarządzania [90].
- ISO/IEC TR 13335-2 (PN-I-13335-2: 2003) opisuje szczegółowo planowanie i zarządzanie bezpieczeństwem systemów informatycznych. Standard określa cel stosowania polityki bezpieczeństwa informacji, wymagania w obszarze bezpieczeństwa, omawia zasady poprawnego przeprowadzania analizy ryzyka oraz reagowania na pojawiające się incydenty oraz przedstawia plan zabezpieczeń [94].
- ISO/IEC TR 13335-3 jest opisem technik zarządzania bezpieczeństwem systemów informatycznych. W normie można znaleźć informacje dotyczące trójpoziomowej polityki bezpieczeństwa, przeprowadzając analizę ryzyka oraz implementację zabezpieczeń. Ponadto, norma opisuje, jak reagować na różne incydenty zagrażające bezpieczeństwu informacji [95].
- ISO/IEC TR 13335-4 omawia zagadnienia dotyczące wyboru właściwych zabezpieczeń. W normie przedstawiono klasyfikacje i charakterystykę różnych form zabezpieczeń, wskazano na możliwość wyboru zabezpieczeń ze względu na rodzaj zagrożenia lub systemu. Norma przedstawia szczegółowe zalecenia wynikające z innych norm oraz branżowych opracowań [95].
- ISO/IEC TR 13335-5 opisuje sposoby zabezpieczeń dla połączeń z sieciami zewnętrznymi. Omówiono w niej metody zabezpieczenia, połączenia sieci wewnętrznej z zewnętrzną [44].

Dobór zabezpieczeń

Norma [21] określa standardy bezpieczeństwa informacji, pokazując praktyczne zalecenia postępowania w przedsiębiorstwach. Norma w sposób merytoryczny opisuje wybór wdrożenia i zarządzania zabezpieczeniami biorąc pod uwagę środowisko i otoczenie, w którym organizacja funkcjonuje. Omawiana norma jest rozwinięciem normy [44]. Standard określa 114 zabezpieczeń oraz opisuje 35 głównych kategorii prewencyjnych. Każda główna kategoria zabezpieczeń opisuje cel stosowania zabezpieczenia wskazując, co najmniej jedno zabezpieczenie, które należy zastosować [81].



Rysunek 9. Kategorie zabezpieczeń informacji wg. standardu ISO/IEC 27002

1.9. Wnioski

Wśród ogólnie dostępnych opinii informacja stała się towarem niezwykle cennym. Można stwierdzić, że kto ma teraz władzę i pieniądze to wcześniej miał informację. Każde państwo poprzez swój wywiad dążyło do zdobycia informacji o potencjale gospodarczym kraju, funkcjonowaniu różnych instytucji wewnątrz innych państw. Posługiwali się oni środkami, które bezpośrednio lub pośrednio pomogły inwigilować cudze obszary.

Obecnie szacuje się, że ok 80% informacji zdobywanych przez konkurencyjną firmę pochodzi z ogólnie dostępnych źródeł, tzn. z białego wywiadu. Z kolei około 15% informacji zalicza się do informacji jawnych, jednak dotarcie do nich nie jest takie łatwe. Natomiast 5% informacji zdobywa się metodą polegająca na szpiegostwie przemysłowym [96].

Korzystając ze źródeł informacji można pozyskać te o firmach poprzez prasę ogólną i specjalistyczną, książki, radio telewizję, banki danych, opisy patentowe. Źródłem informacji mogą być również publikacje z wynikami badań przedsiębiorstwa przeprowadzone na zlecenie prywatnych organizacji. Wskazać także należy na obowiązkowe publikowane wyników w źródłach prawniczych, takich jak: wyroki arbitrażu gospodarczego, wpisy do rejestrów sądowych, wpisy do ksiąg wieczystych. Poza tym informacje można pozyskać poprzez źródła nieformalne, tzn. zbierając je od konkurentów, dostawców, podwykonawców, kandydatów do pracy. Bardzo dobrym źródłem informacji są targi, wystawy salony, kongresy, konferencje oraz uczestnictwo w komitetach czy komisjach [25].

Wobec powyższego w gospodarce zauważalny jest popyt na informacje. Ze względu na prywatny charakter wielu informacji, w niektórych przypadkach może dojść do jej sprzedaży i zakupu, czyli tzw. handlu informacją. Z jednej strony można kupić ją od wyspecjalizowanych oferentów, ale i też można sprzedać ją oferentowi [25].

Kilkadziesiąt lat temu najważniejsze informacje można było znaleźć w sejfach, natomiast dzisiaj najpowszechniej używanym skarbcem wiedzy jest pamięć komputer. Dlatego też niezwykle istotnym zadaniem staje się zabezpieczenie zgromadzonych w niej danych przed ich utratą, nieuprawniona modyfikacją lub dostępem.

Utrata informacji zawarta w pamięci komputera może nastąpić podczas zdarzenia losowego np.: pożarach czy powodzi, nieostrożności użytkownika (np. omyłkowego skasowania danych) lub też typowo działań przestępczych (np. kradzieży komputera z całą jego zawartością lub wprowadzeniu do komputera wirusa niszczącego całą zawartość pamięci). Szczególną grupą wirusów są konie trojańskie, które są zaprogramowane tak by udawały przydatne oprogramowanie, a w rzeczywistości łamią zabezpieczenia komputera, ogromnie szkodząc organizacji gospodarczej. Podsumowując, należy również wspomnieć o szkodliwym oprogramowaniu, jakim są robaki zajmujące pamięć a znacznie obniżające przepustowość sieci, powodując zawieszanie się komputera.

Aby więc chronić zawarte informacje w pamięci komputera zaleca się oprócz stosowania pewnych reguł i zasad postępowania, również podjęcie zabiegów specyficznych (zachowania ostrożności podczas kasowania plików, nieinstalowania programów niewiadomego pochodzenia, czy też nieotwieranie e-maili pochodzących od nieznanych adresów). Ze względu na pojawiające zagrożenia warto zwracać uwagę na niepozostawianie niezabezpieczonego komputera, włączonego do sieci, a także zapoznanie się z listą zabezpieczeń technicznych, organizacyjnych czy zabezpieczeń teleinformatycznych.

Zdaniem autorki pracy złe oprogramowanie, czy też błąd ludzki może być przyczyną ogromnych strat finansowych w przedsiębiorstwie. Większość tych danych jest wynikiem wieloletnich badań, doświadczenia przedsiębiorców, biznesmenów, czy naukowców z wszystkich gałęzi gospodarki światowej. Ponieważ informacja jest podstawą działalności każdej organizacji, warto zwrócić uwagę na prawidłowe funkcjonowaniu jej w danej jednostce. Dobrze przeprowadzona analiza pozyskanych informacji gwarantuje przewagę na rynku zbytu oraz wzrost gospodarczy, dzięki któremu przedsiębiorstwo będzie miało lepszą pozycję wśród konkurujących firm.

Zatem, niezbędne jest zachowanie odpowiedniego poziomu bezpieczeństwa informacji, które koncentruje się na głównych atrybutach bezpieczeństwa tj.; poufność, dostępność, autentyczność i integralność, rozliczalność, niezawodność, i spójność, które rozpatruje się w obszarach bezpieczeństwa fizycznego, prawnego, administracyjno-osobowego, jak również teleinformatycznego.

Współczesna organizacja zobligowana jest do dbania o swoje informacje, gdyż one są jednym z czynników stanowiących przewagę konkurencyjną nad innymi podmiotami. Bezpieczeństwo informacji jest nie tylko normą, lecz koniecznością oraz obowiązkiem [97].

Z pomocą dla organizacji świadomych znaczącej roli bezpieczeństwa i ochrony informacji w procesach realizacji misji i celów, obsługi klienta, przychodzi międzynawowy akt normatywny ISO/IEC 27001: 2017, stanowiący zbiór zaleceń, wymagań oraz dobrych praktyk, których zaimplementowanie do systemu bezpieczeństwa informacji gwarantuje jego niezawodność dla klientów, dostawców i osób trzecich. Nietrudno dostrzec, że dużą zaletą tego standardu jest kompleksowe podejście do bezpieczeństwa informacji.

Reasumując rozważania zawarte w bieżącym rozdziale, należy zwrócić szczególną uwagę na zaistnienie problemu z punktu widzenia ustaw, norm czy rozporządzeń. Bowiem mnogość dokumentów powoduje, że przedsiębiorca nie jest w stanie zaznajomić się z nimi wszystkimi. Dodatkowo chaos informacyjny spowodowany tak dużą ilością wymagań powoduje, że przedsiębiorcy nie wiedzą gdzie ich szukać oraz czy są one jeszcze aktualne. Nie bez znaczenia jest też ciągle rosnącą liczba zagrożeń. Katalog ten nie jest, więc zamknięty i z biegiem czasu identyfikuje się nowe zagrożenia, dotychczas nieokreślone, a jednak pojawiające się w przedsiębiorstwach. Stan taki powoduje konieczność przeciwdziałania nowym technikom ataku. Choć nie ma idealnych zabezpieczeń, to jednak te już istniejące muszą ciągle być doskonalone i uaktualniane zgodnie zasadą cyklu Deminga: Planuj-Wykonuj-Sprawdzaj –Działaj.

2. SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI REDUKUJĄCE RYZYKO UTRATY INFORMACJI W PRZEDSIĘBIORSTWIE

2.1. Wprowadzenie do problematyki systemu zarządzania bezpieczeństwem informacji

Nawet najnowocześniejsze i najbardziej chronione jednostki gospodarcze świata nie posiadają stu procentowego systemu bezpieczeństwa informacji. Mimo tego, iż wyspecjalizowanymi urządzeniami, programami, inwestycjami w techniczne środki ochrony, zdecydowanie można podnieść poziom bezpieczeństwa, to jednak chronią one tylko określony obszar cennych zasobów. Rozwój technik informatycznych daję coraz więcej możliwości włamywaczom wykorzystującym narzędzia, które uniemożliwiają złamanie potencjalnie dobrze chronionych systemów [9].

Dzięki dynamicznemu rozwojowi technologii telekomunikacyjnej, systemy informatyczne przekazują informację w czasie rzeczywistym. Tak szybkie porozumiewanie się powoduje jednak powstanie zagrożeń dotychczas często niezidentyfikowanych. Dla osób, które zajmują się bezpieczeństwem informacji w jednostkach organizacyjnych codziennością stało się otrzymywanie informacji o próbach włamań do systemów komputerowych. Z drugiej strony środki masowego przekazu, stale informują o kolejnej słabości, wadzie i mankamencie w systemach operacyjnych, czy też szkodliwym oprogramowaniu niespełniającym podstawowych wymagań w zabezpieczeniach. Wyniki analizy certyfikacji ISO/IEC 27001 w sektorze przemysłu wskazują, że wielu przedsiębiorców nie wdrożyło w ogóle albo tylko częściowo zaproponowane rozwiązania, dlatego też zauważa się sytuację, w której 80% różnych informacji jest wykradana przez personel organizacji. Organizacje nie chcąc zostać wyłączonym z rynku, zmuszone są uwzględniać w swoich strategiach elementy BI.

Ponieważ zapewnienie bezpieczeństwa informacji oraz redukcja ryzyka (poprzez eliminowanie zagrożeń) związane są z dużym wyzwaniem dla wielu organizacji, które ją wdrażają lub deklarują konieczność wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI z angielskiego Information Security Management System ISMS) to należy bliżej poznać konstrukcje takich systemów.

SZBI to „część całościowego systemu zarządzania, opartego na podejściu wynikającym z ryzyka biznesowego, dotyczącego ustanawiania, wdrożenia, eksploatacji, monitorowania, utrzymania i doskonalenia systemów bezpieczeństwa informacji" [17] [16][15, 48]. Uwagę zwraca sformułowanie „podejścia wynikające z ryzyka biznesowego", które odnosi się do zarządzania ryzykiem (risk management) rozumianego, jako „skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka", który pełni kluczową rolę w planowaniu i dalszym funkcjonowaniu SZBI [82]. Działania te dotyczą wprowadzania zabezpieczeń w technologiach teleinformatycznych i koncentrują się na skutecznym i odpowiednio dobranym zarzadzaniu organizacyjnym i technicznym [16].

Norma ISO/IEC 27001 określa jak zaprojektować, utrzymać i ulepszać SZBI w przedsiębiorstwie. Zaimplementowanie dobrych praktyk do systemu bezpieczeństwa informacji gwarantuje jego niezawodność dla partnerów handlowych, dostawców, czy potencjalnych kontrahentów.

Międzynarodowy standard zaleca kompleksowe podejście do bezpieczeństwa informacji, obejmujące wymagania związane z ustanowieniem i zarządzaniem SZBI, niezbędną dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami SZBI, przeglądami SZBI oraz ciągłym doskonaleniem SZBI. Wszystkie zdefiniowane wymagania winny być spełnione, aby organizacja mogła osiągnąć pewien akceptowalny poziom bezpieczeństwa [17].

W omawianej normie znajdują się obszary skategoryzowane, które mają znaczący wpływ na bezpieczeństwo posiadanych i przetwarzanych informacji. Mowa tutaj o zasadniczej roli aktualnej polityki bezpieczeństwa, obowiązującej w przedsiębiorstwie, dobrej organizacji ochrony informacji, zarządzaniu aktywami, bezpieczeństwie pracowników, bezpieczeństwie środowiskowym i fizycznym, zarządzaniu sieciami i systemami, pełnej kontroli dostępu, zabezpieczeniach systemu informacyjnego, monitorowaniu i kierowaniu powstałymi incydentami w sferze bezpieczeństwa informacji, kierowaniu możliwością ciągłego funkcjonowania oraz zgodnością działania organizacji z prawem i celami, które zamierza osiągnąć.

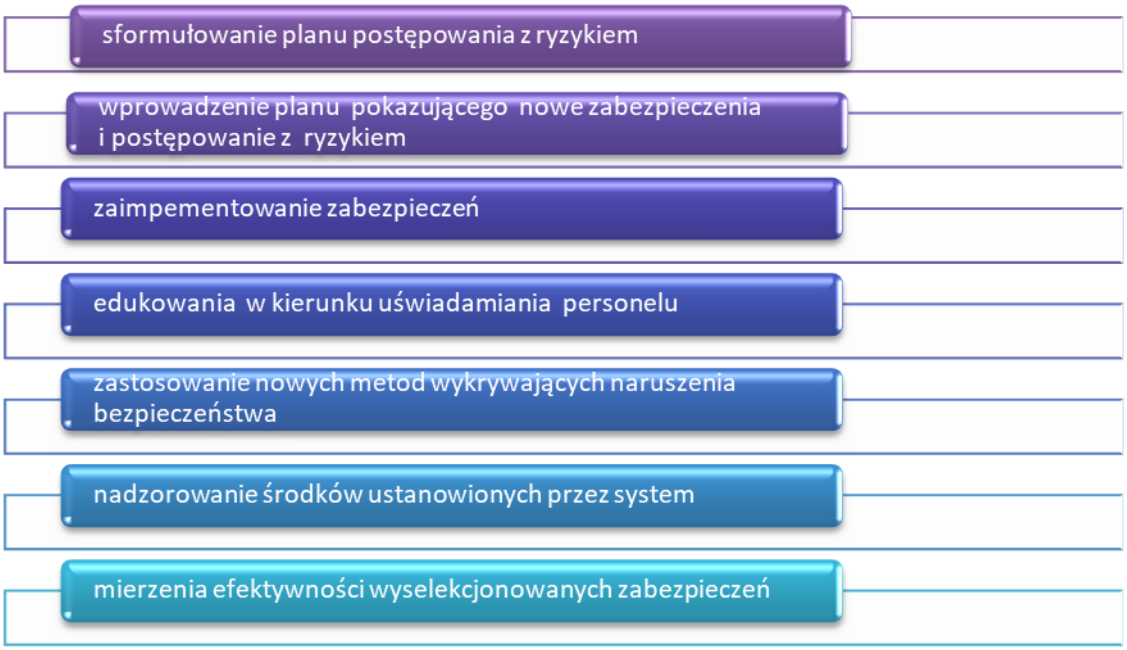
Standard pomaga uświadomić przedsiębiorcom jak poprawnie i należycie ustanowić i zastosować SZBI oraz na co zwracać uwagę, aby wszystkie informacje, które są w posiadaniu danej organizacji były trwale przechowywane, a nie jednorazowo. Dzięki wymaganiom przedstawionym w standardzie dane przedsiębiorstwo może

określić, jak radzi sobie z podstawowymi zasadami dotyczącymi BI, patrząc na fazy związane z działalnością SZBI w organizacji.

Do zasobów SZBI zalicza się całą infrastrukturę, sprzęt informatyczny, urządzenia służące do komunikowania się zasoby fizyczne przedsiębiorstwa, zasoby informacji składowane w dokumentacji oraz bazy danych, systemy operacyjne używane w przedsiębiorstwie, oprogramowanie, aplikacje używane przez personel oraz wszystkie dobra o charakterze niematerialnym (wizerunek i reputacja) [17].

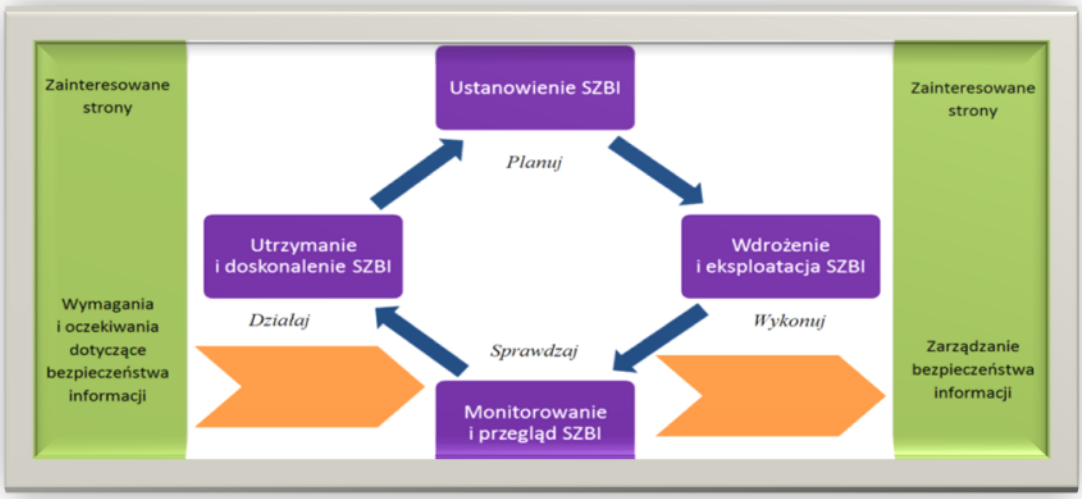
Zastosowanie SZBI ma następujące cele w zakresie bezpieczeństwa osobowego, fizycznego, prawnego. Związane są one z identyfikowaniem aspektów zagrażających bezpieczeństwu informacji oraz wprowadzeniem procedur i działań doskonalących. Oto niektóre z nich:

Rysunek 10. Cele systemu zarządzania bezpieczeństwem informacji



Źródło Opracowanie własne na podstawie [98].

Kontynuując, należy wskazać, że norma ISO 27001`: 2017 opiera się na podejściu procesowym, która w sposób klarowny opisuje wymagania dotyczące modelu Planuj – Wykonuj – Sprawdzaj – Działaj, (w skrócie PDCA). Zarysowana koncepcja klasyfikacji wymagań, dotyczących SZBI w modelu PDCA została zaprezentowana na rysunku 11.



Rysunek 11. Sklasyfikowanie wymagań systemu ujęte w modelu PDCA

Źródło: Opracowanie na podstawie [99].

Rysunek 11. prezentuje, w jaki sposób SZBI przyjmuje wymagania BI i oczekiwania zainteresowanych stron, jako wartość wejściową a poprzez dalsze niezbędne działania dostarcza wartość wyjściową BI, gdzie są już spełnione oczekiwania organizacji.

Model PCDA może być stosowany z całą pewnością przez każdą jednostkę organizacyjną, niezależnie od charakteru jej działalności, wielkości, czy też statusu prawnego. Postanowienie o wprowadzeniu SZBI jest decyzją strategiczną dla każdego przedsiębiorstwa. Na takie ustalenie mają wpływ jej potrzeby i cele biznesowe, wymagania bezpieczeństwa, realizowane procesy oraz sama wielkość i struktura organizacji. Zmianom podlegają obszary w każdej organizacji, dlatego też należy modernizować systemy je wspomagające. Wdrożenie SZBI jest wynikiem potrzeb organizacji, dlatego też wymaga się, aby system zarządzania był rozpatrywany w kontekście systemowym lub procesowym [9]. Model, o którym mowa w normie powinien być stosowany dla całej struktury procesów SZBI.

2.2. Cele i zadania SZBI

Z założenia, celem każdej organizacji jest zapewnienie bezpieczeństwa informacji, a środkiem wspomagającym jest SZBI, który będzie skuteczny i efektywny, jeśli użytkujący go należycie wprowadzą zmiany w organizacji. Dlatego też oczekuje się uwzględnienia w działaniu elementów uznawanych, jako dobre praktyki.
Należą do nich wymagania z serii ISO/IEC, 27001 które zostały podzielone na zobowiązania.

- **Odpowiedzialność kierownictwa**

W systemie zarządzania BI istotną rolę pełni kierownictwo na wszystkich szczeblach zarządzania, specjaliści oraz pracownicy. Do realizowanych dotychczas obowiązków dochodzą im nowe, związane z poszczególnymi elementami SZBI. Pomaga w tym powstanie specyficznych struktur w organizacji o charakterze czasowym lub stałym. I tak w procesie szacowania ryzyka za określenie celów i akceptowalnego poziomu ryzyka są odpowiedzialni:

- dyrektor generalny -strategia organizacji
- dyrektor działu IT- strategia IT-
- pełnomocnik ds. BI -strategia bezpieczeństwa informacji-
- kierownicy wykonawczy BI- planowanie taktyczne związane z BI-
- zarząd, dyrektorzy wykonawczy -planowanie operacyjne w zakresie BI-

Wielkość organizacji oraz przyjęta strategia dyktuje bezpośrednio i pośrednio zadania związane z bezpieczeństwem informacji. W książce pt.: Systemowe Zarządzanie Bezpieczeństwem Informacji ISO/IEC 27001cyt. ”*proponuje się powołanie zespołu, grupy ds. bezpieczeństwa, która byłby odpowiedzialna za elementy zawarte w SZBI”* [17].
Zatem to kierownictwo organizacji jest zobowiązane do zapewnienia:

- ✓ ustanowienia polityki, celów i zakresu SZBI;
- ✓ określenia zakresu odpowiedzialności w ramach systemu SZBI;
- ✓ informowania organizacji o celach istnienia systemu i przyjętych zasadach;
- ✓ zagwarantowania zasobów dla funkcjonowania systemu uczestnictwa w akceptowaniu ryzyka;
- ✓ określenia kryteriów akceptowania ryzyka;

- ✓ przeprowadzenia audytów wewnętrznych w obszarze SZBI;
- ✓ uczestnictwa w przeglądach SZBI;
- ✓ sformułowania kompetencji, co do personelu [82].

Reasumując to kierownictwo jest zobligowane do ochrony informacji, dlatego też powinno ono działać racjonalnie i roztropnie, aby należycie utrzymać zadawalający poziom bezpieczeństwa i ryzyka na akceptowalnym poziomie.

- **Wewnętrzne audyty**

Istota wdrażania systemu zarządzania niesie ze sobą ryzyko powstania niezgodności, które wynikają z niedoskonałości założeń tego systemu. Z jednej strony system jest narażony na zdarzenia i incydenty związane z bezpieczeństwem, a z drugiej strony błędy popełniane poprzez ludzi. Zatem zasadne będzie posłużenie się audytem w celu wykrywania niezgodności w systemie w sposób regularny i zorganizowany oraz wprowadzenia działań po audytowych.

Norma PN-EN ISO 19011: 2018-08 „Wytyczne dotyczące audytowania systemów zarządzania" podaje definicje audytu, jako systematyczny i niezależny, udokumentowany proces pozyskiwania dowodów i wynikającej z tego obiektywnej oceny w celu wyznaczenia stopnia spełnienia kryteriów BI [100].

W tym kontekście, audyty wewnętrzne (tzw. kontrola wewnętrzna) to niezbędny element systemowego zarządzania BI, a w dodatku jeden z głównych elementów sytemu, utrzymujący ciągłość doskonalenia [100] [17]. I mimo, że jest kosztowny to jednak bardzo skuteczny, jako metoda skłaniająca do wprowadzania rozwiązań w zakresie zarządzania organizacją [90]. Wręcz trudno sobie wyobrazić prawidłowe utrzymanie i rozwój systemu bez audytu na etapie wdrażania i doskonalenia SZBI. Potrzeba dokonywania zmian doskonalących i podnoszących skuteczność związana jest ze wszystkimi elementami procesu, jego planowaniem, wykonaniem, dokumentowaniem i działaniem naprawczym po audytowym. To właśnie audyty stanowią mechanizm ciągłego doskonalenia systemu, ponieważ pozwalają na potwierdzenie zgodności rozwiązań i wyłuszczenie wad systemu. Dzięki wykonaniu audytu organizacja ma świadomość, co ma jeszcze do zrobienia, aby system spełniał zaplanowane ustalenia oraz wymagania normy ISO/IEC 27001.

Definicja audytu wskazuje również na proces dokumentowania, który powinien być przeprowadzany zgodnie z ustalonymi kryteriami, obowiązującymi zestawu polityk, procedur i wymagań stanowiących ideę kontroli [99]. Zakres audytu dotyczy

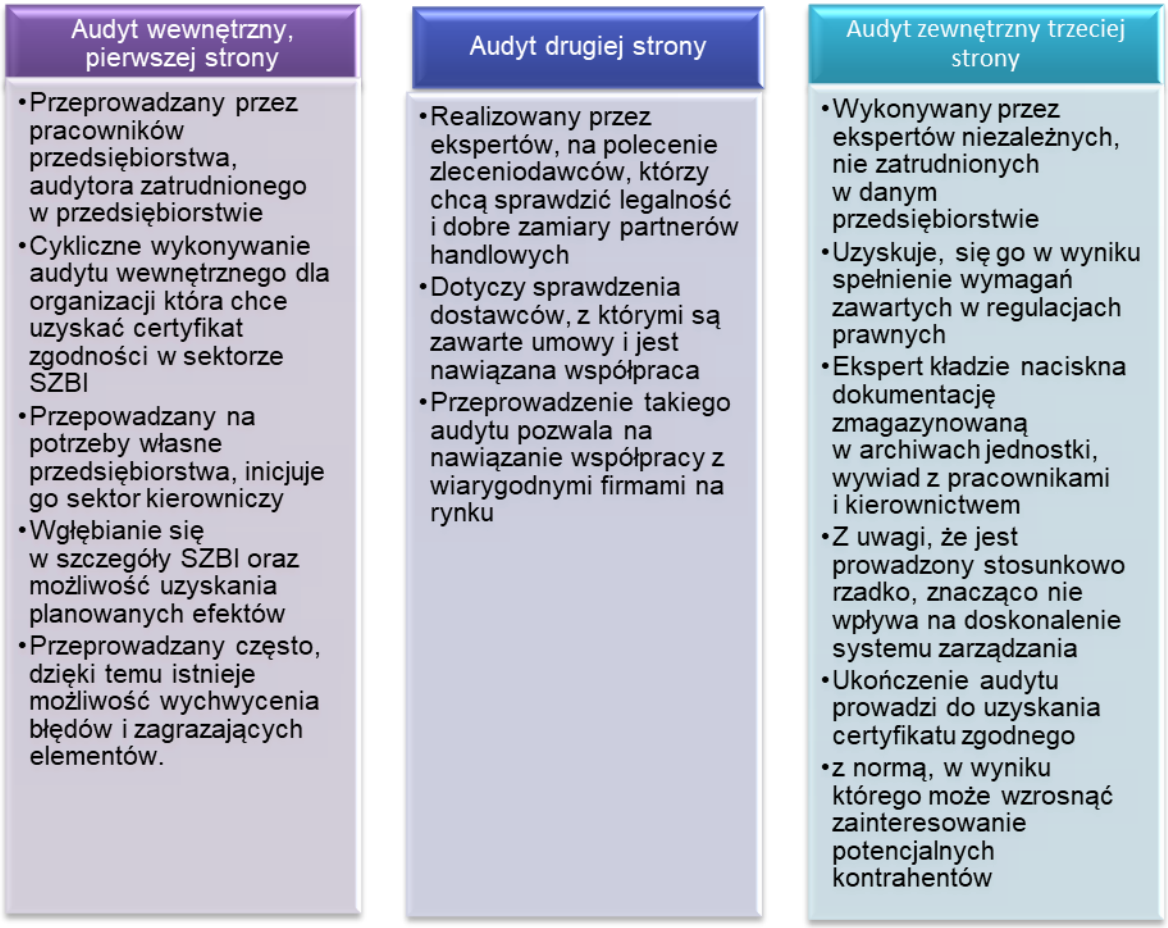
jego obszaru i granic takich jak: fizyczne lokalizacje, jednostki organizacyjne, działania i procesy.

Cele audytu mają za zadanie określić, co ma zostać osiągnięte wskutek procesu i czego mają dotyczyć:

- ✓ określenia zakresu zgodności systemu zarządzania audytowego lub jego części z kryteriami audytu
- ✓ ocenę zdolności systemu zarządzania w celu zapewnienia zgodności wymaganiami prawnymi
- ✓ identyfikację obszarów potencjalnego doskonalenia SZBI
- ✓ ocenę skuteczności systemu zarządzania pod kątem wyspecyfikowanych celów [58].

Audyt powinien cechować się systematycznością, niezależnością oraz udokumentowaniem. Dzięki systematyczności uzyskuje się maksimum korzyści, wykorzystując dostępne środki pozwalające na przeprowadzenie kontroli. Z kolei niezależność oznacza obiektywne i rzetelne podejście do uzyskanych dowodów. Trzecią główną cechą jest dokumentacja, w której opisuje się wykonywane czynności. Natomiast udokumentowane dowody niezgodności powinny zostać, jak najszybciej zweryfikowane i poprawione.

W odniesieniu do wskazań w normie ISO/IEC 27001, to najwyższe kierownictwo zobowiązane jest do zapewnienia sprawnego przebiegu procesu audytów wewnętrznych, w celu dokonania oceny mocnych i słabych stron SZBI. To zespół audytorów wyznacza audytora wiodącego, który ponosi zupełną odpowiedzialność za przeprowadzone badania, we wszystkich fazach audytu. Każda stwierdzona niezgodność powinna zostać precyzyjnie zdefiniowana, wraz ze wskazaniem, dowodów niezgodności[58].



Rysunek 12. Trzy podstawowe rodzaje audytu [58].

W kontekście powyższych uwag szczególnie istotny wydaje się system audytów wewnętrznych organizacji. Ma on opinię skutecznego narzędzia, wykorzystywanego sukcesywnie, do ciągłego doskonalenia organizacji. Szczególnie jest ceniony w branży motoryzacyjnej, spożywczej i innych. Audyt pomaga w zdefiniowaniu kierunków doskonaląco – naprawczych w obszarze BI i rozwoju SZBI [99].

Zatem, uznając istotność i użyteczność procesu audytowania, nieodzownie jest zwrócenie uwagi na respektowanie wszystkich jego etapów. Każdy z tych elementów jest niezbędny i konieczny, aby osiągnąć zamierzony cel. Do podstawowych etapów działań audytowych zalicza się fazy:

- inicjowania audytu;
- przeglądu dokumentacji;
- przygotowania działań audytowych;
- przeprowadzenia działań audytowych;
- udokumentowania działań audytowych;

- udokumentowania rezultatów audytu;
- zakończenia audytu;
- przeprowadzenia działań po audytowych, jako elementu istotnego z uwagi na cel całego procesu audytowego [58].

Fazy przeprowadzenia audytu różnią się od siebie zadaniami i czynnościami, w zależności od wyboru określonego rodzaju audytu. Faza wcześniejsza, łączy się zazwyczaj z fazą późniejszą, dzięki temu można uzyskać najkorzystniejsze dowody z przeprowadzonej kontroli.

Szczegółowe informacje dotyczące faz audytu omówione zostały w pozycjach literaturowych [58] [101] [102].

Dodatkowo oprócz audytów pierwszej, drugiej i trzeciej strony organizacja może być kontrolowana pod względem sytemu, wyrobu, dokumentacji, procesów, operacji, finansów, informacyjnie oraz personalnie.

- **Przeglądy SZBI realizowane przez kierownictwo**

Zapewniając BI należy wykonywać przeglądy, których rolą jest wykrywanie zakłóceń w bezpieczeństwie, identyfikując błędy oraz sprawdzając sprawność już wdrożonych zabezpieczeń.

Podczas przeglądów w gronie najwyższego kierownictwa wymienia się informacje o zarządzaniu SZBI oraz podejmuje się decyzje, co do obszarów zarządzania. W praktyce, nie jest możliwe, aby kierownictwo miało pełną wiedzę na temat głównych elementów zarządzania bezpieczeństwem informacji. Dlatego kadrze zarządzającej z ogromną pomocą (oprócz audytu), przychodzą umocowania prawne w normie, w której znajdujemy zapisy o planowaniu i przeprowadzaniu przeglądów zarządzania. Takie przeglądy powinny odbywać się nie rzadziej niż raz w roku w celu zapewnienia ciągłej poprawności oraz skuteczności. Przegląd winien obejmować ocenę możliwości doskonalenia oraz potrzeby zmian w SZBI, w tym również Politykę Bezpieczeństwa Informacji. Ponadto, przegląd pozwala na sprawdzenie działania systemu, wskazując na potrzeby zmian, i działań korygujących oraz identyfikuje niezgodności, i ich przyczyny. Poza audytami, przeglądy zarządzania są najważniejszymi elementami systemu, które nie pozwalają na jego osłabienie lub brak rozwoju [17, 23].

- **Doskonalenie systemu zarządzania bezpieczeństwem informacji**.

Doskonalenie systemu polega na wdrożeniu nowych zabezpieczeń oraz ich korygowaniu, a w efekcie zapobieganiu występowania niezgodności z wcześniejszych

sytuacji, a także na podstawie wniosków z doświadczeń innych jednostek. Koniecznością, więc będzie poddawanie działań naprawczych ocenie skuteczności poprzez opisane wcześniej audyty wewnętrzne, czy też przeglądy SZBI. Działania zapobiegawcze mogą dotyczyć tematów związanych z incydentami bezpieczeństwa informacji, decyzji podjętych wcześniej na przeglądzie SZBI, czy też audytów wewnętrznych tego systemu i odnotowanych wcześniej niezgodności [60].

- **Dokumentacja Systemu**

Wymagania zdefiniowane w normie PN-EN/IEC 27001: 2017 wskazują na wymagania dotyczące dokumentacji, która powinna być starannie przygotowana oraz wypełniona. Przykładowa dokumentacja winna obejmować:

- ✓ Udokumentowane deklaracje polityki SZBI i jej cele
- ✓ Zakres SZBI
- ✓ Procedury i zabezpieczenia wspomagające SZBI
- ✓ Opis metod szacowania ryzyka
- ✓ Raport z procesu szacowania ryzyka
- ✓ Plan postępowania z ryzykiem
- ✓ Zapisy, które są niezbędne w organizacji do zapewnienia skutecznego planowania, eksploatacji i sterowania procesami bezpieczeństwa
- ✓ Deklarację stosowania.

Dokumenty określone w SZBI powinny w swojej treści zawierać:

- ✓ sposób zatwierdzenia dokumentów zanim trafią one do obiegu;
- ✓ zapewnienie o dostępności dokumentów w miejscach ich zastosowania;
- ✓ sposób identyfikacji zmian (status dokumentów);
- ✓ zobowiązanie do przechowywania, przesyłania i niszczenia dokumentów zgodnie z ich klasyfikacją;
- ✓ zobowiązanie do rozpowszechniania dokumentów;

Wszystkie dokumenty w ramach SZBI powinny być odpowiednio nadzorowane i chronione przez wyznaczoną komórkę w organizacji.

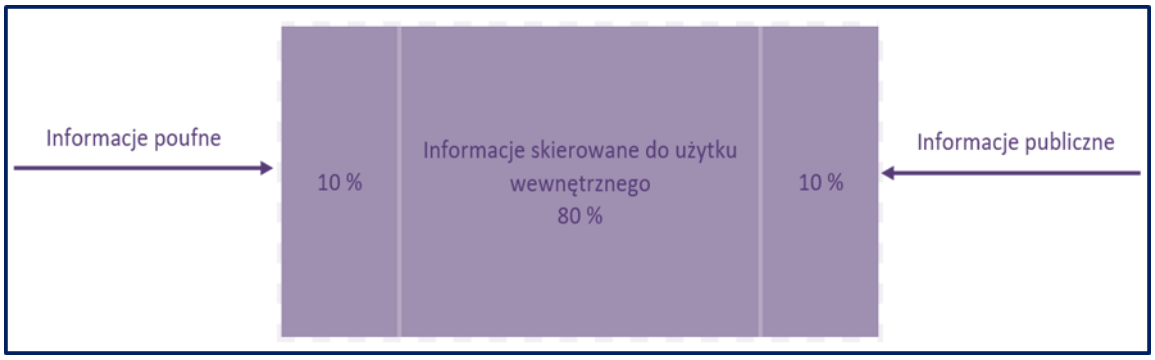
2.3. Rola i zadania elementów SZBI

- **Klasyfikacja informacji**

Aby móc dokładnie określić wartość informacji, jej hierarchiczność, wrażliwość oraz krytyczność zaleca się sklasyfikowanie jej poprzez dokładny spis informacji znajdujących się w organizacji oraz określenie poziomu dostępu dla użytkowników. Przykładowo dane dotyczące zatrudnienia w firmie, informacje o płacach, czy bazy danych klientów, projekty, patenty należy określić innym poziomem dostępu. Takie podejście pozwoli uniknąć swobodnego dostępu do informacji osobom, którym nie są one potrzebne do wykonywania ich obowiązków służbowych. Należy też wykluczyć dostęp osób przypadkowych, które w ogóle nie powinny mieć wglądu do takich danych [101].

Nadrzędnymi potrzebami sklasyfikowania informacji są te ustalone przez jednostkę gospodarczą oraz wynikające z określonego poziomu ochrony podczas ich przetwarzania, czyli który zależy od wrażliwości i krytyczności informacji. Klasyfikacja poziomów ochrony informacji ma na celu określenie odpowiedniego poziomu ważności informacji, uzasadniając powód zastosowania specjalnych środków ochronnych. Dobrą praktyką jest przypisywanie informacji odpowiedniej kategorii. Jest to szczególnie pomocne podczas szybkiego odnajdywania potrzebnych informacji, co ułatwia pracę (w przypadku przechowywania w systemach informatycznych, należy dokonywać weryfikacji technicznej, od kontroli spójności bazy danych, poprzez ilość dostępnej pamięci, a kończąc na zabezpieczeniach) [101].

W jednostce gospodarczej przechowuje się różnego rodzaju dokumenty, mianowicie: plany strategiczne, operacyjne, taktyczne, informacje o dostawcach, klientach, pracownikach, potencjalnych partnerach, finansowe, zasobach, informacje rachunkowe, wygenerowanie z baz danych. Ponadto w dokumentach zawarte są procedury, wyniki audytów, plan utrzymania ciągłości działania, raporty, plany awaryjne, działania korygujące i naprawcze. Poza tym na uwagę zasługuje również fakt korespondencji z kontrahentami, jak również materiały szkoleniowe wykorzystane w firmie, informacje o dostępnych zabezpieczeniach systemowych, patenty, dokumenty własności intelektualnej pracowników itd. Liczba tych informacji jest nieograniczona, dlatego wskazuje się na postępowanie klasyfikacyjne informacji, aby zdefiniować poziom szczegółowości, poświęcając temu odpowiednią uwagę [17].



Rysunek 13. Podział informacji wg. jej klasyfikacji
Źródło: Opracowanie własne na podstawie [103].

Adamczyk w swojej książce „Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania" podzielił informację następująco:

1. Informacje wrażliwe o zasadniczym znaczeniu dla przedsiębiorstwa;
2. Informacje do użytku wewnętrznego, dla działania przedsiębiorstwa. Są dostępne bez ograniczeń dla pracowników, zupełnie przeciwnie niż informacje wrażliwe lub po podpisaniu zobowiązań poufności;
3. Informacje publiczne, które są jawne bez ograniczeń [104].

Taka klasyfikacja wskazuje, że należy wziąć pod uwagę po pierwsze: zobowiązania kontaktowe, po drugie: wrażliwość informacji i finansowe konsekwencje ujawnienia jej na zewnątrz.

Jak podaje J. Łuczak i M. Tyburski [17] znacznym ułatwieniem w identyfikowaniu informacji może być określenie wszystkich informacji tworzonych i wykorzystywanych w procesach wykonywanych w ramach systemu zarządzania lub zarządzania zasobami. Zatem, ważne jest też określenie istotności informacji z punktu widzenia okoliczności dla instytucji, z uwagi na mocowania prawne, zapisy w umowach, czy przydatności do celów zarządzania, wrażliwość oraz krytyczność dla organizacji. Istotne są też oczekiwania biznesowe współdzielenia i ograniczenia dostępu do informacji, jak również konsekwencje wynikające z tych wymagań. W niektórych organizacjach należy identyfikować informację bardzo szczegółowo ze względu na specyfikę prowadzonego biznesu, natomiast w innych wystarczy ogólny poziom kwalifikowania informacji. To właściciel aktywów powinien odpowiednio sklasyfikować informacje, dokonywać okresowych przeglądów, zapewniając tym samym bezpieczeństwo posiadanych aktywów.

Na bazie klasyfikacji informacji powinno się opracować i wdrożyć procedury oznaczenia informacji i postępowania z nią. Dotyczy to aktywów zarówno papierowych, jak i zapisów elektronicznych. Procedury powinny określać sposób przechowywania informacji, w jakich pomieszczeniach, na jakich nośnikach jest zapisana oraz zasady postępowania z informacją tzn. sposób kopiowania, przenoszenia, ewentualnych modyfikacji w razie potrzeby, przesyłania czy udostępniania lub końcu sposobu jej niszczenia [100].

Odpowiednio oznaczone winny być również informacje wrażliwe i krytyczne. Ważność informacji można oznaczyć dwoma sposobami. Jedna z nich to metoda subiektywna, gdzie uprawniona osoba decyduje, które informacje są istotne z perspektywy przedsiębiorstwa. Do drugiej metody zaliczamy ocenę obiektywną.

Pomocne będą również zestawienia tabelaryczne i specjalistyczne lub indywidualnie dedykowane oprogramowanie. O metodzie klasyfikacji informacji zadecyduje sama firma i też ona poniesie odpowiedzialność za sposób przeprowadzenia klasyfikacji. Kategoryzacja informacji ma charakter umowny, jednak należy pamiętać, że powinna być jak najbardziej zbliżona do rzeczywistego znaczenia informacji [17].

Pomocna w klasyfikacji informacji jest również ustawa o ochronie informacji niejawnych, która wskazuje na cztery grupy tajności informacji m.in.: ściśle tajne, tajne, poufne, zastrzeżone. Ponadto, zaleca specjalne przechowywanie informacji w zabezpieczonym pomieszczeniu np. kancelarii tajnej, oznaczenie ich na pierwszych stronach, albo też wprowadzenie rejestru obiegu takich dokumentów [23].

Konkludując można stwierdzić, że klasyfikacja informacji jest jak najbardziej potrzebna w celu zidentyfikowania jej najistotniejszej wartości dla jednostki gospodarczej, które w dalszej kolejności należy poddać precyzyjnie obserwacji, a także takich, które w danym momencie nie wymagają ochrony, ale powinny być śledzone z punktu widzenia zmian.

W rozważaniach na temat klasyfikowania informacji warto wziąć pod uwagę, jakie dokumenty i systemy zawierają informacje ważne ze względu na atrybuty bezpieczeństwa (tj. głównie dostępność, poufność oraz integralność), ponieważ poziom ochrony informacji określany jest też przez analizę pod kątem poufności, integralności oraz dostępności.

Analizując kwestię związaną z klasyfikacją informacji, ważnym i istotnie wpływającym czynnikiem jest prowadzenie odpowiednich zapisów, które określają, kto i w jakim czasie i celu korzystał z danej informacji, wymagających ochrony z punktu

widzenie organizacji. Takie zapisy pozwolą w określenie, kto i kiedy uzyskał dostęp do konkretnie określonej wiadomości, w jakim celu ją przeglądał oraz czy miał do tego potrzebne uprawnienia [100,101].

- **Polityka Bezpieczeństwa Informacji**

Rozważając, rozwiązania proceduralne i organizacyjne konieczne są do zapewnienia bezpieczeństwa, należy rozpocząć od polityki bezpieczeństwa informacji. Polska norma PN-I-13335-2:2003 definiuje ją, jako prawa, reguły i praktyczne doświadczenia, regulujące sposób zarządzania oraz ochrony i dystrybucji informacji wewnątrz określonego systemu.

We wspomnianej normie zdefiniowano i opisano powiązania pomiędzy dokumentami polityki na trzech poziomach.

- ✓ Poziom I- polityka bezpieczeństwa instytucji (określa cele i strategię organizacji);
- ✓ Poziom II- polityka bezpieczeństwa instytucji w zakresie systemów informatycznych (dotyczy polityki bezpieczeństwa cyberprzestrzeni);
- ✓ Poziom III- polityka bezpieczeństwa danego systemu informacyjnego (zajmuje się poszczególnymi elementami składowymi w cyberprzestrzeni, które nie zostały ujęte w poziomie II).

Należy zaznaczyć, iż polityki z poziomu II-go i III-go winny być zgodne z polityką I- go poziomu. Natomiast polityka III poziomu powinna być spójna i wynikać z polityki II poziomu. Takie ujęcie powoduje powstanie polityki niezależnej od profilu organizacji.

Celem stworzenia PBI jest zapewnienie odpowiedniej ochrony dostępu do informacji w jednostce organizacyjnej. Dokument ten powinien zawierać wiele zagadnień związanych z ochroną danych i informacji, uwzględniając przy tym elementy takie jak rodzaj, charakter prowadzonej działalności lub też jej wielkość. Aby przechowywana informacja była należycie chroniona należy określić i stworzyć zbiór zasad i reguł postępowania, instrukcje, procedury, wytyczne, które będą obowiązywać podczas przetwarzania informacji. Z PBI powinno jasno wynikać, co podlega ochronie, jakiego typu są to informacje, jakim sprzętem dysponuje firma, i w jaki sposób planuje się chronić krytyczne zespoły [94, 87].

Tak, więc PBI obejmuje cały cykl życia informacji w przedsiębiorstwie, od jej zebrania, opracowania i przechowywania poprzez gromadzenie, udostępnienie i jej

usunięcie. Omawiany dokument sprawdza się w systemach klasycznych tzn. archiwach, dokumentach w formie papierowej jak i systemach elektronicznych [105][85]. Ponadto, pojęcie PBI odnosi się do rozwiązań zarówno organizacyjnych, jak i technicznych dotyczących ochrony informacji. Dokument ten dzieli się na cztery uzupełniające się strefy a mianowicie:

- ✓ Politykę organizacyjną (dotyczy procedur organizacyjnych i utrzymania ciągłości działania, awarii związanych z zapasowymi środkami przetwarzania);
- ✓ Politykę bezpieczeństwa informacji (dotyczy ochrony i zarządzania dokumentami stanowiącymi tajemnicę oraz informacjami prawnie chronionymi, nośnikami danych i upoważnieniami do przetwarzania w/w informacji).
- ✓ Politykę personalną (określa odpowiedni dobór personelu na dane stanowisko, zawiera procedury dotyczące zatrudnienia osób, które pracują jak i nowo przyjętych osób, włącznie z szkoleniem BHP oraz procedury postępowania w okolicznościach braku odpowiedniego personelu);
- ✓ Politykę ochrony technicznej (dotyczy ochrony budynku, mienia i instrukcje zabezpieczeń na okoliczność niepożądanych zdarzeń) [106][88].

Literatura przedmiotu [9][47] wskazuje że PBI, powinna dotyczyć wszystkich procesów, w których wykorzystuje się informację, bez względu na sposób jej przetwarzania, formie występowania klasycznej np. (dokumenty w formie papierowej, archiwa) czy też w postaci systemów komputerowych. W rezultacie, tak utworzona PBI powinna obejmować, takie elementy jak:

Określenie znaczenia bezpieczeństwa informacji, jej nadrzędny cel, zakres i ważność ochrony dla postępowania z informacją
Oświadczenie o intencjach kierownictwa potwierdzające cele i zasady bezpieczeństwa informacji
Ramy dla wyznaczenia zabezpieczeń, celów zabezpieczeń biorąc pod uwagę szacowanie ryzyka i zarządzania ryzykiem
Deklarację zgodności z obowiązującymi przepisami w obszarze bezpieczeństwa informacji
Informację o zarządzaniu ciągłością działania
Informację dla personelu o konsekwencjach naruszenia polityki bezpieczeństwa
Deklarację świadomości ochrony informacji
Wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa, świadomość ochrony informacji
Informacje dotyczące zapobiegania i wykrywania wirusów oraz złośliwego oprogramowania
Definicję ogólnych i szczegółowych obowiązków przy zarządzaniu bezpieczeństwem informacji, w tym i zgłaszania naruszeń bezpieczeństwa
Odsyłacze do dokumentów będących wsparciem i uzupełnieniem polityki. Mowa tutaj o bardziej szczegółowych politykach mianowicie m.in.: polityka bezpieczeństwa systemu, bezpieczeństwa technologicznego itp.

Rysunek 14. Elementy zawarte w Polityce Bezpieczeństwa Informacji
Źródło: Opracowanie na podstawie [17].

Podejście praktyczne jest związane z ustaleniem rzeczywistych potrzeb we wszystkich obszarach zarządzania, dzięki czemu organizacja będzie miała dobrą

i skuteczną strategię oraz plan wdrożenia [9]. Przyjęta PBI winna być spisana w postaci dokumentu, zatwierdzona przez kierownictwo oraz podana do wiadomości wszystkim pracownikom w sposób jasny, dostępny i zrozumiały. Konstruując PBI należy zastosować rozwiązania kompleksowe, adekwatne do zagrożeń oraz potencjalnych strat, które mogą z nich wyniknąć. Polityka powinna również w jasny sposób formułować procedury postępowania w stosunku do wszystkich osób uprawnionych do korzystania z określonego system teleinformatycznego. Od przyjętych zasad nie powinno być wyjątków. Mianowicie ważne jest, aby dokładnie określić prawa i obowiązki wszystkich użytkowników systemu informatycznego, w tym również administratorów tych systemów oraz członków zarządu i kierownictwa włącznie.

Każda organizacja powinna mieć określony plan postępowania, gdyż z tej strategii będzie wynikał cel zarządzania bezpieczeństwem informacji oraz całego systemu IT. z tego też względu PBI stanowi główny dokument SZBI, a jej zakres zależy od kompetencji i starań danej jednostki gospodarczej.

- **Organizacja Bezpieczeństwa Informacji**

Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie związane jest z wdrożeniem procesów i procedur dotyczących bezpieczeństwa informacji. Ponadto, powinny zostać określone interdyscyplinarne obowiązki i funkcje niezbędne do zarządzania bezpieczeństwem informacji.

Nie do przecenienia jest fakt współpracy z kierownictwem określającym wymagania dla wewnętrznych i zewnętrznych profesjonalistów z obszaru BI, którzy z kolei mają za zadanie koordynować prace związane z SZBI [17].W praktyce zajmuje się tym pełnomocnik ds. bezpieczeństwa informacji przy współpracy z IODO, (jeżeli został powołany).

W ramach organizowania BI kierownictwo zobowiązane jest do zapewnienia następujących czynności:

Zaangażowanie kierownictwa
Koordynowanie wdrażania zabezpieczeń
Identyfikowanie celów bezpieczeństwa informacji
Włączanie celów do odpowiednich procesów
Przeglądy polityki bezpieczeństwa informacji
Monitoring procesów pod względem efektywności
Pomoc w inicjatywach dotyczących bezpieczeństwa informacji
Edukowanie świadomości w obszarze bezpieczeństwa informacji

Rysunek 15. Działania koordynowane przez kierownictwo organizacji
Źródło: Opracowanie na podstawie [107].

Omawiane działania winny być koordynowane również przez osoby upoważnione do zarządzania informacją. Wiąże się to ze ścisłą współpracą kierownictwa z Inspektorem Ochrony Danych Osobowych. Taka współpraca owocuje zapewnieniem zgodności realizowanych zadań według PBI, określeniem postępowań z zaistniałymi niezgodnościami, opracowaniem procesów i zasad klasyfikacji informacji i ostatecznie szacowaniem ryzyka. Ponadto taka współpraca też jest korzystna w rozpoznawaniu zmian zachodzących wokół zagrożeń oraz monitorowaniu incydentów związanych z BI, co jest efektem wcześniejszego kształcenia i uświadamiania o bezpieczeństwie informacji.

Podział odpowiedzialności winien być zgodny z wcześniejszymi ustaleniami w PBI i wyraźnie określać odpowiedzialność za ochronę poszczególnych aktywów i procesów [17]. Niezbędne jest w tym zakresie określenie poziomów uprawnień. Odpowiedzialność powinna być uzupełniona wyraźnymi wytycznymi odnośnie postępowania z daną informacją.

Wobec powyższego, korzystne jest wprowadzenie PBI, która będzie odpowiadać za całokształt działań ustanawiających odpowiedzialność za aktywa, procesy, zabezpieczenia i poziom autoryzacji. Jednak odpowiedzialność za wdrożenie różnych środków ochronnych i wyznaczenie odpowiednich zasobów do realizacji poszczególnych zadań spoczywa na właścicielach poszczególnych aktywów.

W celu wdrożenia procesów autoryzacji nowych środków przetwarzania informacji, stosuje się następujące reguły:

- ✓ nowe środki przetwarzania informacji muszą posiadać autoryzację, co do ich przetwarzania i sposobu użycia;
- ✓ nadawanie autoryzacji powinno odbywać się przez osobę z obszaru kompetencji dotyczącego lokalnego systemu informacyjnego;
- ✓ używanie urządzeń przenośnych, twardych dysków, stosowanych do przetwarzania informacji biznesowych powinno być poprzedzone określeniem i wdrożeniem odpowiednich zabezpieczeń;
- ✓ oprogramowanie i sprzęt powinny być zgodne z innymi systemami przetwarzania informacji, nowe urządzenia powinny mieć określoną autoryzację dla celu jej użycia [86].

Jednak sytuacja użycia innych urządzeń mobilnych (laptopów, telefonów) sprzyja powstawaniu nowych zagrożeń i wymusza zastosowanie następnych zabezpieczeń na

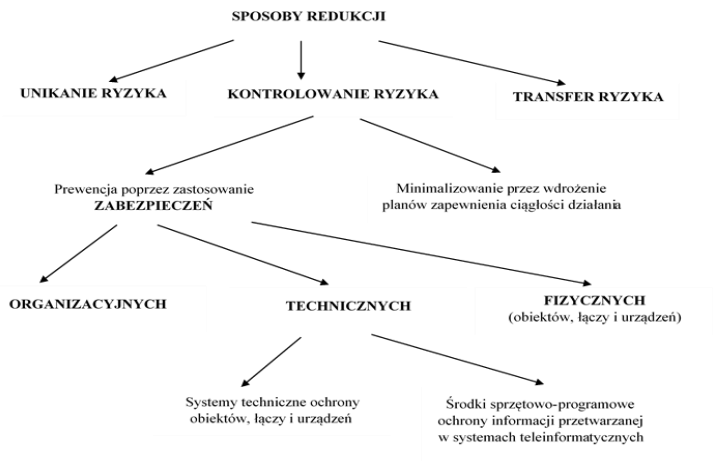
tych urządzeniach. Ponadto, organizacja powinna zastanowić się jak zabezpieczyć informacje, które są jej własnością, a są udostępniane podmiotom zewnętrznym. Nad tym procesem również należy mieć kontrolę.

Zabezpieczenia

W celu zidentyfikowania zagrożenia oraz ryzyka utraty informacji należy dokonać odpowiedniej selekcji wdrożenia efektywnych metod ochrony. Używane dotychczas zabezpieczenia stanowią zbiór procedur obowiązujących w jednostce gospodarczej. Powinny być one dobierane z należytą starannością i uwagą, gdyż tylko podejście indywidualne, uwzględniające specyfikę podmiotu może zminimalizować wpływ zagrożeń oraz podatności, a w konsekwencji zredukować ryzyko do stanu oczekiwanego.

Norma ISO/IEC 27001 w załączniku A określa minimalny zestaw zabezpieczeń, który zaleca się do wprowadzenia zmian. Co prawda, załącznik nie stanowi wyłącznego źródła informacji, jest to zaledwie minimum, które powinno się wziąć pod uwagę w przedsiębiorstwie, jako część procesu, spełniając wymagania procesowe. To specyfika działalności dyktuje dodatkowe cele i związane z tym możliwości stosowania proponowanych zabezpieczeń [17].

Metody ochrony stosowane w podmiotach mogę mieć formę fizyczną, sprzętowo-programową, organizacyjną czy administracyjną. Wspomniane metody zabezpieczeń dotyczą zbioru różnych środków ochronnych w budynkach, pomieszczeniach, dotyczących sprzętu komputerowego, oprogramowania, dokumentów elektronicznych i papierowych oraz personelu. Efektywność wdrożonych metod będzie tym wyższa, im dostosowanie się do metod będzie całościowe, obejmujące całą organizację i wzajemnie się uzupełniające [38].



Rysunek 16. Miejsce zabezpieczeń w metodach postępowania z ryzykiem
Źródło: Opracowanie na podstawie [105].

W wyniku kombinacji unikania, kontrolowania oraz transferu ryzyka i zastosowania wielu zabezpieczeń spełniających kilka funkcji, proces zmniejszenia wartości ryzyka osiągnie poziom akceptowalny, najmniejszym kosztem, i przy minimalnym wpływie na pracę przedsiębiorstwa [105]. Metody zabezpieczeń dotyczą różnych środków, przykładowe z nich to: szyfrowanie, podpis cyfrowy, tworzenie kopii zapasowych, dodatkowe zasilanie prądu, monitoring, kontrola dostępu, programy antywirusowe, korzystanie z zapór ogniowych. Wskazane jest również samodzielne wypracowanie nowych mechanizmów ochronnych dla jednostki gospodarczej.
Organizacyjne środki nie są na tyle efektywne, co mechanizmy techniczne, ale mogą być sprawne i pewne w utrzymaniu bezpieczeństwa procesów, zakładając optymalne koszty.

- **Zabezpieczenia organizacyjne**

Stosuje się do czynności i działań mających związek z określeniem struktury wewnętrznej podmiotu gospodarczego, podejmowanych w celu ochrony cennych zasobów organizacyjnych.

Głównym dokumentem zaliczanym do zabezpieczeń organizacyjnych to polityka bezpieczeństwa, które przedstawia określony sposób działania zapewniający, bezpieczeństwo danych.

Gruntownym opracowaniu polityki kadrowej, w której będą zawarte informacje odnośnie przyjmowania osób, zwalniania ich, przekazywania uprawnień czy też szkoleń
Uszczegółowienie ogólnej polityki bezpieczeństwa danych
Przedstawieniu lokalizacji jednostki gospodarczej i jej przeznaczenia
Utworzeniu jednostek organizacyjnych między innymi działu odpowiedzialnego za bezpieczeństwo danych
Określeniu stref ochronnych w jednostce gospodarczej
Określeniu zakres obowiązków i odpowiedzialności pracowników
Opracowaniu regulaminów, z których będzie wynikać postępowanie pracowników w normalnych warunkach oraz sytuacjach kryzysowych
Scharakteryzowaniu planu organizacji i koordynacji kontroli procesów pracy. Dotyczy to również obiegu dokumentów
Wykupieniu polisy ubezpieczeniowej

Rysunek 17. Działania organizacyjne
Źródło: Opracowanie na podstawie [45].

Zabezpieczenia organizacyjne powinny wpisywać się w ogólną PBI, tzn. zaleca się kilku etapowe i całościowe działanie, które umożliwiałoby wyłonienie słabych stron łańcucha bezpieczeństwa.

Zabezpieczenia administracyjne

Zabezpieczenia administracyjne dotyczą zbioru czynności i technik używanych poprzez kadrę pracowniczą, w celu zapewnienia właściwej ochrony zasobom organizacyjnym.

Administrowanie w organizacji oprócz systemu informatycznego dotyczy wszystkich obiektów oraz zdarzeń zachodzących w przedsiębiorstwie. Do głównych zabezpieczeń administracyjnych należą przedsięwzięcia związane z certyfikacją oraz zarządzaniem systemami informatycznymi, odpowiedzialne zarządzanie dostępem do pomieszczeń, należyte zarządzanie procesami pracy itd. [22].

Elementem, które w znacznym stopniu wpływa na bezpieczeństwo to ochrona sprzętu wykorzystywanego w przedsiębiorstwie. W celu skutecznej ochrony zaleca się zakup urządzeń certyfikowanych do pracy w określonych warunkach. Certyfikacja jest procedurą, w wyniku, której zostaje udzielone pisemne zapewnienie, że obiekt certyfikowany jest zgodny z podstawowymi wymaganiami i nadaje się dla określonego zastosowania. Ponadto, certyfikacja wzmacnia poczucie przewidywalności procesów, które występują w organizacji. Certyfikować można nie tylko sprzęt, lecz stosowane oprogramowanie, urządzenia specjalistyczne, obiekty, pomieszczenia, technologie, dokumenty, a także osoby [58].

Kolejnym działaniem administracyjnym jest opracowanie procedur przyjmowania urządzeń. Dzięki takiej certyfikacji organizacja ma pewność spełnienia przez sprzęt określonych wymogów. Poza tym, kupując urządzenie z certyfikatem, zwiększa się pewność nie wystąpienia usterki, która z kolei mogłaby zaważyć na działaniu przedsiębiorstwa.

Następną ważną kwestią dotyczącą zabezpieczeń administracyjnych jest zarządzanie dostępem do pomieszczeń i obiektów Klucze dostępu powinny być w dyspozycji tylko i wyłącznie osób, które mają do niego upoważnienie, (nie powinno się pożyczać karty wejściowej w celach koleżeńskich).W przeciwnym razie, należy liczyć się z różnymi nadużyciami. Oto kilka z takich sytuacji nadużywających system.

Niedopuszczalnym stanem byłoby przekazanie karty wejściowej jednego z pracowników po jego odejściu z pracy, innemu nowemu pracownikowi. Odpowiedzialność nakazuje natychmiastowe zablokowanie przepustki, aby uniemożliwić ponowne wejście [83].

Ważnym jest fakt świadomości pracowników i użytkowników, którzy wiedzą o używaniu odpowiedniej, jakości i ilości haseł (zasada czystego biurka), zawsze robiąc kopie zapasowe systemu operacyjnego, stanu programów i danych.

Administrator systemów informatycznych (ASI) również powinien cyklicznie kontrolować używany sprzęt, jakość programów oraz przeprowadzać kontrole systemu informatycznego, sprawdzając co pracownicy instalują na swoich komputerach. Do obowiązku administratora należy również dbanie o zainstalowanie odpowiednich zabezpieczeń na styku sieci przyłączonej do Internetu [83].

- **Zabezpieczenia sprzętowo-programowe i zarządzanie IT**

Ten rodzaj bezpieczeństwa dotyczy ogółu środków i czynności, metod oraz środków teleinformatycznych wykorzystywanych w przedsiębiorstwie, w celu ochrony wartości informacji.

Używanie programowych zapór sieciowych tzn. firewall
Wykorzystywanie bieżącego aktualizowanego oprogramowania systemowego i użytkowego, dotyczy to też oprogramowania producenta sprzętu- firmware
Regularne tworzenie kopii bezpieczeństwa danych – backup
Używanie licencjonowanego i certyfikowanego pod względem bezpieczeństwa sprzętu teleinformatycznego dotyczy to również oprogramowania systemowego
Dobieranie odpowiedniej konfiguracji sprzętu i oprogramowania w stacjach roboczych, serwerach i urządzeniach teleinformatycznych
Wykorzystywanie nadmiarowych urządzeń i środków technicznych, dotyczy to również aplikacji pomagających w celu zapewnienia ciągłości przetwarzania, przesyłania, archiwizacji i udostępniania danych: zamienne komputery, serwery z certyfikowanym oprogramowaniem, macierze dyskowe RAID, zapasowe łącza teleinformatyczne
Wykorzystywanie technik kryptograficznych w celu zarchiwizowania danych o kluczowym znaczeniu
Używanie programowej kontroli dostępu do zasobów. Mowa tutaj o dostępie do stacji roboczej, systemu operacyjnego, sieci teleinformatycznych, baz danych
Korzystanie z aplikacji detekcyjnej, która blokuje nieuprawniony dostęp do działań IDS/IRS
Stosowanie skutecznych programów antywirusowych
Wykorzystywanie programów pułapek typu „dzbanek miodu" werbujące intruzów do specjalnie udostępnianych zasobów, umożliwiając w ten sposób wykrycie sprawcy ataku.

Rysunek 18. Zabezpieczenia sprzętowo -programowe
Źródło: Opracowanie na podstawie [45].

W praktyce biznesowej przedsiębiorstwa inicjują różne metody zabezpieczeń. Zaimplementowanie takich środków ochronnych często powoduje duże zmiany w strukturze organizacyjnej jednostki gospodarczej oraz w dotychczasowych procesach biznesowych. Metody zabezpieczeń wdrażane w danym podmiocie gospodarczym powinny być łatwe do użytkowania, kompleksowe oraz spójne z innymi środkami podejmowanymi w celu ochrony istotnych danych. Świat informatyki oferuje całą gamę środków ochronnych pochodzącą od różnych producentów. Należy je wykorzystywać, co jest już mniej komfortowe dla personelu. Zatem, zaleca się równowagę pomiędzy przyjętymi metodami zabezpieczeń, a wygodą użytkowników w korzystaniu z zasobów.

Istotnym kryterium będą relatywnie odpowiednio dobrane zabezpieczenia do ryzyka wystąpienia zagrożenia, ważności zasobów oraz pozycji materialnej danej jednostki organizacyjnej.

- **Zrządzanie bezpieczeństwem IT**

Bezpieczeństwo IT polega na zmierzaniu do osiągnięcia i utrzymania określonego poziomu bezpieczeństwa tzn. poziomu poufności, integralności, dostępności, rozliczalności czy tez niezawodności systemu, przy jednoczesnej redukcji kosztów użytkowania danego systemu. Bezpieczeństwo IT dotyczy zbioru kwestii z obszaru telekomunikacji połączonej z informatyką, a powiązanej z szacowaniem i kontrolą ryzyka powstałego w wyniku użytkowania sprzętów komputerowych, sieci teleinformatycznych, przesyłania danych do innych lokalizacji a rozpatrywanych z punktu widzenia atrybutów informacji. Bezpieczeństwo IT powinno być na tyle skutecznie dobrane do organizacji by zabezpieczyć informację przed takimi sytuacjami jak: włamanie do systemu, kradzież danych, oszustwa, fałszerstwa, szpiegostwo komputerowe, naruszenie atrybutów informacji, zainstalowania złośliwego oprogramowania oraz naruszenia uwierzytelnienia i autoryzacji pracujących w systemach pracowników [58].

Nadzór nad bezawaryjnym i poprawnym funkcjonowaniu systemu informatycznego, wykorzystując sprzętowy firewall, bezpieczne połączenie szyfrowane SSL VPN między serwerem a stanowiskiem użytkownika. Rozwiązania te blokują skanery użytkownika i część połączeń zewnętrznych. SSL VPN zabezpiecza przed włamaniem do sieci
Natychmiastowe usuwanie problemów związanych z użytkowaniem sprzętu komputerowego
Dostosowanie oprogramowania do obowiązujących standardów
Instalacja i optymalizacja sprzętu komputerowego i oprogramowania
Wdrożenie polityki bezpieczeństwa i jej nadzór
Profilaktyka antywirusowa, aktualizacje wykrywające złośliwe oprogramowanie
Pomoc dla odbiorców wykorzystujących programy biurowe
Opracowanie raportów z funkcjonowania systemów informatycznych
Aktualizacja oprogramowania
Monitorowanie zabezpieczeń używanych w firmie
Uruchomienie dodatkowych zabezpieczeń, tzn. tworzenie kopi zapasowych, archiwizowanie danych,
Wprowadzenie systemów integralności danych, chroniąc się przed złośliwym oprogramowaniem
Selekcjonowanie odpowiednich metod programistycznych
Kod źródłowy winien być pobrany od źródła
Przegląd, jakości aplikacji wykorzystywanych w przedsiębiorstwie
Wprowadzenie systemów chroniących przed włamaniami, kradzieżami danych i oprogramowaniem
Zabezpieczenia używanego sprzętu przed szpiegostwem komputerowym
Wprowadzenie autoryzacji i kontroli nad tworzonymi systemami
Obserwowanie rejestrowanych aktywności hostów
Wprowadzenie oprogramowania, które będzie zapisywać incydenty mogące zapisywać naruszenia ochrony i bezpieczeństwa teleinformatycznego przedsiębiorstwie

Rysunek 19. Percepcja działań z obszaru teleinformatycznego
Źródło: Opracowanie na podstawie [82] [58] [108].

Patrząc na całokształt zabezpieczeń systemu i sieci teleinformatycznych mają one za zadanie uniemożliwić niepowołanym osobom dostęp do cennych informacji [15][83]. Mówiąc o zarządzaniu bezpieczeństwem w systemach informatycznych mamy na myśli zadania z zakresu: dokumentowania, zarządzania zmianami, rozdzielania obowiązków, rozdzielania urządzeń rozwojowych (testowych, eksploatacyjnych), monitorowania działalności, wdrożenia zabezpieczeń, rejestrowania błędów oraz przeprowadzenia audytu [9]. Zabezpieczenia informatyczne należy zaliczyć do części ogólnej PBI, która przedstawia działania kompleksowo eliminując słabe punkty procesu bezpieczeństwa tzn. używanie e-maila prywatnego wykorzystywanie podczas pracy przeglądarek internetowych, niewłaściwe korzystanie z polityki haseł [82].

Z pracownikami przedsiębiorstwa powinny być omówione zasady, korzystania z poczty elektronicznej, z przeglądarki internetowej, stosowania polityki haseł oraz obszaru wstępowania najczęstszych zagrożeń.

- **Zabezpieczenia techniczne**

Omawiane zabezpieczenia związane są ze specjalistycznymi rozwiązaniami techniczno-technologicznymi stosowanymi w celu ochrony zasobów danych w jednostce organizacyjnej. Zabezpieczenia te obejmują zbiór różnych czynności i metod, które uzupełniają zabezpieczenia fizyczne [47]. Mowa tutaj o zapobieganiu przed nieuprawnionym dostępem do pomieszczeń danej jednostki i informacji, którą posiada. Na ten rodzaj bezpieczeństwa wpływają też systemy ochrony technicznej takie jak: system przeciwpożarowy i gaśniczy, system kontroli dostępu, system alarmowy wewnętrzny i zewnętrzny, czy system telewizji dozorowej.

Przez elementy techniczne rozumie się:

Odpowiedni poziom systemu klimatyzacji i wentylacji w pomieszczeniach
Wykorzystanie instalacji alarmowych podczas włamania, pożaru, czy zbytniej wilgoci
Wykorzystanie instalacji monitorujących przy użyciu telewizji przemysłowej
Stosowanie blokady do urządzeń i sieci teleinformatycznych ograniczając tym samym możliwość korzystania z klawiatury, czy dysków twardych.
Dobór dodatkowego zasilania energetycznego centralnego lub tylko jednostkowego np.: zasilaczy prądotwórczych UPS, czy też stabilizatory napięcia
Zastosowanie instalacji bezpieczników przepięciowych
Stosowanie elektronicznych środków sprawdzania tożsamości poprzez zamki elektroniczne, systemy biometryczne (odciski palców, głos, rozpoznanie siatkówki oka)
Używanie zabezpieczeń przed podsłuchem np.: dobierając odpowiednie media transmisyjne sygnał (światłowody)
Wykorzystanie narzędzia do ekranowania pomieszczeń, w których są dostępne ważne zasoby np.: używając klatki Faradaya, która nie przepuszcza fal elektromagnetycznych zarówno z zewnątrz ani na zewnątrz
Ograniczenie dostępu do okablowania ukrywając przewodów w podłodze oraz używając mediów transmisyjnych w specjalnych osłonach zabezpieczających.

Rysunek 20. Obszary, w których występują zabezpieczenia techniczne

Źródło: Opracowanie na podstawie [105].

Zabezpieczenia techniczne obejmują, więc kontrole dostępu, ochronę przeciwpożarową, systemy zasilania gwarantowanego, klimatyzację i chłodzenie, zabezpieczenia proceduralne oraz ochronę przed emisją elektromagnetyczną.

Idealnym rozwiązaniem w ramach zabezpieczeń fizycznych i technicznych jest stworzenie specjalnych stref ochronnych (tzn. podzielenie całości przestrzeni na obszary, dla których oddzielnie analizuje się wymagania dotyczące ochrony fizycznej oraz uprawnień dla personelu, mającego dostęp to tych stref), w których to przechowuje się chronione zasoby, a dostęp zarówno dla osób zatrudnionych, jak i ludzi z zewnątrz jest znaczenie utrudniony.

Przy podziale można wyznaczyć następujące strefy:

Strefa 1-ogólnodostępna

Strefa 2- dostępna tylko dla pracowników

Strefa 3-dostępna tylko wyłącznie dla najwyższego kierownictwa oraz osób upoważnionych.

Dostęp do pomieszczeń w chronionych strefach powinny mieć tylko i wyłącznie osoby upoważnione lub członkowie zarządu. Pracownicy, którzy są chwilowo zatrudnieni powinni tam przebywać tylko w obecności osób, które ponoszą pełną odpowiedzialność za bezpieczeństwo pomieszczenia.

Obszary chronione powinny być nadzorowane za pomocą różnych technik. Sprawdzają się tutaj fale akustyczne sygnały elektryczne, fale elektromagnetyczne, światło widzialne i podczerwień. Nie bez znaczenia jest również umiejscowienie obiektu, które powinno ograniczać ilość zagrożeń, ułatwić lokalizację potencjalnych nowych zagrożeń, zminimalizować możliwość podsłuchu, umożliwić szybką i łatwą zmianę umiejscowienia obiektu (drogi ewakuacji) oraz znacznie ograniczyć nadużycia poprzez łatwe kontrolowanie [22]. Istotnym jest również fakt, iż każde z tych pomieszczeń, powinno być otoczone specjalnymi strefami ochronnymi, które wyznaczają gradację dostępu. Strefy te tworzy się w celu opóźnienia czasu dotarcia osoby poruszającej się do obiektu chronionego [22].

- **Zabezpieczenia fizyczne**

Bezpieczeństwo fizyczne jest traktowane, jako pierwsze zabezpieczenie przed zagrożeniem. Normy z serii 27000 wskazują, na *„środki zastosowane w celu fizycznej ochrony zasobów przed umyślnym lub przypadkowym zagrożeniem”* [17, 23, 86]. Mogą to być drzwi, wzmocnienie okien, ogrodzenie, brama wejściowa, kolczatki ochronne itp.

Z kolei inna definicja wskazuje, że bezpieczeństwo fizyczne to zapewnienie zbioru tradycyjnych metod ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak pożar, powódź, kradzież, wandalizm, terroryzm [45].

Do omawianych metod zabezpieczeń fizycznych zaliczamy:

- należyty i selektywny dobór materiałów budowlanych np. szyby, ściany, stropy;
- tradycyjne środki opóźniające dostęp do pomieszczeń biurowych np.: ogrodzenia, sejfy, szafy pancerne, zamki, kraty, kłódki, metalowe drzwi;
- metody odstraszające intruza np.: oznakowanie terenu;
- wykrycie zagrożenia dzięki zastosowaniu telewizji przemysłowej, czy systemów alarmowych;
- przeciwdziałanie zagrożeniom poprzez zastosowaniu monitoringu wejść i wyjść pracowników oraz kontrolowaniu obecności gości na terenie jednostki np.: karty identyfikacyjne, przepustki, recepcja;
- dobór odpowiedniej lokalizacji budynków w celu realizowania procesów związanych z gromadzeniem, przesyłaniem, przetwarzaniem, udostępnianiem danych np. miejsce serwerowni nie powinno być przypadkowe, lecz wcześniej przemyślane przez kierownictwo organizacji, podobnie jak miejsce przechowywania zużytych sprzętów komputerowych czy nośników pamięci, i zużytych dysków,
- istotne będzie nawet usytuowanie pomieszczenia kotłowni (znajdują się tam urządzenia mechaniczne, które wydzielają ciepło, dlatego też wzrasta zagrożenie pożarem) [45].

Zazwyczaj, mówiąc o ochronie przedsiębiorstwa i jego bezpieczeństwie fizycznym mamy na myśli elementy utrudniające wejście do obiektów, podczas, gdy zasadniczym elementem bezpieczeństwa fizycznego są chronione w sposób ciągły trwałe wartości, które w znacznym stopniu decydują o istnieniu i funkcjonowaniu firmy.

Ochronie fizycznej podlegają następujące wartości:

1. ludzie- goście i pracownicy wraz z potencjałem intelektualnym;
2. rzeczy- teren, budynki, finanse, mienie nieruchome i ruchome;
3. informacje/dane;
4. elementy infrastruktury zewnętrznej [11].

Zwiększenie bezpieczeństwa fizycznego możliwe jest dzięki wprowadzeniu odpowiednich zasad pracy w danej strefie. Takie najpopularniejsze zabezpieczenia fizyczne zwyczaj zwiększają sposób bezpieczeństwa w każdej jednostce organizacyjnej.

Pod pojęciem ochrony fizycznej informacji rozumiemy ochronę dostępu do samej informacji, czyli do jej źródeł, nośników, urządzeń ją przetwarzających i archiwizujących. Jednak, ponieważ współczesne przedsiębiorstwo to przede wszystkim systemy informacyjne i informatyczne, więc problem jest o wiele bardziej złożony. W oparciu o przeprowadzoną analizę literatury przedmiotu [11,45] można wnioskować, że należy wprowadzić następujące wytyczne, co do zabezpieczeń.

Strefa ochronna winna być wyraźnie wyznaczona
Wszystkie drzwi pożarowe w obwodzie budynku powinny być zabezpieczone alarmem i wyposażone w zamek samozatrzaskowy
Strefa budynku lub pomieszczeń, w którym znajdują się urządzenia do przetwarzania danych, powinna być odpowiednio zabezpieczona pod względem fizycznym, tak by nie było między nimi przerw w obwodzie, wówczas mogłoby dojść łatwiej do włamania, poprzez swobodne poruszanie się intruza w pomieszczeniach organizacji
Wytrzymałą i solidną konstrukcją powinny odznaczać się ściany zewnętrzne
Stworzenie stanowiska recepcyjnego
Drzwi zewnętrzne należy odpowiednio zabezpieczyć systemem kontroli dostępu czy systemem włamania

Rysunek 21. Środki fizyczne w celu ochrony informacji
Źródło: Opracowanie na podstawie [11].

System wykrywania włamań jest bardzo pomocny w celu odnotowania wszystkich przypadków nietypowej obecności „nieproszonego gościa", sygnalizowanej w miejscu (pomieszczenia technicznego) i czasie oraz nietypowej porze (dni wolne od pracy, noc). Przykładem takiego urządzenia, które można uznać za podstawowe zabezpieczenie jest detektor ruchu na podczerwień i mikrofale. Dzięki systemowi nadzoru telewizyjnego można rejestrować i przesyłać obraz, co znacząco zwiększa skuteczność działań ochronnych [82] [1].

Biorąc pod uwagę zabezpieczenia fizyczne, zaleca się również prowadzenie monitoringu za pomocą kamer rozmieszczonych w najważniejszych miejscach w organizacji. Dzięki takiemu rozmieszczeniu można prowadzić nadzór nad tym, co się dzieje w jednostce gospodarczej. Zazwyczaj stosuje się monitoring, jako pierwszy poziom zabezpieczeń, utrudniając tym samym osobom postronnym dostęp do pomieszczeń, w których pozostają wartościowe zasoby.

Idealnym rozwiązaniem dla przedsiębiorstw jest wdrożenie systemu kontroli dostępu do pomieszczeń za pomocą drzwi ze zintegrowanym czytnikiem biometrycznym, bądź też użycie kart magnetycznych do pomieszczeń o dużym

zagrożeniu. Nie bez znaczenia są również czujniki ruchu, alarmy, syrena na zewnątrz [82][60].

Zabezpieczenia fizyczne wprowadza się już na poziomie planowania prowadzenia działalności. Warto kierować się wymaganiami prawnymi i najlepszymi praktykami w tym zakresie, zawartymi w zaleceniach normatywnych. Tym samym, można już wcześniej częściowo wykluczyć zagrożenia losowe poprzez używanie materiałów wyższej klasy spełniające standardy, jakości oraz bezpieczeństwa. Z opinii ekspertów, można wywnioskować, że jeśli nie wdrożono do organizacji podstawowych środków ochrony fizycznej, to w ogóle nie można mówić o chęci organizacji do poczucia bezpieczeństwa. W praktyce firmy, które kładą dominujący nacisk na ochronę teleinformatyczną zasobów informacyjnych często zapominają o wartości mechanizmów ochrony fizycznej. Jednak brak takiej ochrony może nieść za sobą poważne skutki, a mianowicie: kradzież sprzętu, nośników z danymi, czy awarii zasilania lub też awarii w funkcjonowaniu klimatyzacji w serwerowni [9].

2.4. Zarządzanie ryzykiem w SZBI

Na gruncie nauki właściwe scharakteryzowanie ryzyka należy do niezbędnych czynności.

Ze względu na to, że ryzyko jest terminem rozległym i istnieje wiele jego podziałów, autorka pracy posłużyła się wybranymi definicjami, które są niezbędne w szybkim rozpoznaniu niebezpieczeństwa oraz minimalizacji negatywnych skutków.

Ryzyko związane z bezpieczeństwem informacji definiowane jest, jako „*potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów, powodując szkodę dla organizacji”* [35].

F. Wołowski i J. Zawiła Niedźwiecki zinterpretowali ryzyko, jako miernik narażenia, określający możliwość zaistnienia negatywnego zdarzenia z powodu zasobu.

Natomiast zwięźle przedstawiając istotę ryzyka można scharakteryzować je dwoma następującymi parametrami:

- ✓ prawdopodobieństwem wystąpienia danej sytuacji;
- ✓ skutkiem pojawienia się zdarzenia, czyli strata;

Ryzyko można przedstawić wzorem:

$$\textbf{Ryzyko} = P \times S \qquad (1)$$

Gdzie:

P-prawdopodobieństwo wystąpienia zdarzenia;

S-skutki konsekwencji zdarzenia

W literaturze przedmiotu można znaleźć jeszcze inne metody szacowania ryzyka zarówno te opisowe, jak i z wykorzystaniem skomplikowanych modeli matematycznych. Szerzej ten temat opisano w pozycjach literaturowych [105], [40] [13], [82], [11]. W teorii i praktyce, jednak metody oceny ryzyka obejmują metody ilościowe, jakościowe oraz mieszane (kombinacja metody jakościowej i mieszanej), których istotę przedstawia tabela 11.

Tabela 11. Metody analizy ryzyka

Metody analizy ryzyka	
Metody ilościowe	Subiektywna ocena oparta na doświadczeniu i dobrych wskazówkach. Wynikiem szacowania ryzyka są listy zagrożeń oparte na rankingowaniu ryzyka. Wynikiem są konkretne jednostki miary zazwyczaj w kwotach. Jest to elastyczna metoda polegająca na szybkim dostarczeniu organizacji wyników w zakresie identyfikacji zagrożeń i stosowanych zabezpieczeń. Jednak zakres i koszt szacowania może się bardzo różnić. Wszelkie ryzyko i potencjalne skutki ryzyka prezentowane są w sposób opisowy.
Metody jakościowe	Określa dwa podstawowe parametry: wartość skutku i prawdopodobieństwo wystąpienia tego ryzyka w sposób opisowy. Skutki są określane przez ocenę wyników zdarzeń, jako niskie, średnie czy wysokie. Natomiast wyniki szacowania ryzyka mają wymiar finansowy lub procentowy. Metoda elastyczna na zmiany. Jakościowe metody można podzielić na: grafy ryzyka, matrycowe, wskaźnikowe.
Metody mieszane	Kombinacja dwóch metod: ilościowej i jakościowej. W metodzie tej wykorzystywane są analizy jakościowe, oparte na metodach scenariuszowych przy jednoczesnym użyciu ilościowej analizy określenia kosztów wystąpienia ryzyka. Wiedza z tych analiz uświadamia firmy o potencjalnym ryzyku.

Źródło: Opracowanie własne na podstawie [1]

W normie ISO/IEC TR 13335 scharakteryzowano podstawowe metody szacowania ryzyka. Mianowicie: macierz z wartościami predefiniowanymi, miara ryzyka, jako podstawa rankingu zagrożeń, ocena ryzyka poprzez oszacowanie częstotliwości zagrożeń.

Metody ilościowe:

Macierz z wartościami predefiniowanymi

Macierz z wartościami predefiniowanymi dotyczy wartości następujących parametrów: wartość aktywów (zasobów), poziom podatności oraz poziom zagrożeń. Metoda dotyczy zdefiniowania i punktowej wyceny wszystkich aktywów przy za pomocą skali od 0 do 5. Kolejno następnie dokonuje się identyfikacji poziomu podatności oraz zagrożeń dzięki zastosowaniu jakościowych kategorii (N – niski, Ś – średni, w –

wysoki). Otrzymana wartość aktywów, poziom podatności oraz zagrożeń kształtują macierz. W wyniku takiej kombinacji, składającej się z trzech parametrów szacowana jest wartość ryzyka, którą można określić w skali od 1 do 9.

Miara ryzyka, jako podstawa rankingu zagrożeń

Metoda szacowania ryzyka dotyczy zidentyfikowania wszystkich zagrożeń. Kolejno określa się wartość aktywu (tzn. koszt wystąpienia incydentu związanego z naruszeniem bezpieczeństwa informacji) oraz prawdopodobieństwie pojawienia się zagrożeń w skali punktowej od 1 do 10. Miarę ryzyka stanowi iloczyn dwóch wymienionych wyżej parametrów. Zaletą tej metody jest możliwość zestawienia ze sobą różnych typów zagrożeń, o zróżnicowanej wartości skutków oraz prawdopodobieństwie ich powstania. W efekcie, można otrzymać listę zagrożeń usystematyzowaną wg. rankingu od najbardziej do najmniej ważnych dla jednostki gospodarczej.

Metoda CRAMM- metoda w szczególności dedykowana organizacjom rządowym lub też stosowana w przemyśle. Metoda CRAMM wymaga analizy luk programu poprawy bezpieczeństwa, tworzenia rejestru zasobów informatycznych, definiowania zakresu zarządzania bezpieczeństwem informacji oraz tworzenia dokumentacji wdrożonych już środków zabezpieczeń. Zaletą tej metody jest obszerna baza szczegółowych pytań, praktyczne podejście dla dużych organizacji, możliwość raportowania, generowania wykresów, i schematów. Z kolei słabością tej metody to kosztowne szkolenia, trudna w obsłudze [1].

Metody mieszane:

Ocena ryzyka poprzez szacowanie częstotliwości zagrożeń

Polega na identyfikowaniu aktywów określonego systemu oraz określeniu zagrożeń. Kolejno ogół zidentyfikowanych zasobów poddawane są punktowej ocenie w skali od 0 do 4. Kolejno, oszacuje się dla każdego zasobu 2 parametry, tzn. poziomu zagrożenia oraz poziomu podatności, w skali jakościowej (a mianowicie niski, średni, wysoki). Na bazie tych dwóch wartości oznacza się wartość częstotliwości.

Metody jakościowe:

Do powszechnie stosowanych metod analizy ryzyka zaliczamy: FMEA, HOZOP, COBRA, CRAMM, MEHARI, MARION i OCTAVE.

Analiza defektów FMEA- metoda jakościowa dotycząca zidentyfikowania wad i błędów, wynikłych podczas procesów wytwórczych oraz skoncentrowana na

zapobieganiu powtórnemu występowaniu niezgodności. Dzięki użyciu tej metody konsekwentnie można zidentyfikować wady procesu oraz co bardzo ważne ograniczyć ryzyka z nim związane. Szacowanie ryzyka przy zastosowaniu tej metody oparte jest na szacowaniu czynników ryzyka. Ogólną wartość ryzyka prezentuje poniższy wzór:

$$WPR = Z \times R \times W \qquad (2)$$

Gdzie:

-Z- znaczenie dla klienta,

-R-prawdopodobieństwo utraty integralności, dostępności, poufności,

-W-wykrywalność utraty którejś z cech bezpieczeństwa informacji,

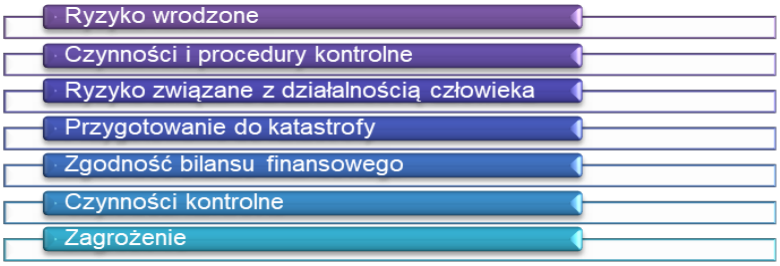
WPR-to wskaźnik priorytetu ryzyka.

Wskaźniki Z, R, W ocenia się w skali od 1-10, biorąc pod uwagę kryterium:

- Z(1-małe, 10-bardzo duże krytyczne),
- R(1-niemożliwe, 10-bardzo często),
- W(1- bardzo wysokie, 10-niemożliwe) [11].

Metoda HAZOP- podstawą metody jest wypracowanie modelu analizowanego systemu, w postaci różnych metod opisu, diagramu przepływu danych i sterowania, grafu przejść między stanami. Z uwagi na to, że modele te mają budowę hierarchiczną, analitycy mogą uwzględnić różny poziom szczegółowości. W toku ukierunkowanej dyskusji, w zespole są identyfikowane możliwe odstępstwa tzw. hazardy. Analizowane są podatności elementów modelu i ich zagrożenia.[2]

Metoda COBRA- dedykowana dla zarządu i kierownictwa przedsiębiorstwa, aby całościowo ocenić ryzyko dotyczącego działalności przedsiębiorstwa, przy uwzględnieniu pozycji i wizerunku organizacji i zgodności, co do obowiązujących przepisów prawnych oraz ustawodawczych. Metoda COBRA składa się z następujących obszarów:



Rysunek 22. Obszary, których dotyczy metoda Cobra
Opracowanie na podstawie [2].

Metoda MARION- metoda oparta o audyt, prowadzący do oceny stopnia ryzyka zastosowanych zabezpieczeń IT, w oparciu o kwestionariusz ankietowy, dający wskazówki poprzez zapisy związane z bezpieczeństwem informacji. Dzięki metodzie można rozpoznać stopień bezpieczeństwa, który jest określany poprzez 27 pytań dotyczących sześciu obszarów (tematów). Zagadnienia są określane w skali od 0 do 4 [1].

Metoda MEHARI- metoda oparta o wytyczne norm ISO/IEC 27001: 2014 i ISO/IEC TR 13335 przy użyciu jednolitego systemu oszacowania ryzyka i odpowiednio dobranych zabezpieczeń. Omawiana metoda przedstawia model szacowania ryzyka, (ujęcie modułowe modelu) dostarcza narzędzia do analizowania różnych incydentów, zasady wyboru różnych działań korekcyjnych ryzyko, umożliwia identyfikację zagrożeń i charakterystyki podatności na zagrożenie oraz pozwala na zidentyfikowanie podatności poprzez narzędzie, jakim jest audyt. Zaletą metody Mehari jest prostota używania, odpowiednia dla małych i średnich przedsiębiorstw, wykorzystujących technologie informatyczne oraz algorytm obliczeniowy, bazę pytań ogólnodostępnych.[1].

Wynika z tego, że ryzyko ma określoną wartość, którą można policzyć i organizacja powinna uwzględnić ją w swojej działalności. Dla organizacji oznacza to powinność porównania wartości ryzyka ze swoimi możliwościami pokrycia ewentualnych strat w przypadku wystąpienia ryzyka. To właśnie od rezultatu porównania określa się strategię oraz politykę w obszarze zarządzania ryzykiem.

Mimo że, każda aktywność gospodarcza wiąże się z podejmowaniem ryzyka to jednak nie powinno się kojarzyć ono jedynie z zagrożeniem, lecz może stanowić również okazję do osiągnięcia sukcesu.

Charakter i kierunek ryzyka w każdej jednostce gospodarczej jest inny i wymaga dostosowania metody łagodzenia ryzyka do specyfiki przedsiębiorstwa, rodzajów realizowanych przez nią operacji, istotności występujących zagrożeń [85].

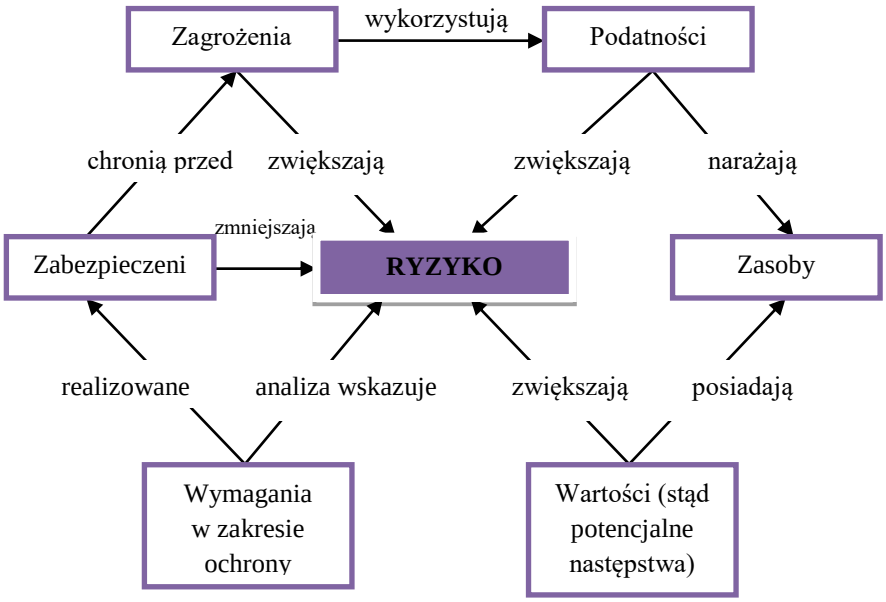
W przedsiębiorstwie ryzyko może wystąpić w różnych jego obszarach funkcjonalnych m.in. w magazynie, biurze, działach rozwojowych, logistyce, czy produkcji. Na każdy z tych działów mają wpływ pracownicy, partnerzy, produkty, maszyny, materiały. Każda z tych części może zostać zagrożona. Przeprowadzona analiza literatury przedmiotu wskazuje, że istnieje kilka rodzajów ryzyka. Można podzielić je na:

ryzyko właściwe (np. klęski żywiołowe), subiektywne (takie, które jest przewidywalne), obiektywne (można ocenić przy pomocy danych z ostatniego zdarzenia czy zdarzenie się powtórzy).

Prowadząc działalność gospodarczą należy zapoznać się również z inną grupą ryzyka, taką jak:

- ryzyko gospodarcze;
- ryzyko finansowe;
- ryzyko niewypłacalności;
- ryzyko handlowe;

Jak widać z powyższego, rola ryzyka utraty BI jest niezmiernie ważna. Co prawda niemożliwe jest całkowite wyeliminowanie ryzyka. Jednak decydenci, aby podjąć mądrą i świadomą decyzję, uwzględniają niebezpieczeństwo, które nie może przekroczyć akceptowalnego poziomu. Dlatego też PBI oraz Krajowe Ramy Interoperacyjności narzucają obowiązek pomocy poprzez wdrożenie w życie systemu bezpieczeństwa [93].



Rysunek 23. Zależności w zarządzaniu ryzykiem
Źródło: Opracowanie na podstawie [35].

Cykl zarządzania ryzykiem w BI jest analogiczny, jak w innych modelach jednak ważne by rozpatrywać ten element, jako jeden z cyklów organizacji, a nie odrębny proces w realizowanym projekcie wdrożenia systemu.

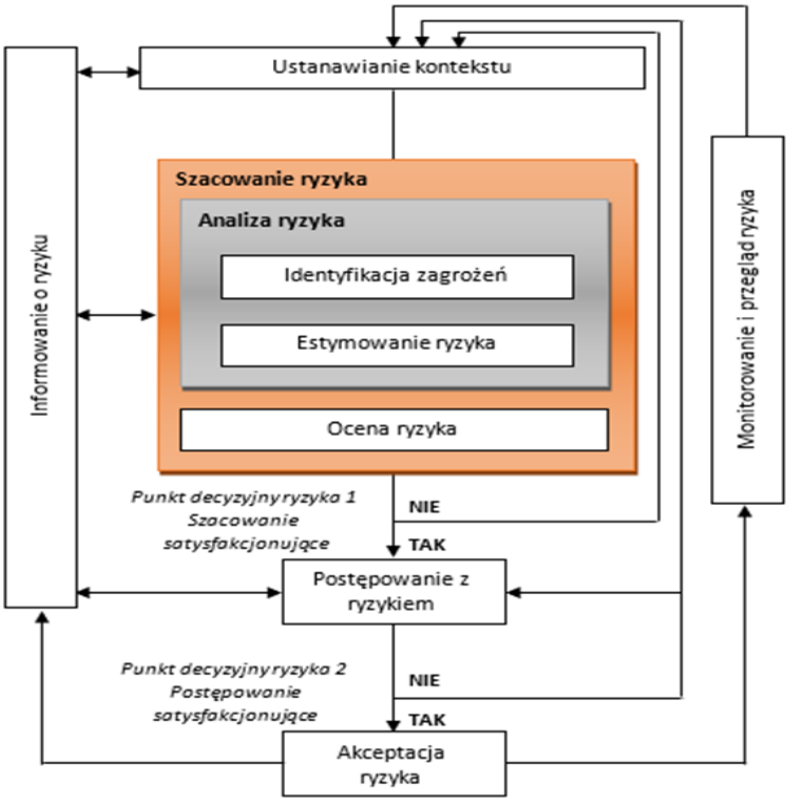
O efektywnym zarządzaniu w przedsiębiorstwie mówimy wówczas, gdy podejmowane są działania w zakresie ciągłego monitorowania i analizy ryzyka oraz

przeciwdziałania nowym zagrożeniom oraz podatnościom wykorzystanym poprzez zagrożenie. [105].

Ponadto, należy zwrócić uwagę, by podejście było typowo przeznaczone do istniejących warunków, jakie panują w organizacji oraz jednolite podczas całego procesu zarządzania ryzykiem. Wdrażając koncepcje z normy może to przynieść skutek odwrotny od zamierzonego i nie osiągnie się zamierzonego celu. Jest to powiązane z czynnikiem ludzkim, czyli nieznanym zachowaniem w obliczu konkretnych warunków.

Głównym elementem zarządzania ryzykiem w BI jest skierowanie pełnego procesu na rozpoznanie okoliczności i czynników, istotnie wpływających na odpowiednie zabezpieczenie cennych aktywów chronionych w przedsiębiorstwie.
Zarządzanie ryzykiem związane jest z planowaniem, kierowaniem i kontrolowaniem zasobów oraz czynnej współpracy stron zainteresowanych informacjami w celu osiągnięcia porozumienia, co do wymagań i wyboru opcji postępowania. Kwestia ta jest niezwykle istotna w budowaniu właściwego SZBI. To właśnie podnoszenie świadomości stron umacnia poczucie bezpieczeństwa i powoduje, że lepiej odpowiada ona ich potrzebom [86].

Niepowodzenie w zweryfikowaniu właściwej istoty ryzyka oraz wyznaczenie jego poziomu może spowodować, że środki naprawcze będą nieadekwatne do kosztów zabezpieczeń. Z tej też przyczyny, zarządzanie ryzykiem powinno się rozpatrywać, jako całość, czyli jako integralną część całego cyklu życia organizacji. Zarządzanie ryzykiem stanowi ważny element wszystkich zadań przeprowadzonych w organizacji oraz wspiera podejmowanie decyzji, gdyż ujawnia pełny przekrój dostępnych informacji i danych na bieżące potrzeby [109]. Zatem, celem zarządzania jest zmniejszenie ryzyka, w wyniku, czego możliwe będzie zmniejszenie ewentualnych skutków niepożądanego zdarzenia. Na rysunku 24. przedstawiono przekładowe działanie procesu zarządzania ryzykiem bezpieczeństwa informacji.



Rysunek 24. Cykl zarządzania ryzykiem w bezpieczeństwie informacji
Źródło: Opracowano na podstawie [44].

Konstrukcja postępowania z ryzykiem ma budowę procesu, opartą o podmiotowe filary i jest złożona z oddziałujących na siebie i po sobie etapów. Należy przyjąć takie etapy, które będą dostosowane do potrzeb danej organizacji.

Poniżej zaprezentowano kolejne etapy zarządzania ryzyka:

1. **Ustanowienie kontekstu**

Do ustanowienia kontekstu można zaliczyć zagadnienia i decyzje związane z organizacją procesu (tzn. kto?, kiedy?, jak?). Ponadto kontekst wyznacza zakres i granice procesu, kryteria oceny i postępowania z ryzykiem. Pierwszy etap cyklu ustala sposoby postępowania opartego o warunki, w jakich się znajduje organizacja, biorąc pod uwagę cele strategiczne, zakres i skalę działania, osoby odpowiedzialne za ryzyko, metodę oceny ryzyka, sposób szacowania ryzyka, poziom tolerowany ryzyka, kryteria ryzyka [110][94].

2. **Szacowanie ryzyka**

W wyniku szacowania ryzyka można ocenić możliwości wystąpienia danego zdarzenia, wyznaczyć granice poziomu minimalizacji akceptowalności ryzyka, do których jednostka będzie dążyła.

Norma 27001 wskazuje na wybór metody poświęconej szacowaniu ryzyka, zapewniającej porównywalne i powtarzalne efekty. Mowa tutaj o metodach ilościowych lub też jakościowych (popularne narzędzia analizy ryzyka obejmują np. Cramm, Cobra, Marion, Mehari, Ebios, itd.) Wiele ciekowych i wartościowych zaleceń znajduje się również w normie PN-ISO/IEC 27005, w której wskazano na integralną część zarządzania bezpieczeństwem informacji poprzez model PDCA.

I mimo, iż niema jedynej polecanej skutecznej metody dla szacowania ryzyka, to decyzja należy do kierownictwa, jakie szacowanie będzie dawać maksymalne efekty, przy jednocześnie małym nakładzie czasu i pracy [82][60].

3. **Estymowanie ryzyka**

Związane jest z oszacowaniem wielkości strat w przedsiębiorstwie, wynikające z naruszenia bezpieczeństwa informacji i jej utraty oraz oszacowaniem prawdopodobieństwa wystąpienia zagrożenia. Dlatego zaleca się wyznaczyć poziom ryzyka [82].

4. **Ocena ryzyka**

Ten etap podzielony jest na trzy części: identyfikację, analizę i ewaluację ryzyka.

Znalezienie źródeł ryzyka i określenie poziomu niepewności ma na celu identyfikację ryzyka, którą przeprowadza się poprzez zgromadzenie jak największej ilości zagrożeń, i na tej podstawie kompleksowo podchodzi się do stworzenia przejrzystej strategii działania podczas wystąpienia w realu takiego zagrożenia [111].

Niebagatelne zaznaczenie ma też czas zlokalizowania miejsca zdarzenia, bowiem niewykrycie go prowadzi w konsekwencji do strat, a przecież chodzi o zachowanie ciągłości procesu i wprowadzenie zmian. W tym celu korzysta się z katalogu zagrożeń (umieszczonego w podrozdziale 1.1.3. Ocena zagrożeń bezpieczeństwa informacji przedsiębiorstwa), pomocne są również statystyki służb odpowiedzialnych za bezpieczeństwo.

Analizę ryzyka stosuje się w celu ustalenia poziomu zidentyfikowanych ryzyk, określając prawdopodobieństwo i skutki potencjalnych zdarzeń oraz czy i w jakim stopniu zagrażają one organizacji, z określeniem, jakie metody analizy ryzyka i narzędzia zarządzania ryzykiem powinno się zastosować. Okresową analizę ryzyka

zaliczamy niewątpliwie do zaawansowanego elementu zarządzania ryzykiem, gdzie identyfikujemy zagrożenia i dokonujemy pomiaru wielkości ryzyka. Metody stosowane do pomiaru powinny być odpowiednio dobrane m.in. metody jakościowe, ilościowe, mieszane, indukcyjne, dedukcyjne, matrycowe, wskaźnikowe, grafy ryzyka [111]. z zasady, ocena ryzyka powinna być wykonana kilkoma metodami, a ocena końcowa będzie wynikiem najkorzystniejszego wyniku oceny.

Ewaluacje ryzyka należy postrzegać, jako porównanie zidentyfikowanego i przeanalizowanego ryzyka do przyjętych kryteriów jednostki uwzględnionych podczas ustalania na początku kontekstu**.**

5. Akceptacja ryzyka

Dzięki akceptacji ryzyka wiemy jak ryzyko zostało zidentyfikowane, jaki został przyjęty poziom akceptacji, co wskazuje na sposób postępowania z nim.

6. Postępowanie z ryzykiem

Polega na stworzeniu planu postępowania, z występującym ryzykiem. Do takiego planu możemy zaliczyć: wprowadzenie należytych zabezpieczeń, poznanie i świadome zaakceptowanie ryzyka, unikanie go, przeniesienie odpowiedzialności za pojawiające się ryzyko na osoby współpracujące z organizacją. Mogą to być ubezpieczyciele, czy np.: dostawcy różnych usług. Na końcu opracowuje się raport, który zawiera cały proces ryzyka bezpieczeństwa informacji oraz sposób działania powodujący jego minimalizację.

7. Przegląd i monitorowanie ryzyka

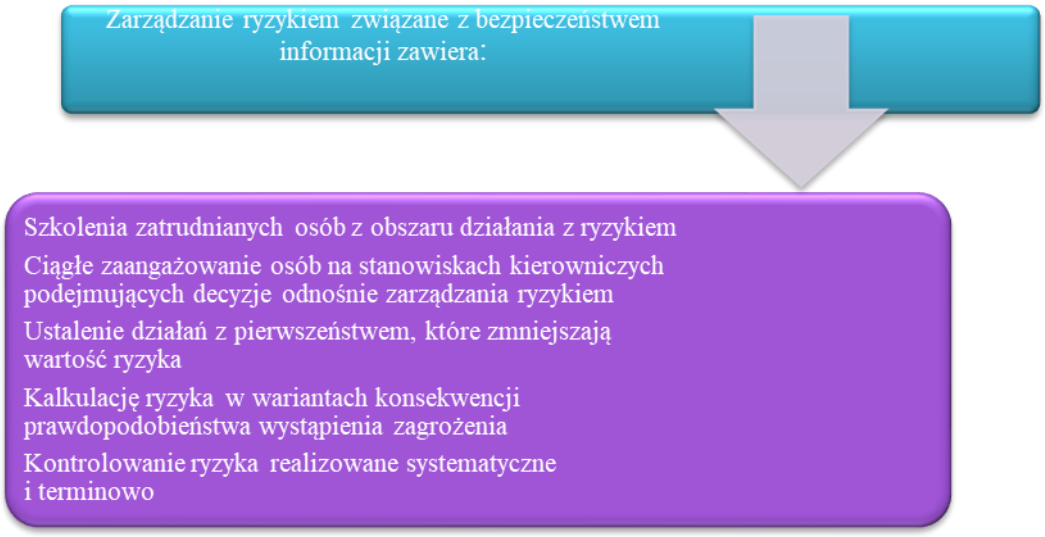
Ostatni element procesu SZBI odpowiadający za identyfikację ryzyka w czasie, który pozwoli na analizę i podjęcie odpowiednich czynności. Do czynników ryzyka, które powinny zostać objęte monitorowaniem zaliczamy m.in. informacje o nowych aktywach zagrożeniach podatnościach incydentach związanych z BI.

Aby skutecznie chronić system, w sytuacji, gdy rozpoznamy zmianę, zaleca się ponowne przeprowadzenie analizy ryzyka, w oparciu o aktualne wartości. Ponadto, zaleca się podczas monitorowania ryzyka zwrócenie szczególnej uwagi na cały proces, a nie na pojedyncze czynniki (np. zadania, które mieli wykonać pracownicy), gdyż wówczas mamy pewność ograniczenia ryzyka do poziomu minimalnego.

Z pomocą przychodzą tutaj cykliczne przeglądy, które skutecznie działają przy zmianach w jednostce w celu korekcji i usprawnienia systemu [112].

Istotne znaczenie w odpowiedniej ocenie sytuacji ma również dostęp do bieżących i rzetelnych informacji oraz umiejętność wykorzystania ich, aby uchronić

organizację przed podjęciem niewłaściwych decyzji, w wyniku błędnie określonego kontekstu, a co za tym idzie niepomyślnie przeprowadzonej analizy i identyfikacji ryzyka [111].



Rysunek 25. Zarządzanie ryzykiem powiązane z bezpieczeństwem informacji
Opracowanie własne na podstawie [111]*[96]*.

Aby przedsiębiorstwa mogły uzyskać odpowiednie zabezpieczenie ważnym jest, aby wdrożenie procesu zarządzania ryzykiem przebiegało w sposób dopasowany do charakteru i specyfiki prowadzonej działalności oraz aby właściwie rozpoznać podatności i słabości mechanizmów kontroli, gdyż mogą one stanowić zakłócenia pracy w organizacji.

2.5. Funkcjonowanie SZBI

W rozważaniach na temat systemów SZBI, można z całą pewnością stwierdzić, że nie są aż tak znane i popularne, jak systemy zarządzania, jakością z serii ISO 9000. Jednak, mimo iż przedsiębiorstwa nie są tak chętne do wprowadzenia SZBI, to z całą pewnością najnowsza norma, 27001: 2017 jest dużą pomocą w poprowadzeniu do dynamicznego rozwoju i może być tzw. drogowskazem w budowaniu bezpiecznej jednostki organizacyjnej. W przytoczonej normie znajduje się model, który może być stosowany w każdej organizacji, niezależnie od rodzaju prowadzonej działalności, wielkości organizacji, statusu prawnego, realizowanych systemów czy struktury organizacyjnej w systemie zarządzania bezpieczeństwem informacji. Aplikowanie systemu wiąże się z podjęciem decyzji strategicznej wypływającej z potrzeb organizacji.

Zastosowanie doskonalącego modelu Planuj-Wykonuj-Sprawdzaj-Działaj (PDCA: Plan-Do-Check-Act) obejmuje przebieg procesów, systemów w całej strukturze SZBI, opierając się o szacowanie ryzyka w projektowaniu, wdrażaniu oraz zarządzaniu bezpieczeństwem informacji, które można wykorzystać we wszystkich systemach zarządzania BI [9]. Podejście procesowe modelu jest podyktowane stosowaniem czterech struktur procesowych, zaciągniętych z modelu Deminga, które mają następujące znaczenie dla użytkownika: (rozdz. 2.1.)

- Przez *Planowanie* rozumiemy opracowanie założeń SZBI, procedur, procesów oraz celów ważnych z punktu zarządzania ryzykiem. Wszystkie działania powinny być dokumentowane tak, aby można było je odtworzyć. W tej fazie dokonuje się identyfikacji oraz szacowania rodzaju ryzyka.
- Poprzez *Wykonuj* rozumie się eksploatację i wdrożenie polityki SZBI, działań ochronnych, połączonych z zabezpieczeniami. Należy poszczególne zasoby przypisać wdrożonym zabezpieczeniom. Faza ta dotyczy też programu uświadamiania, co do potrzeby zarządzania ryzykiem.
- Poprzez *Sprawdzaj* rozumie się monitorowanie i przegląd systemu oraz inne zabezpieczenia w celu szybkiego wykrycia błędów podczas przetwarzania informacji (tworzenie raportów dla kierownictwa). W fazie tej sprawdza się czynności korygujące mechanizmów ochronnych odpowiedzialnych za niedopuszczenie do narażenia organizacji. Do technik testowania należą rutynowe sprawdzanie, samokontrolujące procedury oraz wewnętrzne audyty.
- Poprzez *Działaj* interpretuje się utrzymanie i ciągłe doskonalenie SZBI, opatrzone działaniami korygującymi wprowadzonymi w poprzedniej fazie testów, popartymi wynikami z audytów, jak i wniosków kierownictwa [9, 113]

Poniżej opisano bardziej szczegółowo każdy z wymienionych etapów zarządzania bezpieczeństwem informacji z perspektywy doskonalącego modelu Deminga.

➢ **Planuj: Ustanawianie SZBI**

Jednym z pierwszych zadań w celu ustanowienia SZBI będzie określenie zakresu i ram systemu bezpieczeństwa informacji. Należy określić cel, dla którego został zaprojektowany system, zdefiniować zasad oraz zrozumieć wymagania BI. Należy zastanowić się, co będzie podlegało chroniło, bo przecież wszystkich aktywów nie można objąć ochroną. Spowodowałoby to brak konkurencyjności dla klientów oraz partnerów handlowych. Podczas podjęcia decyzji o wdrożeniu SZBI koniecznym jest uwzględnienie następujących po sobie procesów. Kluczem do zaprojektowania

omawianego systemu jest wsparcie się wynikami szacowania ryzyka. Na etapie wdrażania, utrzymania i rozwoju sytemu niezbędne są działania, które wskazuje rysunek 26.

Rysunek 26. Etapy ustanawiania SZBI
Opracowanie własne na podstawie [17].

Każda organizacja może zaprojektować własny, indywidualny SZBI, ale w przypadku wdrożenia normy z serii ISO/IEC 27001 i ubiegania się o certyfikat niezbędne jest spełnienie omawianych wymogów. Wszystkie, zatem wymagania winny być wnikliwie przeanalizowane i nie może to być deklaracja, lecz dowód stosowania. Ważnym jest, iż w systemie tym nie można dokonywać różnych wyłączeń, jednak można dokonać zmian wobec określonych zabezpieczeń po spełnieniu kryteriów zaakceptowania ryzyka. Wprowadzenie takich zmian nie może jednak wpłynąć na zmianę poziomu ryzyka i obniżenie standardu. Zatwierdzenie takich zmian wymaga wcześniejszego udokumentowania, a w każdym wariancie niezbędna jest weryfikacja pod kątem adekwatności, wystarczalności i efektywności.

Pierwszym krokiem, jaki powinna wykonać firma jest zdefiniowanie zakresu granic systemu BI. Przecież nie wszystko w firmie podlega ochronie. Więc należy dokładnie określić, co, gdzie, kiedy i jak powinno się chronić. Jeśli wszystko w przedsiębiorstwie będzie zabezpieczone to bardzo szybko organizacja stanie się niedostępna dla partnerów, a towary jej mało atrakcyjne. Dlatego każda jednostka powinna zdefiniować własną politykę bezpieczeństwa informacji z uwzględnieniem procesów SZBI [9].

Bardzo ważnym etapem we wdrażaniu i ustanawianiu SZBI jest identyfikacja ryzyka, która bazuje na wskazaniu zasobów oraz przypisaniu do nich zagrożeń, podatności oraz skutków wystąpienia niebezpieczeństwa.

Norma definiuje również konieczność analizy i oceny ryzyka. W tym zakresie koniecznym jest: oszacowanie strat i szkód biznesowych wynikających z naruszenia bezpieczeństwa informacji w organizacji, oszacowanie realnego poziomu wystąpienia takiego zdarzenia, wyznaczenie poziomu ryzyka, stwierdzenie i ustalenie, czy ryzyko jest na poziomie akceptowalnym [15, 17, 114, 82,].

Należy mieć na uwadze, że lista zabezpieczeń z załącznika A zawarta w normie 27001: 2017 nie jest ostateczna i w szczególnych przypadkach może zaistnieć konieczność zastosowania uzupełniających zabezpieczeń. Wykaz wszystkich zaimplementowanych zabezpieczeń i uzasadnienie ich wyboru należy zaznaczyć w tzw. deklaracji stosowania SZBI [115].

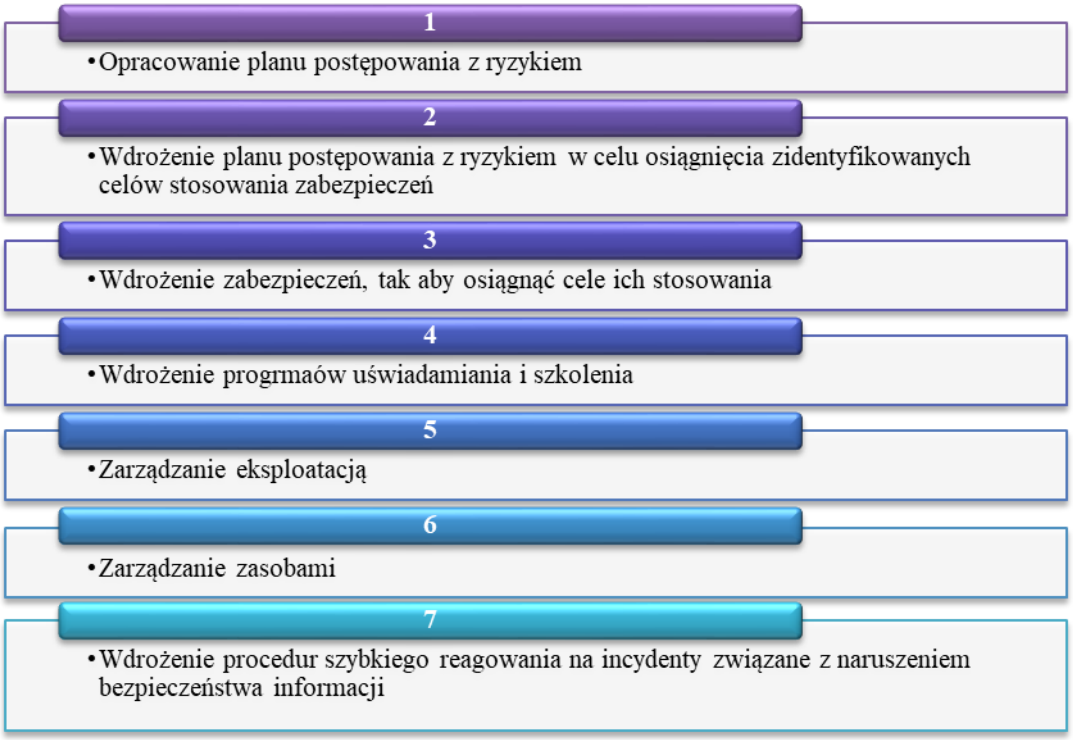
Uzgodnione cele zabezpieczeń oraz zaproponowane ryzyko szczątkowe powinno być zaakceptowane przez kierownictwo organizacji. Po uzyskaniu takiej zgody dopiero można wdrożyć SZBI do realizacji i eksploatacji.

- **Wykonuj: Wdrażanie i stosowanie SZBI**

Informacje o wdrożonej PBI, zabezpieczeniach oraz procesach stanowi dopiero podstawę do wdrożenia SZBI. Decyzja kierownictwa organizacji o wdrożeniu systemu będzie podyktowana wcześniejszym określeniem ryzyka szczątkowego i jego akceptacją. Już sama procedura wdrożenia wymaga znacznego zaangażowania się organizacji i podjęcia stanowczych kroków oraz przygotowania całej dokumentacji wdrożeniowej, gdyż system wymaga przeszkolenia kadry pracowniczej, co do podstawowych zasadach bezpieczeństwa informacji oraz stworzenia planu postępowania z ryzykiem.

Przeprowadzenie szkoleń uświadamiających pracownikom powody, dla których wdrożono system i nałożenie na nich dodatkowych obowiązków ma duże znaczenie dla skuteczności stosowania przyjętych zasad. Szkoleniem powinien zostać objęty cały personel firmy, począwszy od najwyższego kierownictwa po pracowników szeregowych. Ponadto, powinno ono być przeprowadzane w sposób okresowy, obejmując tematy kompleksowej ochrony informacji, zasad przyjętych w ramach systemu, udokumentowane sprawdzianem wiedzy pracowników, jaki i ich podpisem.

Sukces całego projektu polega na widocznym zaangażowaniu kierownictwa i poważnym traktowaniu przyjętych procedur. Zdarza się, że choć firma posiada wiedzę i środki do samodzielnego projektowania systemu, to jednak zatrudnia konsultantów z zewnętrznej firmy.



Rysunek 27. Strategia postępowania podczas zastosowania SZBI
Źródło: Opracowanie na podstawie [9].

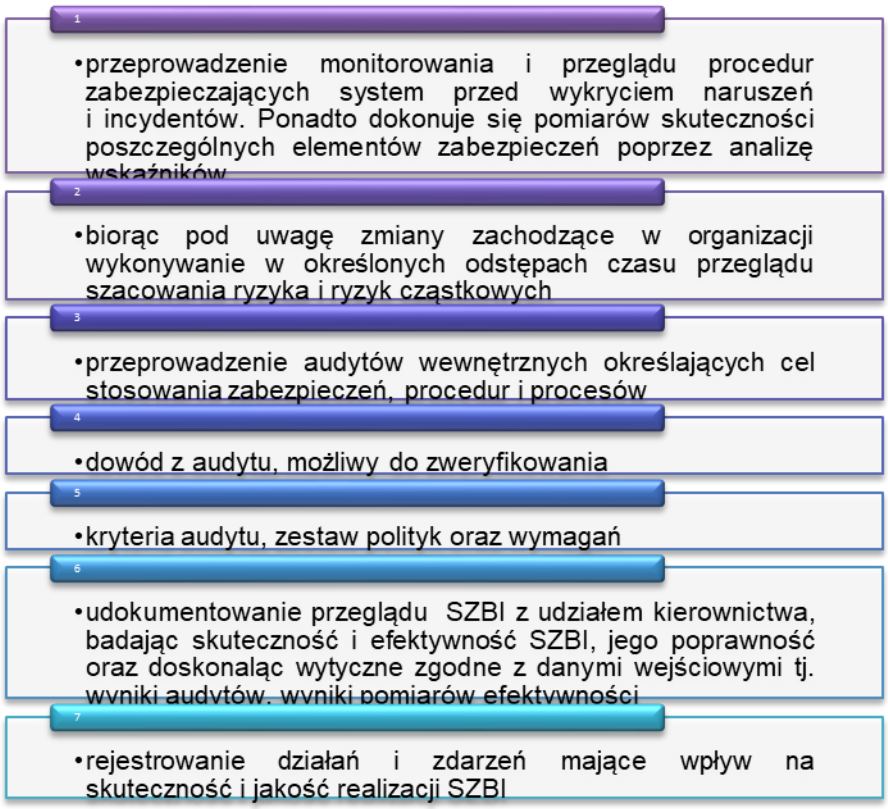
Mimo, że są to ogólne wymagania, to jednak definiują strategię i kierunki działań w systemie. Nawiązują bezpośrednio do oczekiwań, dotyczących ustanowienia oraz wdrożenia systemu. Wskazują też nowe kierunki rozwiązań, dotyczących zabezpieczeń wskazanych w deklaracji stosowania. Spełnienie w/w elementów może spowodować wdrożenie etapów zabezpieczeń zgodnych z celami i PBI [9].

- **Sprawdź: Monitorowanie i przegląd SZBI**

Dobrze działający system zarządzania bezpieczeństwem informacji powinien podlegać monitorowaniu i przeglądzie tak, aby można było zidentyfikować błędy, wykrywać aktualnie pojawiające się zakłócenia w bezpieczeństwie, kontrolować wykonywane obowiązki przez pracowników, zgodnie z oczekiwaniami pracowników oraz od razu uzyskiwać informacje o sprawności i efektywności istniejących zabezpieczeń systemu.

Ważnym są również szkolenia uświadamiające pracowników o postępowaniu zgodnym z przyjętymi zasadami w PBI. Niezbędne jest ustawiczne weryfikowanie i przestrzeganych procedur przez okresowe audyty wewnętrzne [115].

W ramach monitorowania i przeglądu SZBI wymaga się następujących działań:



Rysunek 28. Postępowanie podczas monitorowania i przeglądu SZBI

Opracowanie na podstawie [9,15].

- **Działaj: Utrzymanie i doskonalenie SZBI**

SZBI dotyczy również utrzymania i doskonalenia omawianego systemu. Działaniom naprawczym powinny podlegać niedociągnięcia i wady w systemie. Informacje o zagrożeniach pojawiają się w oparciu wyniki uzyskane na drodze audytu SZBI oraz przeglądów zrealizowanych przez kierownictwo organizacji. Niezwykle ważnym są również uwagi od partnerów, którzy mogli naruszyć system bezpieczeństwa.

Procedury związane z działaniami korygującymi powinny być zawsze udokumentowane. Zatem, działania prewencyjne w celu ochrony przed powstaniem niezgodności mają ogromne znaczenie [17] [115] [9].

Organizacja, która chce utrzymać certyfikat SZBI powinna wdrożyć system wraz z działaniami doskonalącymi, podjąć działania ochronno-zapobiegawcze, poinformować swoich klientów i partnerów o podjętych działaniach oraz zapewniać organizacji skuteczne efekty wytyczonych przedsięwzięć. Ogół tych działań ma na celu wyeliminowanie nieprawidłowości w systemie.

Wszystkie te czynności, zmierzające do utrzymania i nadzorowania systemu znacznie wpływają na skuteczność utrzymania ustalonego poziomu bezpieczeństwa tzw. poziomu atrybutów bezpieczeństwa omawianego w podrozdziale 1.1. Takie czynności powinny być z góry zaplanowane, wtedy zawczasu będą eliminowane pojawiające się niezgodności. Postępując w ten sposób organizacja w sposób ciągły poprawi skuteczność SZBI, a nawet, jeśli dojdzie do nieprawidłowości to będą one szybko rozeznane i wyeliminowane działaniami korygującymi.

- **Zalety wdrożenia systemu SZBI**

Zapewnienie bezpieczeństwa informacji okazuje się kłopotem, dylematem oraz utrudnieniem większości przedsiębiorstw, którym nie udaje się zastosować mechanizmów kontroli podczas przetwarzana informacji oraz reguł, usprawniających ciągłość pracy na rynkach polskich czy zagranicznych. W dobie nowych technik, pokazujących nowe możliwości urządzeń, oprócz tych pozytywnych stron pojawiają się również i te negatywne, które mogą doprowadzić do krytycznej sytuacji. Wiele organizacji jest, więc bardzo ostrożnych sprawdzając inne podmioty pod kątem wiarygodności i poziomu bezpieczeństwa podczas przetwarzania informacji [17].

Dlatego też z pomocą takim organizacjom przychodzi zaaplikowanie systemu zarządzania bezpieczeństwem informacji (SZBI).

Niezaprzeczalnie należy stwierdzić, że dysponenci pracujący w ramach tego systemu wykazują się znacznym poziomem świadomości w postrzeganiu wagi BI. Takie działanie powiązane jest z szybką identyfikacją ewentualnych zagrożeń w wielu obszarach jednostki organizacyjnej. Tym samym ogranicza się skutki ujawnienia poufnych informacji, zniszczenia jej, strat finansowych, utraty wiarygodności, awarii, co ma kluczowe znaczenie w stosunku do ponoszonych kosztów w organizacji [17].
Poniżej przedstawiono wybrane korzyści wewnętrzne i zewnętrzne, wynikające z zastosowania SZBI. Oto niektóre z korzyści wewnętrznych:

- Następny etap w rozwoju firmy, podwyższenie sprawności personelu
- Zagwarantowanie zgodności z wymogami prawa, poprzez systemowe podejście do spełniania wymagań prawnych
- Wiedza, która powoduje wpływ na zdarzenia wewnątrz organizacji
- Zabezpieczenie informacji w przypadku wystąpienia jakieś katastrofy lub też awarii
- Zwiększona świadomość załogi pracującej w obszarze ochrony informacji- edukowanie pracowników
- Uniknięcie (uniknięcie) kar za naruszenie BI
- Ochrona informacji w przedsiębiorstwie
- Usprawnienie przepływu i dostępu do informacji podczas wzrostu bezpieczeństwa procesów realizowanych w jednostce gospodarczej
- Wdrożenie mechanizmów okresowej weryfikacji efektywności stosowanych zabezpieczeń
- Określenie odpowiedzialności i uprawnień pracowników w zakresie BI
- Oszacowanie ryzyka, dotyczącego zarządzania informacją
- Budowanie zaufania do własnej organizacji
- Utwierdzenie kontrahentów, dostawców organizacji oraz osób trzecich, że ich dane są odpowiednio przechowywane
- Przestrzeganie zasad, odpowiedzialności, procedur, i podejmowania działań (pracownicy wiedzą, kto ma, jakie obowiązki)
- Pracownicy wiedzą jak postępować w zakresie ochrony informacji
- Działania pod kątem usystematyzowanie dokumentów pod wymagania standardu ISO/IEC 27001:2017
- Wprowadzenie okresowych audytów BI oraz inne mechanizmy kontroli oceny i doskonalenia
- Wdrożenie i utrzymanie mechanizmów potrzebnych do utrzymania ciągłości działania w organizacji
- Podejście BI oparte na zarządzaniu ryzykiem
- Rozwój kompromisowych i elastycznych działań poprzez lepsze dopasowanie struktury do wewnętrznych i zewnętrznych wymagań funkcjonowania
- Przedsiębiorstwo bezpieczeństwa fizycznego i informatycznego informacji
- Zmniejszenie ryzyka utraty, dezinformacji, niepowołanego dostępu do wewnętrznych informacji

- Zarządzanie systemami informatycznymi i sieciami komputerowymi pod kątem BI
- Uszczegółowienie precyzyjnie przyczyn powstania ryzyka, i przeciwdziałanie jego powstaniu
- Przewidywanie zagrożeniom poprzez wprowadzenie rozwiązań pomagających w wykrywaniu potencjalnych incydentów bezpieczeństwa [17].

Biorąc pod uwagę korzyści wskazać można następujące:

- W sposób zorganizowany odbywa się zarządzanie BI
- Zwiększenie wiarygodności wśród kontrahentów nawet zagranicznych
- Stwierdzenie wysokiego poziomu kultury organizacji
- Zaznaczenie wysokiej pozycji na rynku wśród konkurencyjnych firm
- Spełnienie wymagań i oczekiwań przetargowych w obszarze informacji
- Niezależny nadzór wykonywany przez jednostki zewnętrzne
- Uwiarygodnienie jednostki gospodarczej w oczach kontrahenta, dla którego bezpieczeństwo jest bardzo ważne
- Poszanowanie wynikające z uzyskanych certyfikatu SZBI
- Pozyskiwanie nowych klientów z nowych obszarów, dla których spełnienie wymagań określonych w norm jest jednym z podstawowych warunków nawiązania współpracy handlowej
- Progres w wizerunku jednostki, jako bezpiecznego, wiarygodnego i nowoczesnego partnera handlowego [17].

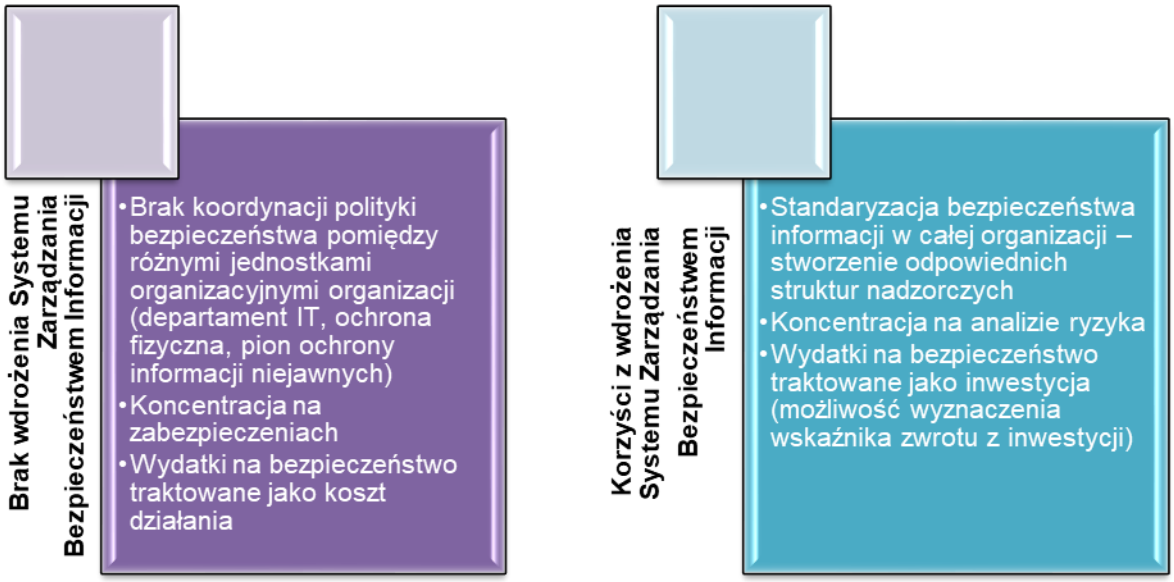
Uzyskując certyfikat z zakresu zapewnienia BI jednostka gospodarcza buduje profesjonalny wizerunek jednostki gospodarczej godnej zaufania, a co za tym idzie wzrasta prestiż organizacji oraz jej produktów w oczach obecnych klientów, ale i tych potencjalnych. Tym samym, zwiększa poczucie pewności i zaufania do firmy, czym podnosi wiarygodność i zapewnienie, że powierzone, przetwarzane informacje są chronione. Istotną kwestią jest też uzyskanie efektu postrzegania przez partnerów, jako organizacji oferującej produkty i usługi na najwyższym poziomie w obszarze BI.

Reasumując, istniejący stan wiedzy pozwala na wytypowanie korzyści wdrożenia SZBI dla kontrahenta, partnera i osób trzecich w jednostce organizacyjnej. Należą do nich:

- zadowolenie klientów, i zwiększenie satysfakcji w wyniku spełnienia jego oczekiwań poprzez zastosowanie się do zasad sytemu zarządzania BI;
- zapewnienie kontrahentów i potencjalnych partnerów, że ich dane są właściwie chronione;
- wszyscy współpracownicy wiedzą, kto, za co odpowiada i jak maja postępować w zakresie ochrony informacji, znają procedury i odpowiedzialność za nieprzestrzeganie zasad współpracy.

Wdrożenie SZBI zapewnia organizacji szereg przesłanek, adekwatnych do zagrożeń, wymagań biznesowych i tych wynikających z przepisów prawa.

Istnieje zdecydowana przewaga korzyści, jakie daje SZBI, czego przykładem jest poniższy rysunek zestawiający funkcjonowanie przedsiębiorstwa przed i po wprowadzeniu systemu SZBI.



Rysunek 29. Wynikające korzyści oraz ich brak z wdrożenia SZBI
Źródło Opracowanie własne na podstawie [97] [114].

Zatem, omawiany system bezpieczeństwa informacji cechuje się stabilną i bezawaryjną pracą we wszystkich krytycznych systemach informatycznych. Możliwe jest to dzięki wyselekcjonowaniu efektywnych i w pełni skutecznych zabezpieczeń. Ma to nadrzędne znaczenie, dla jakości świadczonych usług, chroniąc się przed możliwością utraty relacji z partnerami biznesowymi, zwiększając tym samym skuteczność planowania i podejmowania strategicznych decyzji na podstawie danych w systemie.

Natomiast w przypadku wystąpienia uchybień, jakość informacji wpłynie na szybkość znalezienia odpowiedniego rozwiązania problemu i od razu wprowadzenia działań korygująco naprawczych.

Ważnym czynnikiem jest powołanie zespołu zarządzającego ryzykiem, składającego się z członków każdego działu w celu szerszego spojrzenia na wystąpienie ryzyka oraz jego agregacji [116]. Odpowiedzialność za udostępnienie zasobów i implementacja zabezpieczeń powinna zostać przypisana nie jednej osobie, lecz

odpowiedzialnym kierownikom, gdyż ułatwi to wskazanie właściciela danego zasobu i który będzie też odpowiedzialny za codzienną ochronę.

Należy podkreślić, że przypisywanie odpowiedzialności powinno być zawarte w PBI. W organizacjach to najczęściej pełnomocnik ds. bezpieczeństwa informacji będzie odpowiedzialny za rozwój i implementację bezpieczeństwa oraz jego pomoc będzie nieodłączną częścią identyfikacji zabezpieczeń. Podczas tak przyjętych założeń należy mieć na uwadze, że w wyniku planowanych działań, związanych z postępowaniem z ryzykiem zawsze pozostaje kwestia akcentacji ryzyka szczątkowego.

2.6. Praktyczne przykłady systemów bezpieczeństwa informacji

W dostępnej literaturze przedmiotu można znaleźć różne przykłady rozwiązań propozycji doskonalenia zarządzania bezpieczeństwem informacji w postaci modelu, projektów, które wskazują na zwiększenie skuteczności podatności na zagrożenia [42, 117, 118].

Należy tutaj wspomnieć chociażby o modelu zarządzania BI, który obejmuje strukturę organizacyjno-techniczną oraz narzędzia zarządzania czynnikiem ludzkim, który opracowano na podstawie wyników analizy ryzyko utraty BI przeprowadzonej za pomocą metod FMEA oraz Pareto Lorenza. Zaproponowany model posłużył, jako rozwiązanie problemów dotyczących zarządzania BI, wskazując kierunki zmian organizacyjno- technicznych oraz szkoleniowych, które w istotny sposób wpływają na wzrost BI podmiotów gospodarczych. W modelu przyjęto, że o jego skuteczności działania będą decydować funkcjonalności zaprezentowanych podsystemów zarządzania, mianowicie: ochrony fizycznej, aktywów informacyjnych, świadomości, uprawnieniami, odejściami pracowników, bezpieczeństwem prawnym, kulturą bezpieczeństwa informacji oraz nadużyciami. Pierwszym elementem innowacyjnym, zaproponowanego modelu jest zarządzanie kulturą bezpieczeństwa informacji odnosząca się do promowania dobrych praktyk, postaw i zasad wskazanych w PBI organizacji. W opinii autora pracy [117] możliwe jest to dzięki zaangażowaniu najwyższego kierownictwa. Wówczas pracownicy będą zobowiązani do przestrzegania założeń, przekonań opartych o PBI i może wzbudzić to w nich większe poczucie odpowiedzialności za wykonywanie założonych celów, identyfikowanie nowych zagrożeń oraz monitorowanie ryzyka. Ponadto autor pracy wskazał na inne założenie

zarządzania kulturą bezpieczeństwa, mianowicie codzienne przyzwyczajenie pracowników, które w istotny sposób wpływa na nieprzestrzegania obowiązujących zasad w organizacji (dotyczy to najczęściej osób o niskiej motywacji, czy też innym światopoglądzie). Kolejnym innowacyjnym elementem jest zarządzanie nadużyciami, które wkomponowuje się w obszar zarządzania kulturą bezpieczeństwa. Ma ono na celu zwalczanie oraz, co ważniejsze zapobieganie nadużyciom, jakich mogą dopuścić pracownicy. Dzięki wcześniejszej profilaktyce można znacząco ograniczyć zakres strat i szkód opracowując schemat postępowania w sytuacji zdiagnozowania nadużycia. Omawiany model spełnia 2 funkcje bezpośrednią związaną z minimalizacją ryzyka oraz pośrednią pomocną w realizacji celów i zamierzeń w organizacji [117].

Dokonując dalszej interpretacji warto powołać się również na źródło, jakim jest opracowanie naukowe [42] w którym jest zamieszczony model procesu zarządzania ryzykiem w jednostkach administracji samorządowych w aspekcie zarządzania kryzysowego [42]. Model prezentuje udoskonalenie wprowadzonych już zadań jednak proponuje, aby być przygotowanym na pojawienie się zagrożenia oraz od razu minimalizować skutki jego powstania. Model obejmuje działania organizacyjne wraz ze stosowaną metodyką analizy ryzyka i jego zarządzania, które usprawni system. Zaprezentowany model uwzględnia zależności między założeniami dotyczącymi kierowników zmian w zakresie zarządzania ryzykiem a dziedzinami, których te zmiany dotyczą. Zmiany te dotyczą czterech obszarów tzn. elementów modelu, obszarów wymagających zmian, kierowników zmian, koncepcji zmian. Zdaniem autora pracy znacznego doskonalenia wymagają obszary: niedostatecznego wykonywania zadań całego procesu zarządzania ryzykiem, deficyt w standardach zarządzania ryzykiem, niedostateczna ilość wyszkolonej kadry pracowniczej, nie ma systemu zarządzania ryzykiem, który obejmowałby większość szczebli administracyjnych, źle dobrane metody zarządzania ryzykiem, brak pełnej dokumentacji związanego z zarządzaniem ryzykiem oraz brak regularności w dokonywaniu czynności związanych z zarządzaniem ryzykiem w tym analizy ryzyka. Elementami nowej koncepcji zmian zarządzania ryzykiem było zaproponowanie zmian dotyczących: terminologii, standaryzacji procesu, dokumentacji, etapów procesu metodyki liczenia ryzyka, wspomagania komputerowego procesu oraz samego systemu. W pracy powołano się na zmianę dotyczącą metody analizy ryzyka „schodkową", obejmującą wartości prawdopodobieństwa, strat oraz siły wpływu negatywnego, dla których kolejno tworzy się macierz ryzyka. Metoda schodkowa dotyczy również występowania zdarzeń

negatywnych, które mogą generować zagrożenia, dlatego i dla nich również oblicza się ryzyko. Model posiada odzwierciedlenie w koncepcji zarządzania ryzykiem [42].

W podobnym kontekście jest przytoczony w pracy naukowej [118], autorski model opierający się na normie ISO 27001. Model w sposób czytelny i łatwy prezentuje obszary zgodności z przepisami, zarządzania aktywami oraz incydentami i zagrożeniami. Autor pracy pogrupował 12 obszarów tematycznych z normy 27001 w 3 główne, mianowicie: zgodność z przepisami, zarządzanie aktywami oraz zarządzanie incydentami i powstałymi zagrożeniami. Warto zaznaczyć także, że zaprezentowane rozwiązania w modelu są odpowiedzią na pojawiające się niedoskonałości systemu zarządzania BI. Jednak nie obejmują wszystkich środków, które mają istotny wpływ na ulepszenie procesu BI.

W fachowej literaturze opisano rozwiązania doskonalące koncepcje systemu zarządzania bezpieczeństwem informacji, zwiększające skuteczność podatności na zagrożenia. Rozwiązania te w swojej strukturze i idei mają za zadanie minimalizować powstawanie nowych zagrożeń. Niektóre z prezentowanych modeli są bardziej dostosowane do struktury organizacji, inne z kolei mniej. Jednak reasumując aktualny stan wiedzy nadal można wytypować w strukturze organizacji obszary, które wymagają dalszego udoskonalenia i wdrożenia innowacyjnych rozwiązań, bardziej dopasowanych do nowo pojawiających się zagrożeń. Stosowane zabezpieczenia w pełni nie nadążają i nie zabezpieczają organizacji przed dynamicznie przyrastającymi niebezpieczeństwami. Stąd też, mechanizmy szybkiego reagowania muszą posiadać dobrze dopasowane funkcje systemu reagowania, na potencjalne zagrożenia.

Dlatego też, wdrożenie odpowiedniego systemu BI, wpasowanego będzie w potrzebą zabezpieczenia przedsiębiorstwa. Zabezpieczenia stosowane w organizacjach nie są wystarczające, więc powstają luki w systemie BI.

3. CEL i ZAKRES ROZPRAWY

3.1. Geneza podjęcia tematu pracy

Aby odpowiednio zdiagnozować istniejący stan wiedzy dotyczący, tematyki rozprawy doktorskiej dokonano przeglądu literaturowego: fachowych publikacji, czasopism naukowych oraz książek, które interpretują obszar zainteresowań pracy autora. W rozdziale 1 dokonano analizy dostępnych źródeł w aspekcie bezpieczeństwa, wskazując na standardy normatywne oraz ustawodawstwo, jako te, które poruszają obszar propozycji ochrony jednostek gospodarczych przed podatnościami, które realnie mogą wywołać zagrożenie. Jednak należy zauważyć, że w aktach normatywnych temat bezpieczeństwa informacji jest poruszany dość ogólnikowo, nie wgłębiając się w omówienie szczegółowo sposobów dotyczących wprowadzania metod i zasad utrzymania bezpieczeństwa informacji. W rozdziale 2 wskazano rolę i zadania SZBI. Jednak istnienie mnogości aktów prawnych, rozporządzeń, ustaw, czy norm polskich, europejskich powoduje powstanie chaosu informacyjnego w wyniku, którego nie dysponując odpowiednią wiedzą można zmarginalizować wiele istotnych podatności na zagrożenia. Pomimo wykorzystywania technicznych środków ochrony typu: antywirusy, firewall-e, IDS-y, przedsiębiorcy stykający się z różnymi nowymi podatnościami wywołującymi zdarzenia, które w konsekwencji doprowadzają do naruszenia bezpieczeństwa systemu, w którym przetwarzane są informacje. W związku z tym są istotnie zainteresowani propozycjami adekwatnych zabezpieczeń, które ochraniałyby ich przedsiębiorstwa przed utratą, ujawnieniem, modyfikacją, zniszczeniem informacji. Zarządy organizacji świadome powstałych luk w systemie poszukują prostych i szybkich metod identyfikowania nowo powstałych zagrożeń, połączonych z prawidłowym zarządzaniem ryzykiem.

Nie ulega wątpliwości fakt, że przy najlepszych zabezpieczeniach brak kontroli ich zasad przestrzegania lub też pobieżne respektowanie wybranych zabezpieczeń, może doprowadzić do ujawnienia informacji. Stąd potrzeba regularnej analizy ryzyka, która uświadomi zarządzającym konsekwencje braku wdrożenia wymaganych zasad przestrzegania zabezpieczeń.

Zaobserwowano problemy dotyczące samej metodyki analizy ryzyka, trudności w przeprowadzeniu procesu szacowania ryzyka, co przekłada się na brak regularności w jej wykonywaniu. Nie bez znaczenia jest nie ustanowienie osoby odpowiedzialnej za zredukowanie poziomu ryzyka. Ponadto, zaobserwowano braki w edukowaniu

pracowników w zakresie przeprowadzania takich analiz i oceny bezpieczeństwa informacji. Problem również stanowi niedostatecznie dobrze dobrana grupa personelu zapraszana na szkolenia, ograniczająca się najczęściej do pracowników wyższego szczebla, zapominając o pozostałym personelu.

Pojawienie się tych problemów spowodowało niedostateczne zabezpieczenie organizacji gospodarczych przed sytuacjami zagrażającymi, dlatego też sprecyzowano przedmiot i cel badań, które przyjmuje opracowanie modelu systemu zmniejszenia ryzyka utraty informacji. Niemożliwe jest zabezpieczenie organizacji przed nieznanym zagrożeniem, z tego też względu nieodzownym jest potrzeba identyfikacji pojawiających się zagrożeń. Ich znajomość umożliwia odpowiednie zabezpieczenie posiadanych zasobów, poprzez staranne dobranie odpowiednich zabezpieczeń. Organizacje korzystają wielokierunkowo ze środków zaradczo ochronnych, do których należą między innymi:

- zabezpieczenie programowo sprzętowe, zapory ochronne oddzielające ochraniany system od otwartych sieci o powszechnym dostępie, wykrywające włamania;
- system weryfikacji użytkownika (karta jednokrotnych haseł, który wyświetla zmienny ciąg znaków), osobisty numer PIN;
- szyfrowanie danych, aby nie dopuścić do ujawnienia informacji podczas jej transmisji; użycie kryptografii powoduje, że odczytanie tekstu staje się praktycznie niemożliwe bez dysponowania kluczem prywatnym oraz kluczem publicznym;
- stosowanie podpisu cyfrowego, który uwiarygadnia dokumenty elektroniczne, przy czym moc prawna podpisanego dokumentu jest taka sama, jak oznaczonego podpisem tradycyjnym;
- oprogramowanie antywirusowe;
- stosowanie narzędzi archiwizujących, skracające czas zapisu backup;
- ochrona przeciwpożarowa zasobów informatycznych;
- ochrona fizyczna przed dostępem do budynku osób nieupoważnionych;
- ochrona przed emisją elektromagnetyczną (Klatka Faradaya, użycie włóknistych materiałów przewodzących poprzez ściany, sufity, podłogi oraz komputery osobiste z zakłóceniami źródła wejścia).

Szerzej podział zabezpieczeń wraz z podziałem na kategorie, stosowane przez przedsiębiorstwa omówiono w rozdziale 2 (ponadto opisy przeprowadzenia ochrony prawnej, fizycznej wartości, fizycznej informacji, fizycznej obiektu, technicznej, sprzętowo programowej, organizacyjnej, administracyjnej czy teleinformatycznej przedstawiono w następujących pozycjach [107, 15, 59, 11]).

W organizacjach brakuje przejrzystego systemu BI uwzgledniającego zdecydowaną większość obszarów możliwego ujawnienia informacji (systemów i podsystemów przynależnych do organizacji). Obszary te powinny obejmować personel, narzędzia, techniki, metodę. W organizacjach rozumianych, jako całość zatrudnionego personelu nie przywiązuje się odpowiedniej wagi do wiedzy o BI traktując ją, jako powszechną i oczywistą. W skutek tego często zasady i wskazówki dotyczące BI nie wykraczają poza kierowników zarządzających. Dbając o wizerunek i dobre imię organizacji, należy uczynić zadaniem priorytetowym przekazanie listy potencjalnych zagrożeniach oraz sposobów ochrony przed nimi wszystkimi pracownikom przedsiębiorstwa.

Celem pracy jest zidentyfikowanie aktualnych czynników zagrażających bezpieczeństwu informacji w badanych organizacjach i opracowaniu systemu, który wyposażony będzie w funkcje autoadaptacji, umożliwiające dynamiczne reagowanie na pojawienie się nowych zagrożeń.

Przedmiot badań

Analizując zasady zawarte w aktach prawnych czy standardach dotyczących SZBI może się wydawać, że organizacje są należycie zabezpieczone przed zagrożeniami. Jednak należy zauważyć, iż mimo zdobytej wiedzy dalej zauważa się występowanie szeregu naruszeń i zagrożeń ujawniających niedostateczne zabezpieczenia aktywów posiadanych w organizacjach. Przedsiębiorstwa nie wiedzą, jak w prosty sposób wprowadzić zmiany, zapewniające kompleksową ochronę procesów informacyjnych, gwarantujących utrzymanie równowagi między skutkami zagrożeń a poniesionymi kosztami wprowadzanych zabezpieczeń. Ważnym elementem jest również sposób przekazu zasad BI oraz sposób wdrożenia środków bezpieczeństwa, które okazują się zawiłe i znacznie odbiegają od przejrzystej formy, której tak bardzo potrzebują organizacje. W związku z powyższym występuje konieczność zdefiniowania problemu badawczego. W celu skonkretyzowania omawianego problemu badawczego posłużono się następującymi pytaniami:

- W jakie systemy ochrony wyposażone zostały przedsiębiorstwa?

- Czy stosowane zabezpieczenia są na tyle dobre, aby wystarczająco i należycie ochronić organizacje przed zagrożeniami?
- Na jakie czynniki powinien być ukierunkowany projekt systemu zarządzania bezpieczeństwem informacji w jednostkach gospodarczych?
- Z jakich etapów powinien składać się proces wprowadzania projektu systemu zarządzania bezpieczeństwem informacji w organizacjach?
- Czy mnogość aktów prawnych regulujących temat bezpieczeństwa informacji powoduje, że przedsiębiorcy muszą szukać innych prostszych i szybszych rozwiązań?

W celu udzielenia odpowiedzi na postawione pytania problemowe zostały przeprowadzone badania. A w wyniku tak postawionych pytań problemowych postawiono hipotezę badawczą.

3.2. Cel pracy i hipoteza badawcza

W wyniku tak postawionych problemów badawczych w pracy postawiono następującą hipotezę:

„Intensywny wzrost ilości zagrożeń bezpieczeństwa informacji w przedsiębiorstwach wymaga stosowania adaptowalnych systemów zarządzania bezpieczeństwem, w których środki techniczne i proceduralne dostosowane będą do wymagań określonych aktualnymi analizami ryzyka utraty informacji".

W związku z tak postawioną hipotezą określono cel w dwóch aspektach tzn. naukowym i utylitarnym.

Z uwagi na sytuację problemową dotyczącą poziomu bezpieczeństwa informacji w przedsiębiorstwach oraz wynikającej z niej potrzeby przeprowadzenia badań w dziedzinie ujętej w tytule rozprawy, przyjęto cel dysertacji, jako: *określenie aktualnego poziomu bezpieczeństwa informacji w badanych przedsiębiorstwach z branży automotive wskazując na zastosowanie innowacyjnej metodyki analizy ryzyka. Wiąże się to z poznaniem źródeł zagrożeń, przeanalizowaniem poziomu zabezpieczeń wybranej grupy przedsiębiorstw, które znacząco wpływają na ryzyko utraty informacji.*

Aby udowodnić cel naukowy oraz utylitarny konicznym jest przeprowadzenie badań, w tym analizy ryzyka poszczególnych podatności innowacyjną metodą szacowania ryzyka.

Natomiast celem utylitarnym pracy będzie opracowanie koncepcji wytycznych w zakresie zarządzania bezpieczeństwa informacji dla grupy przedsiębiorstw, które będą uwzględniały pomijane dotychczas czy bagatelizowane zagrożenia bezpieczeństwa

informacji. W nowo powstałym systemie będą uwzględnione zidentyfikowane zagrożenia utraty informacji ukierunkowane na ochronę BI wraz ze wskazaniem na innowatorski projekt systemu zarządzania bezpieczeństwem informacji dedykowany potrzebom przedsiębiorców.

Badania obejmowały przeprowadzenie następujących etapów:

- Przeprowadzenie badań ankietowych, wywiadu oraz obserwacji ukierunkowanych na określenie poziomu bezpieczeństwa informacji w badanych jednostkach.
- Określenie źródeł zagrożeń i ocenę ich wpływu na działalność oraz funkcjonowanie przedsiębiorstwa.

- Przeprowadzenie procesu szacowania ryzyka utraty bezpieczeństwa informacji za pomocą autorskiej metody oceny ryzyka (przy wykorzystaniu założeń opracowanych przez kancelarię prawną Lubasz i Wspólnicy)
- Opracowanie projektu zarządzania bezpieczeństwem informacji otwartego na potrzeby i preferencje otoczenia wewnętrznego przedsiębiorstwa.

3.3. Charakterystyka grupy badawczej

Relatywnie wąskie grono organizacji jest zobowiązane do wyjątkowego chronienia informacji, jakie tworzy, przetwarza i którymi jest dysponentem. Zaliczamy do tej grupy banki, urzędy, koncesjonowanych dostawców związanych umowami z przemysłem zbrojeniowym. Zdecydowana większość organizacji nie musi,, aż do tego stopnia chronić swoich aktywów. Jednak chcąc utrzymać wysoką pozycję na rynku pracy, dbając o swoje dobre imię oraz klientów powinna chronić informacje, zapewniając im skuteczny poziom ochrony. Do omawianej grupy należą również dostawcy części motoryzacyjnych, którzy do pierwszego montażu zobligowani są zachować poufność wobec zamówionych przez klienta wyrobów, opracowanych projektów i szczegółowych informacji dotyczących produktu [15].

W związku z powyższym w pracy zdecydowano zbadać, w jaki sposób jest przechowywana oraz przetwarzana informacja w przedsiębiorstwach z sektora motoryzacyjnego. Badaniami zostali objęci pracownicy administracyjno- biurowi oraz kadra zarządzająca 9-cioma przedsiębiorstwami, którzy bezpośrednio zarządzają informacją lub też mają bezpośredni wpływ na jej ochronę. Należą do nich:

- Kierownicy wyższego szczebla – osoby zarządzające organizacją np. prezes, vice-prezes, dyrektor określonej sekcji typu produkcji, finansowy, zamówień, sprzedaży
- Kierownicy niższego szczebla – kierownicy określonych działów np. HR, kierownik działu technologii.
- Niekierownicy – osoby, które zajmują się zadaniami na określonych stanowiskach, nie zajmują stanowisk kierowniczych.

Wykorzystana w pracy próba badawcza wynosiła 158 osób.

Pierwszym przedsiębiorstwem jest przedsiębiorstwo (PR1), które zajmuje się usługami projektowymi w gałęziach przemysłu samochodowego, szynowego oraz lotniczego. U podstaw każdej z tych gałęzi stoi wiedza oraz doświadczenie nabyte przez pracowników podczas realizacji projektów dla europejskich liderów w swoich branżach. Firma realizowała projekty dla trzech największych producentów samochodów w Niemczech. Dzięki takiej współpracy firma zdobyła olbrzymie doświadczenie oraz know-how w następujących dziedzinach.

- Urządzenia dla procesów zgrzewania karoserii
- Urządzenia precyzyjnego montażu
- Chwytaki robotów do transportu elementów karoserii (Greifern)
- Urządzenia do procesu walcowania, zagniatania itp. (Falzen)
- Urządzenia do łączenia dwóch elementów karoserii (Schachteln)
- Konstrukcje spawane
- Trawersy
- Sprawdziany
- Oprzyrządowanie do szybkiej realizacji prototypów
- Dokumentacja techniczna

Wykonywane do tej pory projekty dotyczyły elementów zewnętrznego osprzętu w samochodach osobowych. Projekty obejmowały przednie i tylne systemy zderzaków, osłony nadkoli, pokrycia nadkoli tylnie i przednie, progi, kompletne systemy kanałów prowadzenia powietrza, przednia pokrywa silnika CFK, dolna osłona silnika. Natomiast do wewnętrznego osprzętu w samochodach osobowych firma projektowała: wytłumienie w drzwiach przednich i tylnych, elementy paneli drzwi, elementy kokpitu samochodowego, wykładziny dywanowe kierowcy oraz pasażera. Firma zajmuje się usługami inżynierskimi, uczestnicząc na każdym etapie tworzenia produktu, począwszy od fazy konceptu poprzez badania, projektowanie i rozwój, a kończąc na wdrożeniu do

produkcji elementów samochodowych. Grupa badawcza składała się z 24 ankietowanych.

Drugim przedsiębiorstwem jest przedsiębiorstwo (PR2), które istnieje z pełnym powodzeniem na rynku pneumatycznym, gdyż działa od roku 1938. W przeciągu tak długiego okresu firma zdobyła zaufanie klientów, zarówno w Polsce jak i za granicą. Wykwalifikowana kadra zapewnia w pełni profesjonalny serwis sprzedawanych urządzeń dostępnych w każdym miejscu w kraju. Firma specjalizuje się w różnego rodzaju produktach pneumatycznych, począwszy od pistoletów lakierniczych, przez sprężarki śrubowe do autobusów i aut ciężarowych. W badaniu wzięło udział 14 respondentów.

Trzecie z przebadanych przedsiębiorstw (PR3), zajmuje się profesjonalnymi systemami łączności radiowej dla dużych i małych przedsiębiorstw, instytucji publicznych, agencji ochrony, firm transportowych oraz osób indywidualnych. Firma projektuje i wykonuje specjalistyczne urządzenia elektroniczne, zaawansowane systemy elektroniczne oraz diagnostyczne stosowane w technice motoryzacyjnej. Informatycy i programiści tworzą specjalistyczne oprogramowanie, które okazuje się być liderem na polskim rynku warsztatowym oraz firma odczytuje i kasuje kody usterek w samochodach jak i koduje parametry bieżące.
Firma w polskim oddziale zatrudnia 200 osób. W badaniu wzięło udział 16 ankietowanych.

Kolejno, czwartą badaną grupą (PR4), jest producent i dostawca wiodący na światowym rynku części zamiennych, oferujący rozwiązania naprawcze dla wszystkich popularnych typów pojazdów w sektorze samochodów i pojazdów użytkowych. Omawiana grupa łączy wysokie standardy, jakości z wyraźnym ukierunkowaniem na klienta.
Marki trzech międzynarodowych produktów, zakotwiczone w ramach jednej grupy oferują techniczne części. Ponadto, wymagania niezależnych warsztatów są szczególnie uwzględniane. Korzyść dla klientów i partnerów jest taka, iż otrzymują produkt z jednego źródła. Połączenie kompetencji i usług oznacza, że z jednego miejsca oferuje ponad 60 000 różnych części zamiennych do wszystkich popularnych modeli samochodów i pojazdów użytkowych.

Firma posiada 21 międzynarodowych filii i przedstawicieli w ponad 70 krajach, więc opisywana grupa jest jednym z wiodących graczy na niezależnym rynku części zamiennych.
Oprócz technicznych części zużywających się dla trzech marek motoryzacyjnych firma produkuje również komponenty dla różnych sektorów przemysłu
Polski oddział zatrudnia 50 osób, a w badaniu uczestniczyło 10 osób.

Działalność kolejnego piątego przedsiębiorstwa (PR5), obejmuje biznes Retail, sieć stacji i sklepów motoryzacyjnych, łącznie ok. 420 obiektów w całym kraju, oferujących pełną gamę usług od sprzedaży paliwa przez myjnie po pełną ofertę kart paliwowych. Firma oferuje paliwo dla flot samochodów osobowych i vanów oraz dla operatorów transportu ciężkiego – samochodów ciężarowych i autobusów oraz środki smarne. w Krakowie działa, jedno z największych centrów nowoczesnych usług dla biznesu w Polsce, stanowiące wsparcie dla grupy oddziału firmy zajmujące się finansami, logistyką, zakupami, procesami kadrowymi, obsługą klientów, jak również w komunikacją zewnętrzną oraz wewnętrzną. W badaniu wzięło udział 4 respondentów. W przypadku tego przedsiębiorstwa badanie za pomocą kwestionariusza ankiety zostało przeprowadzone w grupie osób ze ścisłego kierownictwa, natomiast kwestionariusz wywiadu i obserwacji został przeprowadzony wśród ogółu pracowników. Stąd też, wzięto pod uwagę taką nieliczną grupę 4 respondentów.

Następne szóste przedsiębiorstwo (PR6), to światowy lider w produkcji łożysk, przegubów homokinetycznych, techniki liniowej, rolek prowadzących, części zawieszenia oraz powiązanych usług i szkoleń.
Przedsiębiorstwo skupia się na innowacjach, niezależnie od gałęzi przemysłu m.in.: lotnictwo, motoryzacja, cementownie, energia wiatrowa, kolej, obrabiarki, włókiennictwo, rolnictwo, maszyny budowlane, kopalnie i kamieniołomy, pompy próżniowe, huty stali, itp.
Europejski oddział korporacji zajmującej 3 miejsce na świecie w produkcji łożysk, działa na rynkach w Europie, Ameryce Południowej, Afryce i na Bliskim Wschodzie.
Ma 26 zakładów produkcyjnych, w których produkuje 430 000 części dziennie. Próba badawcza wyniosła 11 respondentów.

Kolejna siódma przebadana organizacja (PR7), to globalny koncern technologiczny, który dostarcza rozwiązania dla samochodów osobowych, komercyjnych oraz dla przemysłu, wspierając w ten sposób rozwój mobilności nowej

generacji. Dzięki bogatej ofercie, koncern oferuje zintegrowane rozwiązania w obszarze mobilności producentom pojazdów, firmom przewozowym oraz start-up'om.
Firma zatrudnia 149 tysięcy pracowników w około 230 lokalizacjach w 40 krajach na świecie. W Polsce działalność jest prowadzona w 6 lokalizacjach tzn. w Bielsku-Białej, Czechowicach-Dziedzicach, Częstochowie, Gliwicach, Łodzi i Warszawie.
W Polsce znajdują się Zakłady Produkcyjne, Centra Inżynieryjne, Centra Usług Wspólnych takich jak IT, Finanse, Zakupy czy Rekrutacja oraz dział Aftermarket.
Zakład produkcyjny pasów bezpieczeństwa wytwarza pasy bezpieczeństwa oraz zamki zarówno do samochodów osobowych jak i dostawczych. Zakład produkuje różnorodne elementy niezbędne do tworzenia pasów bezpieczeństwa, służące utrzymaniu pasażera w odpowiednim miejscu podczas wypadku, ograniczając tym samym jego negatywne skutki dla zdrowia i życia.
Firma w Polsce posiada 5 oddziałów. Badania przeprowadzono wśród 35 respondentów.

Ósme przedsiębiorstwo (PR8), to światowy lider w rozwoju, projektowaniu i produkcji układów napędowych pojazdów. Przedsiębiorstwo zajmuje się:

- układami paliwowymi typu: - moduły dostarczania paliwa, pompy paliwowe, wtryskiwacze, GDi – PFI, pompy, wtryskiwacze, części naprawcze, SRA - SCR, filtracja
- rozwiązaniami konserwacyjnymi: hamowanie, układ kierowniczy i zawieszenie, klimatyzacja
- elektroniką pojazdu i zarządzanie silnikiem: sterowniki, zapłon, czujniki
- diagnostyką i wsparciem technicznym: narzędzia diagnostyczne, sprzęt do testowania oleju napędowego, sprzęt do testowania GDi, szkolenie

Asortyment obejmuje wiele nowości i patentów, między innymi: zaawansowane czujniki, sterowniki, falowniki, konwertery i ładowarki pokładowe oraz produkty do zapłonu. W oddziale polskim udział wzięło 26 respondentów.

Ostatnią dziewiątą organizacją (PR9), można skojarzyć z przełomowymi wynalazkami w technice samochodowej. Technologie i produkty takie jak świeca zapłonowa, rozrusznik, ABS, ESP czy też CommonRail nierozerwalnie wiążą się z omawianą firmą. Nowatorskie technologie wdrażane i rozwijane przez firmę stanowią znaczny wkład w rozwój i technologię produkcji samochodów. Firma oferuje produkty dedykowane dla każdego modelu samochodu, do których należą między innymi:

akumulatory, alternatory, czujniki, filtry, klocki hamulcowe, komponenty układów wtryskowych dla silników benzynowych i diesla, świece zapłonowe, tarcze hamulcowe, rozruszniki, wycieraczki i żarówki.
Omawiane produkty firmy dostarczane są do większości globalnych producentów samochodów, m. in. do BMW, Tesli, koncernu PSA, Hondy czy Toyoty. Wzrost produkcji i poszerzenie gamy produktów w ostatnim roku jest dowodem zaufania, jakim cieszy się zakład u długoletnich klientów. W polskim oddziale firmy w badaniu wzięło udział 18 respondentów.

Do próby badawczej wybrano te przedsiębiorstwa, które są liderami wśród dostawców na rynku motoryzacyjnym w Europie, zaznaczając swoją pozycję na rynku zbytu, jako potentata i wyróżniając się pod względem przetwarzania grupy informacji określonych, jako tajemnica przedsiębiorstwa. Jako dostawcy przemysłu motoryzacyjnego są często w posiadaniu informacji poufnych, dotyczących części stosowanych w nowych rozwiązaniach konstrukcyjnych, wykorzystywanych przez kontrahentów.

Omawiane przedsiębiorstwa są w posiadaniu listy aktywnych dostawców, listy odbiorców oraz umów z nimi zawartymi oraz informacji dotyczących prowadzonych aktualnie negocjacji cenowych. Do tej kategorii zalicza się też korespondencję handlową, złożone już oferty współpracy oraz otrzymane od potencjalnych partnerów handlowych zapytania ofertowe. Firmy są w posiadaniu informacji dotyczących rozpoznania na rynku handlowym potrzeb klientów w zakresie asortymentu, który już produkują lub też będą w krótkim czasie produkować. Istotne znaczenie mają również wynalazki patentowe, prototypy, plany i strategie sprzedaży oraz przyszłe plany rozwoju organizacji. W tym przypadku mówimy również o danych marketingowych, finansowych, sprzedażowych, danych uzyskanych z kontroli, jakości, danych produkcyjnych oraz wszystkich wewnętrznych danych firmowych łącznie z raportami i sprawozdaniami finansowymi.

Nie bez znaczenia jest fakt, że omawiane przedsiębiorstwa są w posiadaniu polityki rozwoju, przekazując swoje strategie i plany rozwoju, które stanowią tajemnicę przedsiębiorstwa i ujawnienie tych informacji byłoby równoznaczne z zagrożeniem wypracowanej stabilnej pozycji na rynku. Organizacje mają również dostęp do informacji jawnych tzn. polityki i wymogów, jakości. Wymienione przedsiębiorstwa są wpisane do Krajowego Rejestru Sądowego, produkując określony asortyment, który posiada swoją ofertę.

Nieodłączną grupą informacji, która stanowi tajemnicę przedsiębiorstwa są również dane dotyczące relacji koszt-cena, stosowane procedury (w tym procedury kontroli, jakości), know-how, kierunki i plany związane z rozwojem firmy (plany reklamowe i marketingowe oraz kwoty pieniężne przeznaczone na tą operację), wyniki uzyskanych badań (rozpoznanie rynku konkurencji) oraz statystyki czy informacje dotyczące wynagrodzeń pracowników.

Jednostki gospodarcze są w posiadaniu wiedzy know-how, która umożliwia efektywny i bardzo skuteczny sposób na utrzymanie wyjątkowej i prestiżowej pozycji na rynku światowym.

W kolejnym rozdziale pracy przyjęto wskazaną wyżej numerację zgodną z kolejnością prezentowanych przedsiębiorstw.

3.4. Metody, narzędzia i techniki badawcze

W wybranych przedsiębiorstwach badania przeprowadzono wśród osób zajmujących stanowiska kierownicze wyższego i niższego szabla oraz pracowników na stanowiskach nie kierowniczych, którzy wyrazili swoją opinię w kwestionariuszu ankiety. Pozwoliło to uzyskać opinię szerszego zakresu kadry pracowniczej od pracowników produkcyjnych do zarządzających. Na tej też podstawie określono, jakie najczęściej występują zagrożenia, z którymi borykają się przedsiębiorcy.

Ponadto, posłużono się metodami badawczymi takimi jak: analiza, synteza, funkcje myślenia, czyli indukcja i dedukcja, analiza dokumentów, interpretacja, definiowanie, selekcja, czy też sondaż diagnostyczny, które znajdują się w pracy.

W celu poszerzenia wiedzy i uzyskania rzetelnych wyników autorka pracy skorzystała z instrumentów, które poniżej zostaną szerzej omówione:

- Analiza dokumentów i literatury przedmiotu
- Ankieta
- Obserwacja
- Wywiad

Dzięki zastosowaniu kwestionariusza ankiety w możliwie krótkim okresie czasie uzyskano dostęp do szerszego grona respondentów. Ankieta kształtuje poczucie anonimowości, więc posłużono się nią, aby zgromadzać materiał badawczy o charakterze ilościowym.

Ankieta została podzielona na dwie części, w której we wprowadzeniu, poinformowano o celowości badań, ogólnym instruktażu udzielania poprawnych odpowiedzi, wskazując sposób poprawnego wyrażenia swojej opinii. Zapewniono również o anonimowości wypełnionych kwestionariuszy. Zasadnicza część kwestionariusza ankiety, która zamieszczona została w załączniku 1 opiera się na 38 pytaniach zamkniętych oraz półotwartych, dotyczących istniejącego stanu BI w jednostkach gospodarczych oraz znajomości przez personel możliwych do zaistnienia zagrożeń bezpieczeństwa informacji. Odpowiedzi pracowników pokazały ich faktyczny stan wiedzy i niewiedzy, wobec obowiązujących zasad przetwarzania, przechowywania, udostępniania informacji innym podmiotom. Ponadto, interesariusze wyrazili swą opinię, co do poczucia bezpieczeństwa poprzez zastosowanie w organizacjach odpowiednich mechanizmów ochronnych i korekcyjnych.

Kwestionariusz na końcu opatrzony został również czterema pytaniami z metryczki, w celu głębszej analizy badanych osób, odnośnie zajmowanego stanowiska, stażu pracy oraz uzyskanego wykształcenia respondentów.

W kolejnym etapie pracy badawczej posłużono się również narzędziem, jakim jest obserwacja naukowa, polegająca na celowym przyglądaniu się badanemu przedsiębiorstwie oraz zjawiskom tam zachodzącym. Autorka pracy użyła w badaniach technikę obserwacji postronnej tzn. nieuczestniczącej. Z kolei narzędziem badawczym, które wykorzystano do tego celu, był arkusz obserwacji zamieszczony w załączniku 2. Autorka pracy nie brała żadnego udziału w pracach i procesach badanego przedsiębiorstwa, ani też nie miała żadnego udziału organizacyjnego. Wyniki z analizy udostępnionych dokumentów i przeprowadzonej obserwacji oraz wywiadu zostały zaprezentowane w podrozdziale 4.2.

Ponadto ważną rolę w znalezieniu odpowiedzi na pytania problemowe odegrał wywiad. Posiada on szereg zalet. m.in.: skorzystano z możliwości zadawania szeregu dodatkowych pytań i obserwowania zachowania osoby odpowiadającej na nie.

W wywiadzie bezpośrednio stawiano pytania kierownikom, dyrektorom reprezentującym działy, którzy mają dostęp do strategicznych informacji dając tym samym możliwość uzyskania pełniejszej i wnikliwszej bardziej dogłębnej odpowiedzi niż w przypadku wywiadu pisemnego.

Posłużono się w tym celu techniką wywiadu nieskategoryzowanego, tzn. prowadzonego w sposób wolny, swobodny, luźny, a jednak ukierunkowany na problemie badawczym.

Pytania miały charakter otwarty, a zebrane arkusze wywiadu charakter jakościowy. W załączniku 3 znajduje się wzór tego dokumentu.

Ankieta i wywiad oraz obserwacja naukowa zostały wykorzystane zarówno we wstępnej fazie badań, jak i później. Omawiane metody umożliwiły autorce pracy opis badanych przedsiębiorstw, ustalenie faktów, motywacji pracowników oraz ich poziom świadomości w stosunku do przechowywanej informacji i oczekiwań dotyczących stosowanych zabezpieczeń w jednostce zatrudniającej.

Ustalenie powiązań między teorią, a metodami badawczymi uzyskanymi z przeprowadzonych badań ankietowych (metodą wykładni) oraz wyników z obserwacji, wywiadu, zostały zamieszczone w podrozdziale 4.3.

Reasumując, w wyniku przeprowadzenia analizy ryzyka zdiagnozowano istniejący stanu bezpieczeństwa i wykryto istotne luki w systemie BI. Uwieńczeniem praktycznego podejścia do tematu bezpieczeństwa informacji w organizacji okażą się konkluzje autorki.

3.5. Organizacja i przebieg badań

Po merytorycznym przygotowaniu założeń celu pracy oraz zweryfikowaniu trafności hipotezy oraz określeniu zakresu i obszaru badań, skoncentrowano uwagę na przeglądzie literaturowym, analizującym artykuły naukowe, akty prawne, rozporządzenia, normy z serii ISO oraz źródła internetowe oraz inne materiały dotyczące omawianej tematyki. W ten sposób rozpoznano problem badawczy, który rozwiązano dzięki użyciu empirycznych badań w oparciu o znane metody naukowe. Po zidentyfikowaniu celu pracy wykorzystano narzędzia badawcze typu: ankieta, obserwacja, wywiad do zdiagnozowania zagrożeń w grupach przedsiębiorstw. W fazie identyfikacji zagrożenia nie przyjęto wszystkich sposobów jego wyeliminowania. Opracowanie wyników posłużyło do przygotowania nowego katalogu zagrożeń na podstawie, którego przeprowadzono analizę ryzyka. Pozwoliło to na wyłonienie luk w systemie, które powinny być udoskonalone w systemie usprawniającym BI w warunkach przedsiębiorstw.

W części teoretycznej pracy, użyto metody teoretycznej i praktycznej wykorzystując narzędzia badawcze tj. kwestionariusz ankiety, obserwacji oraz wywiadu, ponadto zaplanowano analizę dokumentacji i analizę statystyczną.

Przedstawiono aktualne stanowisko przedsiębiorstw wobec istniejącego stanu poziomu bezpieczeństwa informacji oraz stosowanych zabezpieczeń. Konkluzją badań

było zestawienie danych, opracowanie ich i dokonanie analizy ryzyka oraz stworzenie pomysłu na zmiany w obszarze badanych zagadnień wraz z projektem zmniejszającym możliwość utraty informacji w organizacji (rozdział 6). Projekt służy nie tylko ocenie stanu rzeczywistego, jednak przedstawia też, co należy ulepszyć w działaniu przyszłościowym tak by lepiej, skuteczniej i efektywniej zarządzać organizacją.

Po przygotowaniu kwestionariusza ankiety, obserwacji i wywiadu, przeprowadzono badania, zgodnie z procedurami tzn. przygotowano grupę badawczą do badań, sprecyzowano czas i miejsce, zapoznano pracowników z problematyką i sposobem przeprowadzenia badań. Ponadto zwrócono uwagę na zapis we wstępie, iż kwestionariusz ankiety jest anonimowy. Rozdano pracownikom zarządu oraz pracownikom administracyjno- biurowym przetwarzającym informacje, kwestionariusze ankiety. Wcześniejsze objaśnienia pomogły w szybkim i sprawnym zebraniu kwestionariuszy ankiety. Zebrane wyniki badań poddano analizie.

Po zakończeniu etapu związanego z ankietowaniem przystąpiono do 2 części badań, czyli do obserwacji nieuczestniczącej, w której to zanotowano spostrzeżenia do16 pytań z kwestionariusza obserwacji. Wyniki zostały uzupełnione trzecią częścią procesu badań, tzn. wywiadem z prezesem danego przedsiębiorstwa motoryzacyjnego. Podczas takiego wywiadu zadano 28 pytań, na które uzyskano odpowiedzi. Otrzymane informacje wywiadowcze przekazane przez uprawnioną osobą zostały wpisane w kwestionariuszu wywiadu i arkuszu obserwacji celem syntezy.

Kolejnym krokiem było przeprowadzenie doświadczenia w postaci badania eksperymentalnego, mającego na celu sprawdzenie rzeczywistego stanu istniejącego w przedsiębiorstwach. W wyniku badania praktycznie zweryfikowano postępowanie pracowników w organizacjach w związku z zaistniałymi potencjalnymi sytuacjami zagrażającymi.

Po zdefiniowaniu celu i zakresu pracy oraz przeprowadzeniu badań za pomocą metod naukowych ankietowania, obserwacji oraz wywiadu zdiagnozowano zagrożenia w grupach przedsiębiorstw. Opracowane wyniki i wyselekcjonowane najbardziej realne zagrożenia BI, pozwoliły na utworzenie nowego katalogu zagrożeń, występujących w obszarze funkcjonowania omawianych przedsiębiorstw. Na podstawie tego katalogu przyjęto dalsze działania niezbędne w celu prowadzenia analizy ryzyka w trakcie, której wyłoniły się luki w systemie, które powinny być usprawnione.

Po otrzymaniu usystematyzowanych wyników, zdiagnozowano istniejący stan zagrożeń, który wskazał, co powinno być spełnione, aby zachować odpowiedni poziom zabezpieczeń informacji w organizacjach uwzględniając w tym obowiązujące normy, akty prawne, dyrektywy, decyzje, zalecenia oraz rozporządzenia. Przeprowadzenie analizy ryzyka pozwoliło na określenie tych najsłabszych elementów, które stwarzają największe zagrożenie dla organizacji.

Ostatnia część prac, wskazuje na wdrożenie systemu zabezpieczeń, który ma realny wpływ na zabezpieczenia, zwiększając tym bezpieczeństwo i redukcję ryzyka utraty informacji. W tym też celu zainicjowano koncepcję projektu systemu zarządzania bezpieczeństwem informacji, który usprawni pracę organizacji i określi, co należy udoskonalić w działaniu organizacji tak by skuteczniej zarządzać informacją.

4. WYNIKI BADAŃ WŁASNYCH

4.1. Analiza i wnioski z badań ankietowych

Analiza danych empirycznych przeprowadzona na podstawie wyników badań ujawniła szereg problemów, związanych z brakiem zapewnienia atrybutów bezpieczeństwa informacji, z którymi zmagają się badane organizacje. W celu znalezienia rozwiązania problemu badawczego i udowodnienia hipotezy przeprowadzono badania oraz dokonano analizy poziomu bezpieczeństwa informacji w dziewięciu przedsiębiorstw a szerzej opisanych w rozdziale 3.

Badania przeprowadzono w działach: księgowo-finansowym, płacowo-kadrowym, kontrolingu, sprzedaży, technologicznym, marketingu, IT, badawczo-rozwojowym oraz w dziale BHP. Przeprowadzono badania wśród pracowników zatrudnionych w działach, które są w posiadaniu aktywów informacyjnych, do których zaliczamy wszelkiego rodzaju zbiory danych i środki do ich gromadzenia, przetwarzania i transmisji. Do zasobów tych należą: projekty technologii prototypów, prototypy, oprogramowanie, sprzęt komputerowy i sieciowy, bazy danych, dokumentacje systemowe, procedury i umowy, raporty sprzedażowe, wyniki z przeprowadzonych audytów wewnętrznych i zewnętrznych oraz doświadczenie i wykorzystywane umiejętności pracującej załogi.

Zgadnie z celem pracy, aby należycie ocenić ryzyko wystąpienia zagrożeń najpierw posłużono się badaniem ankietowania. Pracownikom przedsiębiorstw zadano pytania dotyczące rodzaju zagrożeń i prawdopodobieństwa ich wystąpienia, sugerowanych przyczyn zagrożeń, oceny poziomu bezpieczeństwa informacji w organizacjach gospodarczych, jak również wykorzystywanych sposobów zapobiegania dalszemu powstawaniu ryzyka.

Głównym celem przeprowadzenia badań ankietowych było wskazanie, które zagrożenia są powszechnie zauważalne, a które mniej znane i rzadziej występujące. Taka analiza pozwoliła na stworzenie rzeczywistego katalogu zagrożeń wstępujących w organizacjach. W badaniu poświęcono uwagę na pytania, które dotyczą obszarów, powodujących pojawienie się podatności na zagrożenia. Z tego też względu odpowiedzi respondentów, które wskazywały na prawidłowe postępowanie w zakresie bezpiecznego przechowywania informacji dalej nie analizowano. Natomiast gruntownej

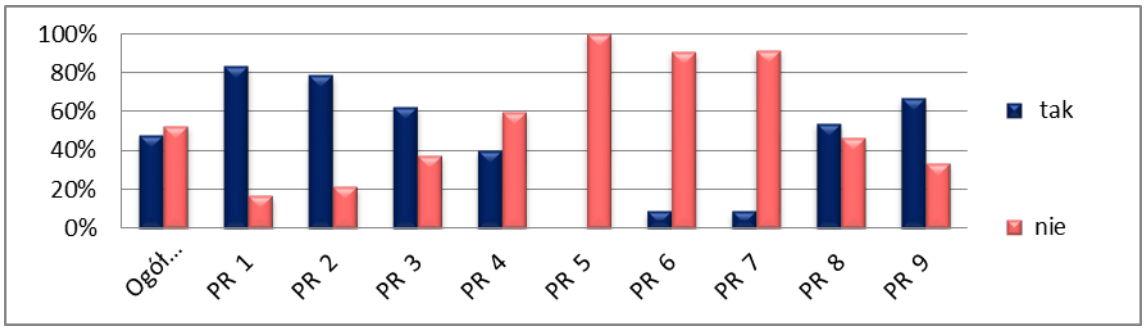
analizie poddano te pytania, z których wyraźnie widać możliwość pojawienia się podatności dla zagrożeń utraty BI. Stąd też wyselekcjonowano grupę pytań. Badano pracowników w organizacji wraz ze wskazaniem ich wykształcenia oraz stopnia zajmowanego stanowiska w pracy.

Cel ankiety został przedstawiony w rozdziale 3, natomiast rozdział 4 będzie zawierał przeprowadzoną analizę otrzymanych odpowiedzi na zadane pytania, pokazując tym samym czy rozpoznane zagrożenia występują w większości organizacji, czy tylko w niektórych spośród przebadanych. Przeprowadzone badania pozwolą na uogólnienie otrzymanych wyników w testowanym sektorze motoryzacyjnym.

Poniżej przedstawiono udział procentowy określonych odpowiedzi na wybrane pytania przebadanych grup respondentów, które są kluczowe w tematyce sprawdzenia poziomu bezpieczeństwa informacji w badanych organizacjach. Przedsiębiorstwa zostały oznaczone symbolem PR 1 do PR 9.

Badane przedsiębiorstwa zostały oznaczone na rysunkach symbolem PR1do PR 9.

Podstawowym elementem regulującym bezpieczeństwo informacji powinno być wdrożenie standardu ISO 27001. w związku z tym w pytaniu 1. Z kwestionariusza ankiety dokonano analizy stanu wdrożenia normy w badanych organizacjach *(Czy w Państwa firmie jest wdrożona norma ISO 27001 (dotycząca bezpieczeństwa informacji)?*



Rysunek 30. Wdrożenie normy ISO 27001 w poszczególnych przedsiębiorstwach wg. opinii przebadanych

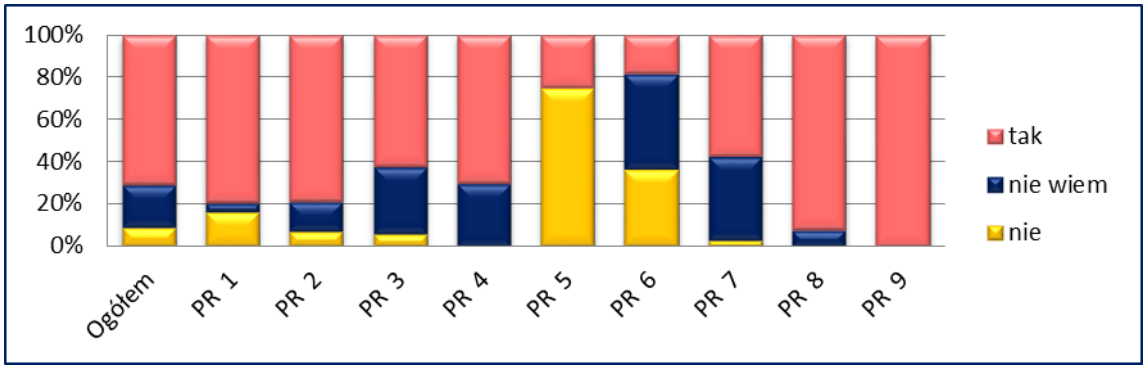
Źródło: Opracowanie własne na podstawie badań ankietowych

Z danych przedstawionych na rysunku 30 można stwierdzić, iż są trzy przedsiębiorstwa (PR5, PR6, PR7), w których pracownicy prawie w 100% nie posiadają jeszcze wiedzy na temat wdrożenia normy ISO 27001. Taki stan wiedzy pozwala na stwierdzenie, że w organizacjach nie został wdrożony standard bądź też pracownicy nie mają świadomości, zaimplementowania i obowiązywania w ich organizacjach takiej

normy. Taka sytuacja może narazić przedsiębiorstwo na nieświadome narażenie danych przechowywanych w przedsiębiorstwie, a w efekcie na ich wyciek, udostępnienie czy modyfikację.

Patrząc na ogół udzielonych odpowiedzi stan ten zdecydowanie nie, jest zadawalający skoro 50% przebadanych twierdzi, że w organizacjach nie ma wdrożonej normy ISO 27001. Świadczy to o braku szkoleń, na których to pracownicy dowiadują się o zamiarach i planach przygotowania organizacji do wprowadzenia zasad z nowych norm, rozporządzeń i posiadają wiedzę dotyczącą czy są już wdrożone czy też nie.

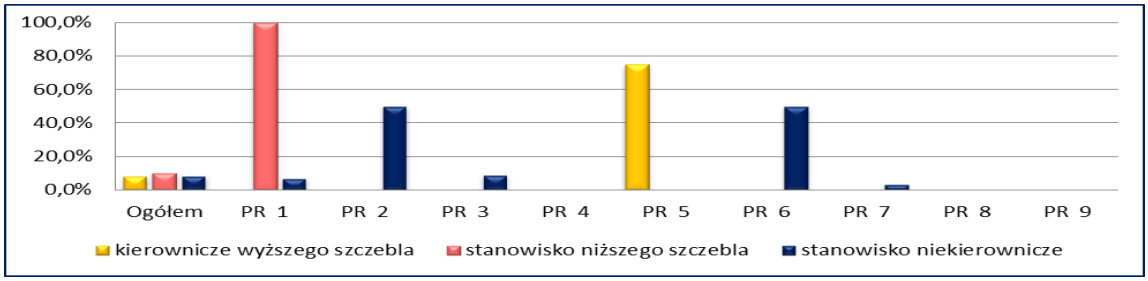
Innym aktem prawnym obowiązującym wewnątrz organizacji jest PBI. Zawiera ona definicje bezpieczeństwa informacji, cele wynikające z jej wdrożenia, procedury podczas szkoleń pracowników i ich postępowania podczas pojawienia się zagrożenia lub też konsekwencje wynikające z niezastosowania się do obowiązujących zaleceń. Pytanie 2 kwestionariusza ankiety porusza ten temat *Czy w Państwa firmie została opracowana i wdrożona Polityka Bezpieczeństwa Informacji?*



Rysunek 31. Wdrożenie normy ISO 27001 w poszczególnych przedsiębiorstwach wg. opinii przebadanych uwzględniające wszystkie możliwe odpowiedzi
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

Z danych empirycznych można stwierdzić, że większość respondentów (70,9%) posiada wiedzę na temat wdrożenia PBI, natomiast 9% nie jest świadomych czy polityka jest w wdrożona, a 20% wyraziła zdanie, że nic o tym nie wie. Zatem można stwierdzić, iż mimo przewagi odpowiedzi twierdzących pozostają jednak osoby, które są nieświadomie i w wyniku tego mogą narażać dane firmowe na ich utratę. Wzorowym przedsiębiorstwem w tym wypadku okazało się PR 8 oraz PR 9, gdzie uzyskano niemal 100% zgodność, co do wdrożenia PBI.

Rysunek 32 przedstawia dane wskazujące na odpowiedzi „nie" dla wszystkich 9 organizacji z podziałem na stanowisko pracy.



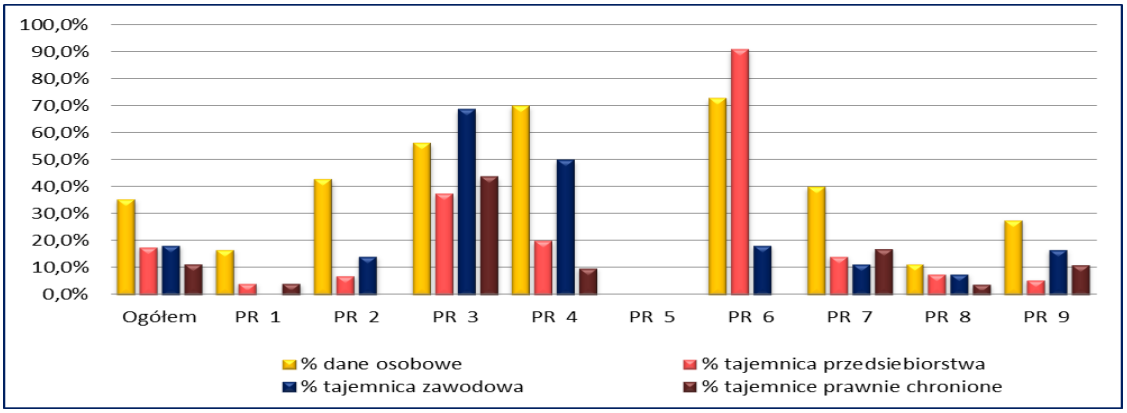
Rysunek 32. Wskazanie odpowiedzi negatywnej o wdrożeniu PBI wg. zajmowanego stanowiska w organizacji

Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

Analizując dane można stwierdzić, że osoby, które nie wiedzą czy w organizacji jest zaimplementowana PBI zajmują w większości stanowiska kierownicze niższego szczebla. Wskazuje to na brak świadomości tych pracowników w zakresie wdrażania reguł i zasad wynikających z wprowadzenia PBI.

Kolejno interpretując dane, 5-te przedsiębiorstwo przoduje w niewiedzy pracowników na stanowiskach kierowniczych o wdrożeniu PBI. Świadczy to o złej sytuacji w tej organizacji. Skoro zarząd nie wie, czy obowiązują zasady PBI w organizacji to, w jaki sposób prowadzić szkolenia o prawidłowym postępowaniu z informacją.

Z punktu widzenia bezpieczeństwa informacji bardzo ważnym jest, jakiego rodzaju informacje przetwarza się w organizacjach. Znając wartość i rodzaj informacji łatwiej dokonać klasyfikacji informacji. Zatem, wiadomo jak postępować z określonym rodzajem informacji, jak ją zabezpieczyć, przetwarzać lub zniszczyć. Ważnym jest też, kiedy i kto uzyskał dostęp do określonego jej rodzaju, w jakim celu ją przeglądał lub też czy miał do tego upoważnienie. W związku z powyższym w ankiecie zadano pytanie, 9: Do jakiego *rodzaju informacji ma Pani/Pan dostęp?*

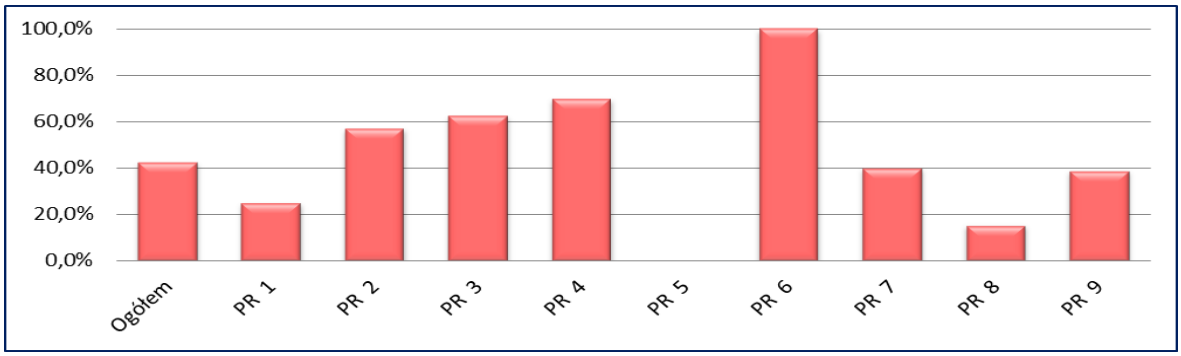


Rysunek 33. Dostęp do grup informacji kierowników niższego szczebla oraz pracowników na stanowiskach niekierowniczych

Źródło: Opracowanie własne na podstawie badań ankietowych

Analiza danych pozwala stwierdzić, że w obecnej sytuacji przedsiębiorstwa przetwarzają różnego rodzaju informacje począwszy od wewnętrznych, jawnych (ujęte w ankiecie natomiast nieujęte na rysunku) po dane osobowe (35,4%) oraz tajemnice przedsiębiorstwa (17,7%), zawodową (18,4%) oraz prawnie chronioną (11,4%).
W wyniku przetwarzania tak dużej liczby informacji, zupełnie realne staje się ujawnienie jej lub narażenie na incydent, bez względu na jej kategorię. Może do tego dojść w wyniku błędu, pomyłki, czy nieznajomości aktów prawnych przez osobę przetwarzającą dane. Należy, więc dołożyć wszelkich starań, aby wszystkie grupy informacji odpowiednio chronić ograniczając tym samym dostęp osób nieuprawnionych do takich wiadomości. Ograniczenie to związane jest m.in.: z tajemnicą przedsiębiorstwa, zawodową i prawnie chronioną.

W celu uszczegółowienia rysunek 34 prezentuje jak na pytanie 9 odpowiedziała grupa pracowników niepełniąca funkcji zarządczych w organizacji (kierowników niższego szczebla oraz pracowników na stanowiskach niekierowniczych), która również może być upoważniona do dostępu i przetwarzania tego rodzaju informacji.



Rysunek 34. Dostęp do grup informacji kierowników niższego szczebla
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

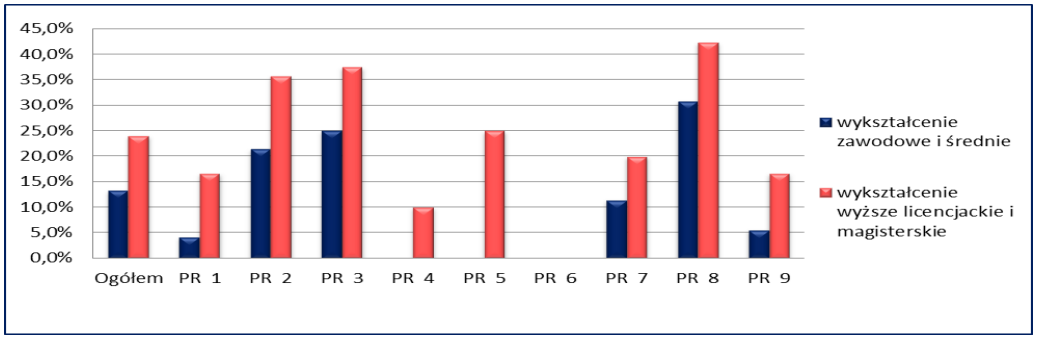
Z analizy danych zamieszczonych na rysunku 34 wynika, iż odpowiedzi są bardzo zróżnicowane, jednak ogółem 42,4% ankietowanych deklaruje dostęp do informacji. Dane osobowe, tajemnica przedsiębiorstwa jak i zawodowa oraz informacje prawnie chronione zarezerwowane powinny być tylko dla wybranych grup uprawnionych użytkowników do przetwarzania tego typu informacji uwzględniając przy tym określony sposób postępowania z takimi danymi (stosując specjalne zabezpieczenia w celu ich ochrony). W PR 6 istnieje duża grupa personelu kierowniczego niższego szczebla oraz niekierowników, (blisko 100%), która posiada dostęp do informacji typu tajemnica przedsiębiorstwa. Stanowi to dodatkowe źródło zagrożenia ujawnienia informacji, które ze względu na swoją wartość powinno być

chronione przed nieuprawnionym dostępem. W pozostałych organizacjach również część pracowników wskazuje, że posiada dostęp do tego rodzaju informacji.

Otrzymane wyniki wskazują na możliwość zaistnienia poważnego problemu dotyczącego wycieku informacji. Należy jednak przeanalizować czy otrzymane wyniki w pełni odzwierciedlają stan rzeczywisty w organizacjach oraz czy wszyscy ankietowani udzielili szczerych odpowiedzi.

Istotnym elementem dokumentu PBI, zawierającym zalecenia i zadania zabezpieczenia organizacji jest wprowadzenie zapisów w zawieranych umowach o zachowaniu poufności. Strony zlecenia powinny zdawać sobie sprawę ze swojej odpowiedzialności dotyczącej przechowywania poufnych informacji. Stąd też istotnym wydaje się zbadanie tego stanu rzeczy w umowach w 9-ciu organizacjach. Pytanie 11 dotyczy zapytania *czy w realizowanych projektach, umowach z kontrahentami istnieją zapisy dotyczące zachowania poufności informacji?*

Tylko w pełni świadoma konsekwencji kadra pracownicza, będzie umiała należycie przygotowywać umowy, chroniąc przy tym tajemnicę przedsiębiorstwa i zawodową oraz prawnie chronioną. Dlatego szczególnie zwrócono uwagę na odpowiedzi *„nie”* oraz *„nie wiem”* wraz ze wskazaniem na posiadane wykształcenie badanych.

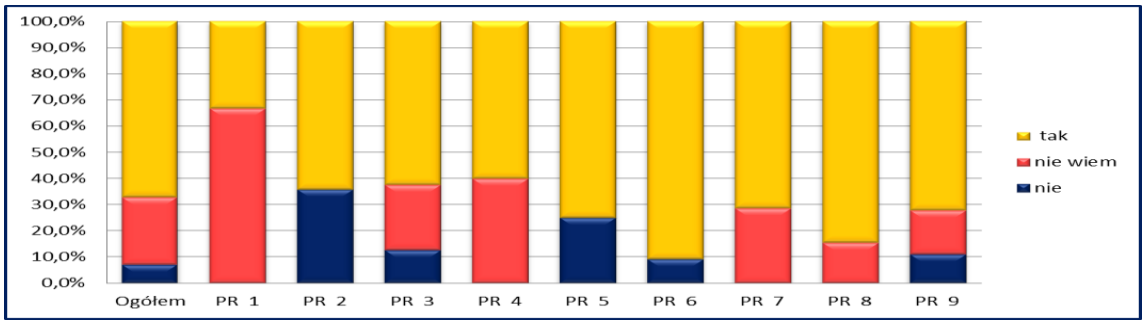


Rysunek 35. Wskazanie odpowiedzi *"nie", " nie wiem"* wg. uzyskanego wykształcenia
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

Analizując dane przedstawione na rysunku 35 można stwierdzić, że dla zdecydowanej większości pracowników znany jest zapis o poufności w umowach, czy kontraktach (w sumie 62,7% po zagregowaniu odpowiedzi wg. grupy pod względem wykształcenia, średnie-zawodowe oraz wyższe licencjackie oraz magisterskie odpowiedziało *„tak”*). Niepokojące jest jednak to, iż 37,3% przebadanych nic o tym *„nie wie”* (33,5%) lub też po prostu wybrali odpowiedz *„nie”(3,8%).* Osoby z wykształceniem zawodowym oraz średnim być może nie zdają sobie sprawy, z czym

związany jest brak tak ważnych zapisów, i jakie straty może ponieść przedsiębiorstwo niestosujące się do tego. Warto zaznaczyć, że wskazanie odpowiedzi *„nie wiem”* jest odpowiedzią negatywną a kontrakty zawarte przez te osoby są najprawdopodobniej nie poprawnie skonstruowane. Dotyczy to również osób posiadających wyższe wykształcenie we wszystkich przedsiębiorstwach oprócz PR 6.

Również pracodawca zobowiązany jest chronić posiadane aktywa poprzez zastosowanie klauzuli o zachowaniu poufności z pracownikami. Odpowiedź na to pytanie daje obraz na ile jest to praktykowane w przedsiębiorstwach. W związku z tym pytanie 13 dotyczy podpisywania oświadczenia o zachowaniu poufności informacji.

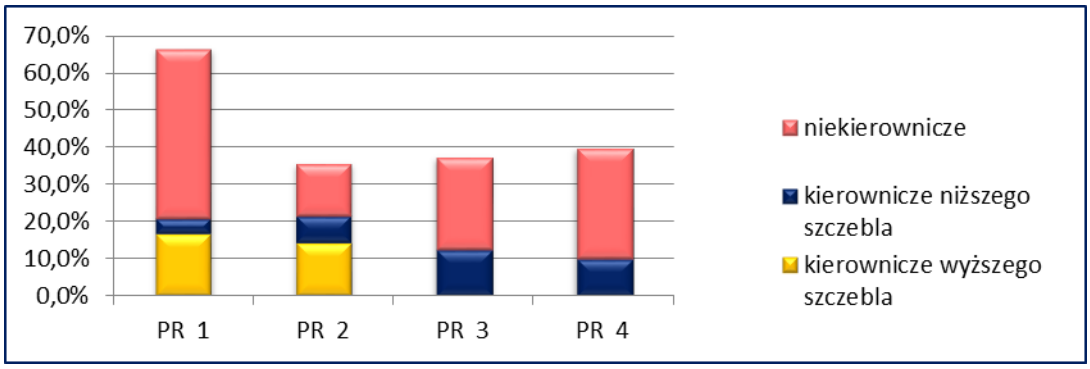


Rysunek 36. Podpisywanie oświadczenia o zachowaniu poufności informacji
Źródło: Opracowanie własne na podstawie badań ankietowych

W przeważającej większości we wszystkich przedsiębiorstwach można zauważyć stosowanie się do procedury podpisywania oświadczeń o zachowaniu poufności informacji.

Analiza danych empirycznych utwierdza w przekonaniu, że w sumie 67,1% przebadanych w organizacjach podpisała takie oświadczenie.

Jednak nie wszystkie przedsiębiorstwa w pełni stosują omawianą procedurę. Na szczególną uwagę zasługuje PR1, PR 2, PR 3, PR 4, PR 5 i PR 9, gdzie można znaleźć grupy osób, które nie podpisywały takiego oświadczenia lub po prostu wymijająco udzieliły odpowiedzi „*nie wiem”*. Jednak szerzej przeanalizowano dokładnie tylko niektóre z tych przedsiębiorstw, oznaczone PR 1, PR 2, PR 3, PR 4 sprawdzając, jaka grupa pracowników brała udział w takich odpowiedziach (do badań przyjęto próg odpowiedzi *„nie wiem”* i *„nie”* powyżej 30%).

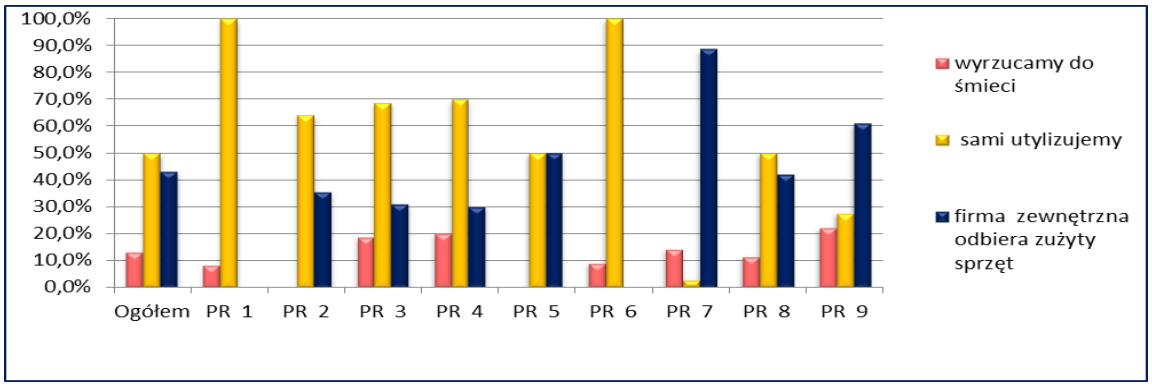


Rysunek 37. Wybór odpowiedzi „nie" lub "nie wiem" w zależności od zajmowanego stanowiska
Źródło: Opracowanie własne na podstawie badań ankietowych

Do grupy osób, które nie podpisały jeszcze oświadczenia o zachowaniu poufności zaliczamy pracowników na stanowiskach niekierowniczych (PR 1 - 45,8%, w PR 2 -14,3%, PR 3-25%, PR4 -30%), kierowniczych niższego szczebla (PR1 -4,2%, PR 2 -7,1%, PR 3- 12,5% PR 4 -10% (oraz kierowniczych wyższego szczebla PR1 - 16,7%, PR 2-14,3%) Jest to niepokojące, gdyż kierownicy na stanowiskach zarządczych decydujących o strukturze, organizacji i jej przyszłości zazwyczaj mają dostęp do informacji, które nie powinny nigdy zostać ujawnione innym podmiotom. W tym też celu podpisuje się klauzulę o zachowaniu poufności.

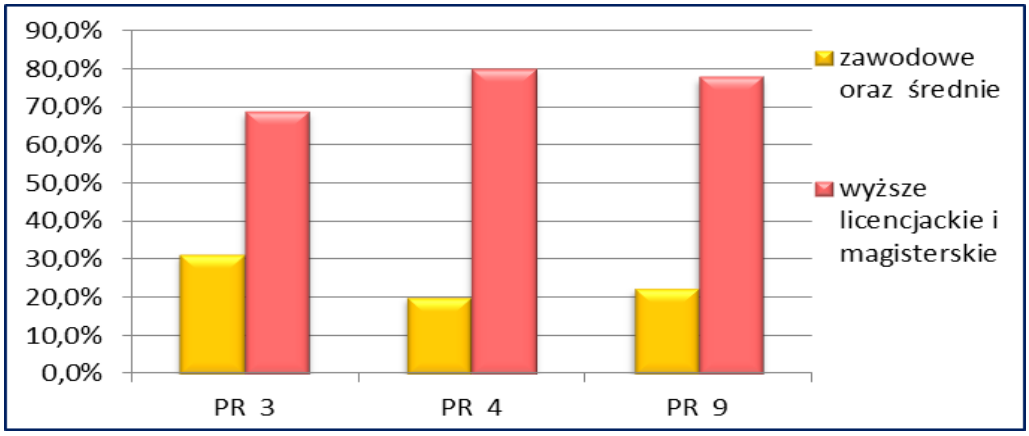
W organizacji wszyscy pracownicy powinni być świadomi powagi przetwarzanych danych począwszy od pracowników administracyjno – biurowych aż po kadrę zarządzającą.

Stosowane w przedsiębiorstwach nośniki informacji, mimo że nie są używane to jednak nadal posiadają informacje tam zawarte. Z punktu widzenia BI nadal ważnym jest, więc dbałość o właściwy sposób likwidacji tych nośników, gdyż nieodpowiedni sposób może przyczynić się do powstania zagrożeń. Stąd też pojawia się pytanie, w jaki sposób odbywa się utylizacja takiego sprzętu. W kwestionariuszu ankiety zadano pytanie 15 *Jak w Państwa firmie odbywa się utylizacja sprzętu używanego w przedsiębiorstwie np.: nośników danych?* Spośród odpowiedzi kluczowym jest wskazanie odpowiedzi „wyrzucamy do śmieci", „sami utylizujemy" lub „firma zewnętrzna odbiera zużyty sprzęt".



Rysunek 38. Sposób utylizacji sprzętu komputerowego w organizacjach
Źródło: Opracowanie własne na podstawie badań ankietowych

Ogół respondentów stwierdziło, że sami utylizują zużyty sprzęt, wewnątrz organizacji. Należy jednak wziąć pod uwagę, że w większości organizacji znajdują się osoby, które pozwalają sobie na wyrzucanie nośników danych do śmieci. Zanim jednak taki nośnik pamięci zostanie wyrzucony, warto się zastanowić czy kadra pracownicza jest absolutnie pewna, że informacje tam zawarte zostały całkowicie usunięte. Jest to bardzo niebezpieczne zjawisko, gdyż nośnik dostając się w niepowołane ręce przy użyciu różnych metod i technik może zostać ponownie użyty odzyskując zawarte tam dane. Tylko 43% ogólnie korzysta z usług firmy zewnętrznej do utylizowania urządzeń. Analiza wymaga, aby sprawdzić, w której grupie wykształcenia jest najwięcej odpowiedzi „wrzucamy do śmieci".

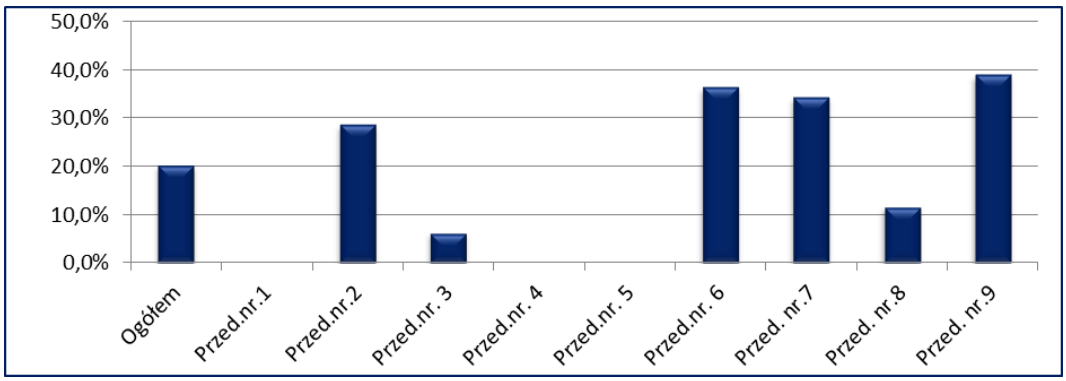


Rysunek 39. Organizacje wyrzucające do śmieci np.: nośniki danych wg. zajmowanej grupy stanowisk
Źródło: Opracowanie własne na podstawie badań ankietowych

Spośród 9 organizacji wybrano te, które odróżniały się od reszty, mianowicie PR 3, PR 4, PR 9. w toku dalszych badań przeanalizowano bardziej szczegółowo omawiane trzy organizacje, które potwierdziły fakt wyrzucania do śmieci sprzętu typu

nośniki danych. Dodatkowo sprawdzono grupę osób, która udzieliła takiej odpowiedzi. Okazało się, że w większości, czyli (22,5%) takie zdanie wyraziły osoby z wykształceniem zawodowym oraz średnim. Nasuwa się sugestia, iż te osoby są nie właściwie wyedukowane, o postępowaniu zagrażającym rozwojowi i bezpieczeństwu firmy. Personelowi nie został wskazany właściwy i odpowiednio bezpieczny sposób utylizacji sprzętu firmowego. Niepokoi również fakt, ponad 70% badanych w tych trzech organizacjach, z wykształceniem wyższym licencjackim oraz wyższym inżynierskim magisterskim lekceważą zasady bezpieczeństwa podczas utylizacji nośników danych, co zwiększa możliwość ujawnienia informacji na zewnątrz organizacji.

Niewątpliwie istotnym elementem z punktu widzenia systemu ochrony informacji jest zabezpieczenie sieci komputerowych poprzez korzystanie z loginów czy haseł. Niebezpieczne w skutkach jest udostępnienie takiego uwierzytelnienia innej osobie lub nieupoważnionej do tego rodzaju systemu. W pytaniu 16 zawarto podobną treść *Czy dopuszczalne jest wg. Pani/Pana udostępnienie swojego służbowego loginu i hasła innemu współpracownikowi lub stażyście?*

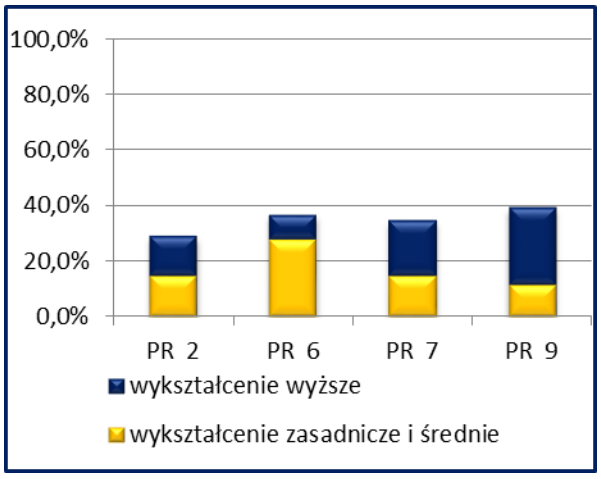


Rysunek 40. Wskazanie odpowiedzi pozytywnej udostępnienia swojego służbowego loginu lub hasła innemu współpracownikowi lub stażyście
Źródło: Opracowanie własne na podstawie badań ankietowych

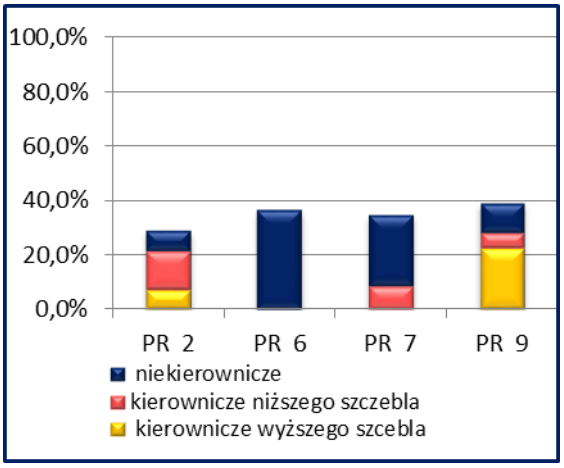
Rysunek 40 prezentuje niepokojącą opinię wydaną przez (20%) badanych, dla których dopuszczalne jest udostępnienie swojego loginu lub hasła koledze, czy koleżance z pracy.

Wprowadzając hasła i loginy weryfikujemy tożsamość użytkownika systemu, dzięki temu wiemy, kto pracował w danym systemie i kto mógł ewentualnie dokonać modyfikacji. Jest, więc to czynność niedopuszczalna i organizacje nie mogą bagatelizować tego problemu. Kolejne wykresy ujawniają podział grup pracowniczych,

które tak odpowiedziały z uwzględnieniem stażu pracy oraz posiadanego wykształcenia. Warto szerzej przeanalizować ten stan.



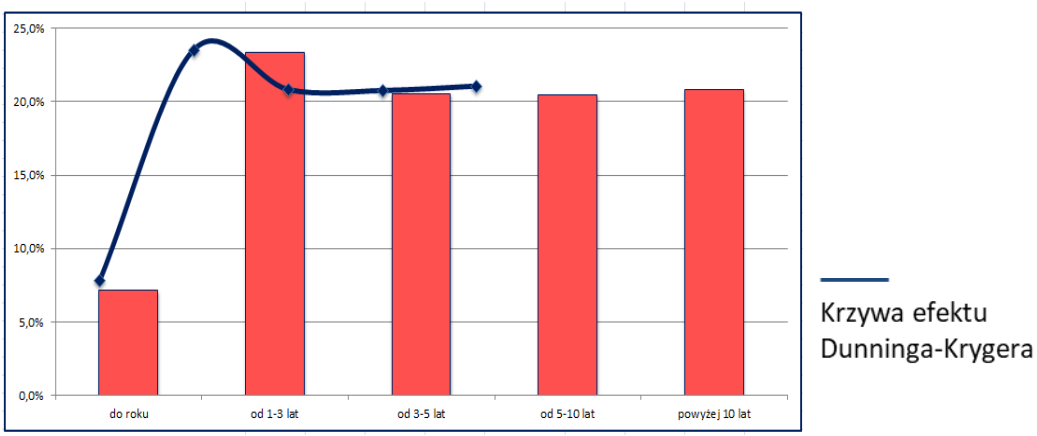
Rysunek 41. Dopuszczenie do udostepnienia loginu wg. uzyskanego wykształcenia
Źródło: Opracowanie własne



Rysunek 42. Dopuszczenie do udostepnienia loginu wg. zajmowanych stanowisk pracowniczych
Źródło: Opracowanie własne

Wyraźnie od ogólnego trendu organizacji odróżniają się PR 2, PR 6,PR 7,PR 9. Dla tych też organizacji przygotowano analizę udzielonych odpowiedzi pod kątem stażu pracy oraz wykształcenia. Rysunek 42 wskazuje, że w PR 2 pozytywnie wypowiadających się było 7,1% niekierowników, 14,3% kierowników niższego szczebla oraz 7,1% kierowników wyższego szczebla. W PR 6 do takiej sytuacji dopuściłaby tylko grupa niekierownicza w liczbie 36,4% respondentów. W PR 7 postąpiłaby tak grupa pracowników na stanowiskach: niekierowniczych 25,7 % natomiast kierowniczych niższego szczebla 8,6% badanych. Natomiast w PR 9 tylko 11,1% niekierowników udzieliło twierdzącej odpowiedzi oraz 22,2% kierowników wyższego szczebla i 5,6% kierowników niższego szczebla. Istotnym jest to, że osoby zajmujące stanowiska kierownicze wyższego szczebla dopuściliby do takiej sytuacji. Podsumowując w dziewięciu organizacjach takich kierowników wyższego szczebla było 4,4%. Natomiast nie ma znaczenia wpływ uzyskanego wykształcenia, gdyż z rysunku 41 z lekką przewagą na wykształcenie wyższe praktykują takie zachowania pracownicy posiadający wykształcenie średnie oraz zawodowe. Należy jasno powiedzieć, że obecna sytuacja jest istotnie zagrażająca bezpieczeństwu organizacji, skoro są w niej osoby, które nie zdają sobie sprawy z zagrożenia, jakim jest ujawnienie swojego hasła czy loginu mimo piastowanego przez nich tak wysokiego stanowiska. Analiza udzielonych odpowiedzi na to pytanie wskazuje na istnienie dużego problemu

z danymi do autoryzacji systemu, loginem i hasłem. W związku powyższym dokonano analizy, struktury pracowników pod względem stażu pracy, którzy wskazali, że dopuszczają do ujawnienia swoich danych autoryzacyjnych innym osobom.



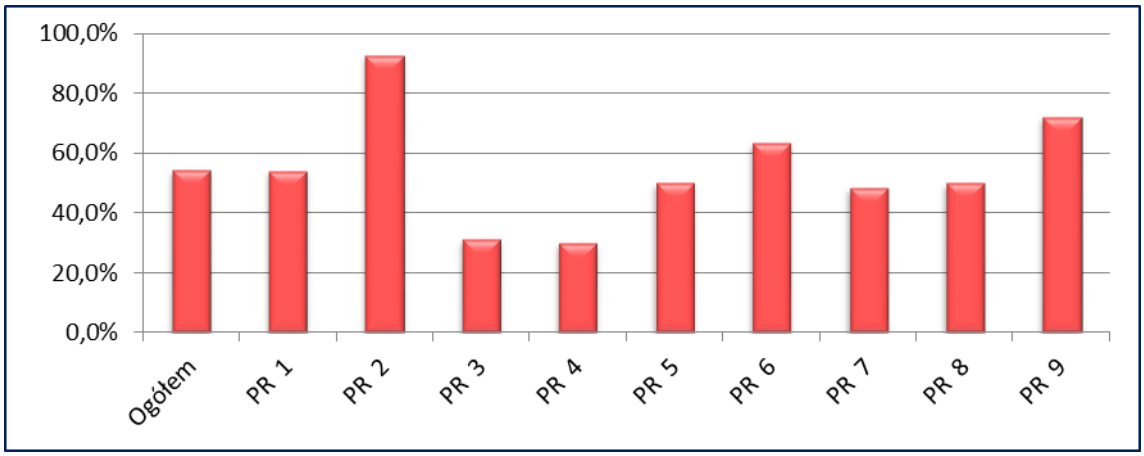
Rysunek 43. Dopuszczenie do udostepnienia swojego loginu lub hasła innym osobom
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

Analizując szersze spektrum dotychczasowej sytuacji warto jeszcze przyjrzeć się długości czasu pracy poszczególnych grup pracowniczych. Rysunek 43 obrazuje bieżącą sytuację, gdzie okazuje się, że im dłuższy staż pracy, tym pracownicy bardziej są skłonni podzielić się wiadomością o swoim służbowym loginie bądź haśle z innymi. Najprawdopodobniej załoga z dłuższym stażem opiera się na zaufaniu do współpracowników. Natomiast nowo przyjęte osoby wiedzą, że login i hasło należy chronić z zasady. Poza tym rozpoczynając pracę w nowej organizacji ludzie boją się i są w swoich zachowaniach ostrożni, jednak z czasem przeceniają swoje możliwości. Nabierają pewności siebie na zajmowanych stanowiskach i zaczynają lekceważyć dotychczas przestrzegane zasady. Nie bez znaczenia jest fakt, że starsze osoby obawiają się technologii informatycznych i być może proszą innych pracowników o pomoc. Rośnie, więc tendencja do zaufania innym pracownikom oraz w wyniku tego udostępnienia im swojego hasła i loginu.

Rysunek 43 obrazuje zjawisko psychologiczne zaprezentowane na krzywej efektu Dunninga- Krygera, gdzie zauważalne jest przecenienie swoich możliwości poprzez niewykfalifikowaną kadrę, podczas gdy osoby wykfalifikowane nie doceniają swoich umiejętności.

Wykrywanie zagrożeń oraz reagowanie na incydenty ma decydujące znaczenie dla ochrony danych. Dlatego też przeprowadza się identyfikację nowo pojawiających się zagrożeń oraz analizuje się na nowo powstałe ryzyko, przeprowadzając analizę

ryzyka. Aby stwierdzić czy jest ona dokonywana w przedsiębiorstwach zadano pytanie 19 *Proszę określić czy w jednostce jest dokonywana identyfikacja oraz analiza ryzyka?*

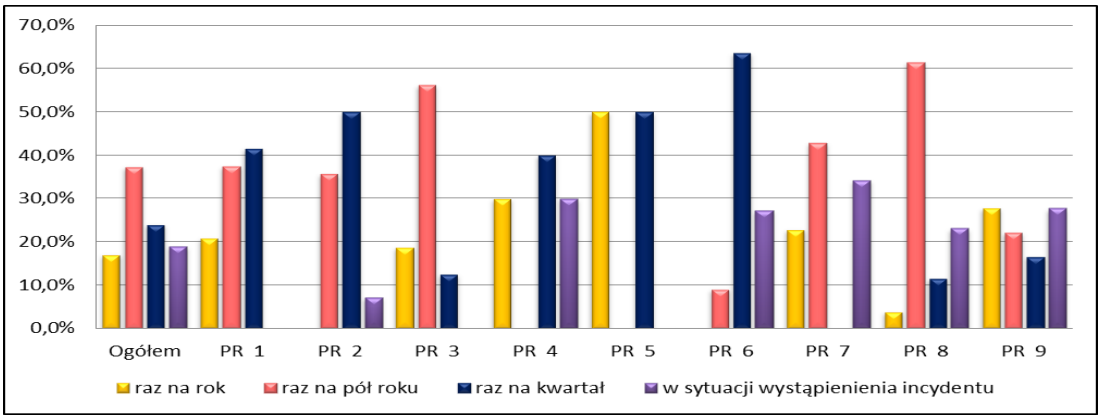


Rysunek 44. Wskazanie odpowiedzi „identyfikujemy i analizujemy ryzyko"
Źródło: Opracowanie własne na podstawie badań ankietowych

O działaniach potrzeby identyfikacji oraz analizy ryzyka świadomych jest ogółem (54,4%) przebadanych. Jednak, aby zachować odpowiedni poziom bezpieczeństwa w organizacjach, należy przez cały czas kontrolować ryzyko, a co za tym idzie szukać możliwości zaimplementowania nowych zabezpieczeń. Należy uznać, ze niedokładnie i nienależycie przeprowadzona analiza ryzyka może zmniejszyć ogólny poziom bezpieczeństwa informacji w organizacji.

Z otrzymanych wyników zauważono, że pracownicy mają małą wiedzę dotyczącą analizy ryzyka. W tym przypadku nie da się pominąć opinii respondentów z PR 3, PR 4, PR 5 i PR 8, które odbiegają od innych organizacji.

W ramach badań kolejne pytanie jest powiązane z pytaniem poprzedzającym i dotyczy wskazań, jak często jest dokonywana identyfikacja i analiza ryzyka. Rozkład odpowiedzi na pytanie 20 umieszczony został na rysunku 45.

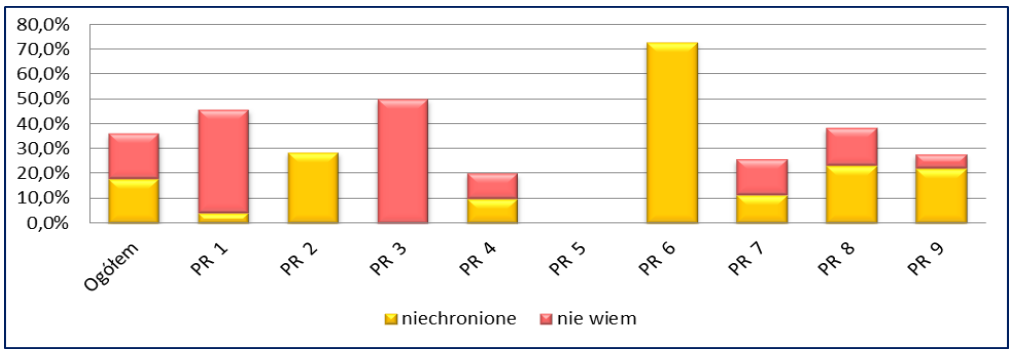


Rysunek 45. Częstotliwość dokonywania identyfikacji oraz analizy ryzyka w przedsiębiorstwach
Źródło: Opracowanie własne na podstawie badań ankietowych

Zauważając zróżnicowane odpowiedzi w tym temacie można odnieść nieodparte wrażenie, że pracownicy nie wiedza, z jaką częstotliwością powinno się dokonywać takiej analizy.

W literaturze przedmiotu, wskazuje się na poprawność dokonywania analizy ryzyka, co najmniej raz na rok. Można, więc przyjąć, że tylko 17,1% przebadanych utożsamiło się z tym zdaniem. Ale nie bez znaczenia jest też przeprowadzenie jej w sytuacji pojawiających się nowych zagrożeń. Przeprowadza się wtedy badanie rodzaju i poziomu ryzyka oraz niezidentyfikowanych dotychczas nowych zagrożeń.

Z uwagi na to, że nadal przechowuje się dokumenty w formie papierowej to należy liczyć się z ich dużą podatnością na zagrożenia ze strony człowieka. Używanie papieru, jako formy zapisu informacji wymaga zapewnienia szczególnego jej przechowywania w archiwach, pokojach biurowych, zamykanych szafach, uniemożliwiając tym samym dostęp do nich tylko osobom nieuprawnionym. Z tym też związane jest pytanie 25 z kwestionariusza ankiety.



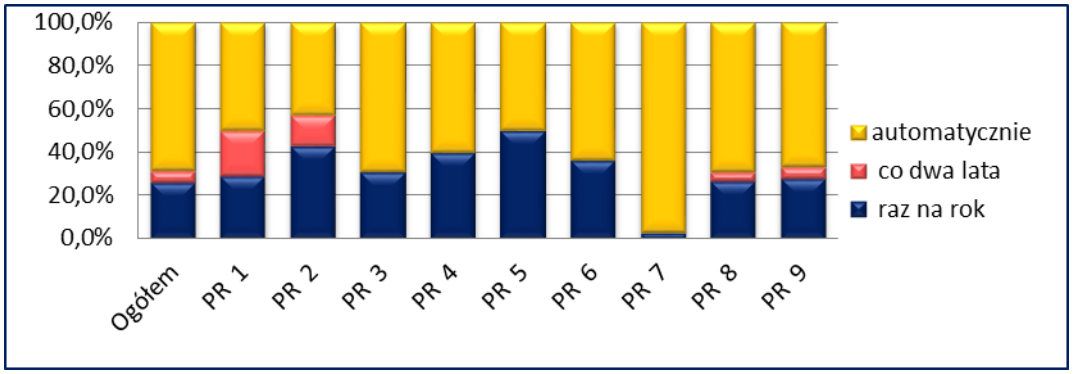
Rysunek 46. Sposób przechowywania dokumentów w organizacjach
Źródło: badania własne na podstawie przeprowadzonych badań ankietowych

Przedstawione odpowiedzi respondentów w większości pokazują trend, jaki panuje wewnątrz przedsiębiorstw. Przedstawione wyniki badań wskazują, że organizacje nie przestrzegają zasad związanych z właściwym przechowywaniem dokumentów, gwarantującym poufność informacji. W opinii 17,7% respondentów negatywnie oceniono sposób przetrzymywania dokumentów, z kolei 18,4% ogółu respondentów w ogóle nie wie, jak są przechowywane dokumenty. Należy podkreślić, że nieodpowiedni sposób przechowywania dokumentów może być ściśle powiązany z przypadkowym bądź celowym ujawnieniem informacji i może być źródłem zagrożenia szpiegostwa gospodarczego. Z analizy danych wynika, że PR 2, PR 6 mają poważny problem, nie wiedząc jak przechowywać dokumenty. W 6-tym

przedsiębiorstwie z uwagi na tak duży odsetek zaznaczonych negatywnych odpowiedzi (72,7%) przeanalizowano, jaka grupa badawcza zajęła takie stanowisko. W mniejszym stopniu dotyczyło to również drugiego przedsiębiorstwa (28,6%) gdzie uzyskano podobne odpowiedzi.

Dokonując szerszej analizy szóstej organizacji kierownicy wyższego szczebla są przekonani o potrzebie odpowiedniego zabezpieczania dokumentów. Jednak w świetle przeprowadzonych badań należy zauważyć, że 54,5% pracowników zatrudnionych na stanowiskach niekierowniczych, wyraziła opinię odmienną niż w innych przedsiębiorstwach twierdząc, że dokumenty są nieodpowiednio zabezpieczone. Świadome dopuszczenie do takiego zjawiska jest oznaką braku edukowania pod względem odpowiedniego zabezpieczenia dokumentów bądź też ignorowania obowiązujących przepisów.

Z uwagi na to, że informacja i systemy informatyczne to aktywo o ogromnym znaczeniu, więc wymaga się zabezpieczenia jej niezależnie od występującej formy zapisu. Zapewnienie bezpieczeństwa systemom informatycznym jest składową BI. Z tego też względu, aby bezpiecznie użytkować sprzęt komputerowy należy zaopatrywać się w autoryzowane programy certyfikowane, zgodne z najwyższymi wymogami ISO. Należy również zwrócić uwagę na programy antywirusowe, które podlegają aktualizacji. Z tą tematyką związane jest pytanie 27 *Jak często dokonuje się w Pani/Pana firmie aktualizacji oprogramowania antywirusowego?*

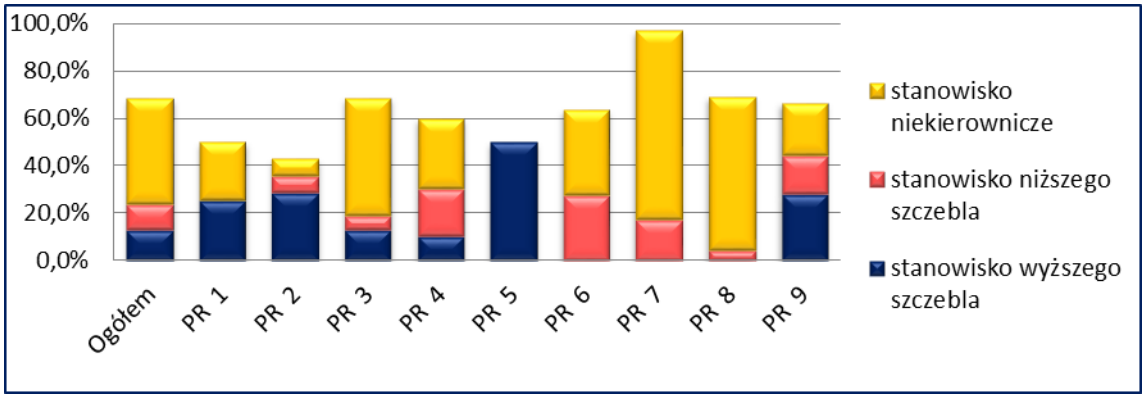


Rysunek 47. Rozkład odpowiedzi respondentów dotyczących częstotliwości aktualizacji oprogramowania antywirusowego
Źródło: Opracowanie własne na podstawie badań ankietowych

Należy przyznać, że infrastruktura informatyczna w organizacji jest jednym z elementów podatnych na zagrożenia bezpieczeństwa informacji. Wiąże się to nieodłącznie z kontrolowaniem przez cały czas oprogramowania antywirusowego i pobierania coraz to nowych dostępnych aktualizacji, zgodnie z działaniem systemu.

Profilaktyka antywirusowa ma za zadanie zminimalizować ryzyko strat powstałych na skutek działalności wirusów oraz złośliwych programów, dlatego też zaleca się przeprowadzanie regularnych aktualizacji oprogramowania, w tym aktualizacji baz wirusów. Z taką opinią zgadza się 68,4% ogółu przebadanych z wszystkich przedsiębiorstw. Wyjątkiem są PR 1 PR 5 (50%) oraz PR 2 (42,9%), w których automatyczna aktualizacja stosowana jest najrzadziej. Ważnym jest, aby pracownicy wiedzieli, że automatyczna aktualizacja zabezpiecza w pełni system antywirusowy, w wyniku, czego nie narażają organizacji na dodatkowe incydenty związane z atakami komputerowymi.

Dalsza analiza pozwoli na szersze spojrzenie, w jakich grupach badani pracownicy udzielili odpowiedzieli „ aktualizacja automatyczna".

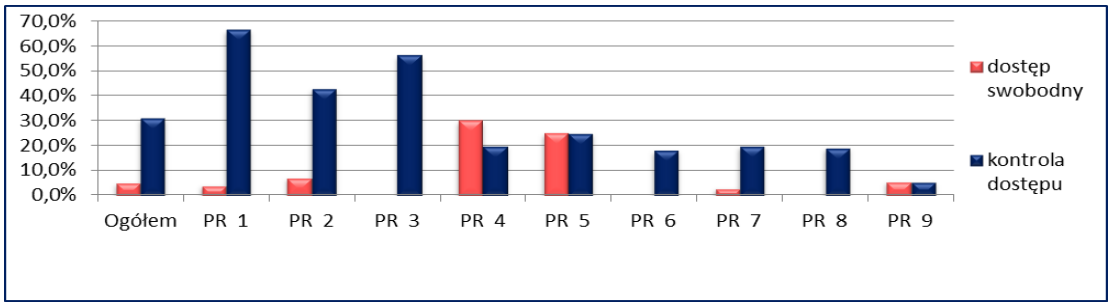


Rysunek 48. Wskazanie aktualizacji automatycznej, jako poprawnej odpowiedzi wg. zajmowanego stanowiska

Źródło: Opracowanie własne na podstawie badań ankietowych

Wyniki przeprowadzonych badań pokazały, że to właśnie kadra niekierownicza jest niejednokrotnie doskonale zorientowana, jeśli chodzi o aktualizację oprogramowania antywirusowego (44,9%). Pozostali badani z innych grup stanowiskowych również znali odpowiedź na to pytanie i zdają sobie sprawę z konieczności automatycznej aktualizacji oprogramowania, choć w nieco mniejszym stopniu. Wskazuje to na bardzo dobrą świadomość, znaczenia roli i funkcji działania sprawnego sytemu oprogramowania antywirusowego.

Równie istotnym elementem gwarantującym zachowanie bezpieczeństwa samych budynków organizacji jest nadzór nad dostępem do pomieszczeń poprzez zastosowanie sposobu kontroli wejścia osób postronnych na teren organizacji. Z tym też związane jest pytanie, 29: w *jaki sposób zorganizowany jest w przedsiębiorstwie dostęp do budynków i pomieszczeń biurowych?*. Odpowiedzi przedstawione zostały na rysunku 49.

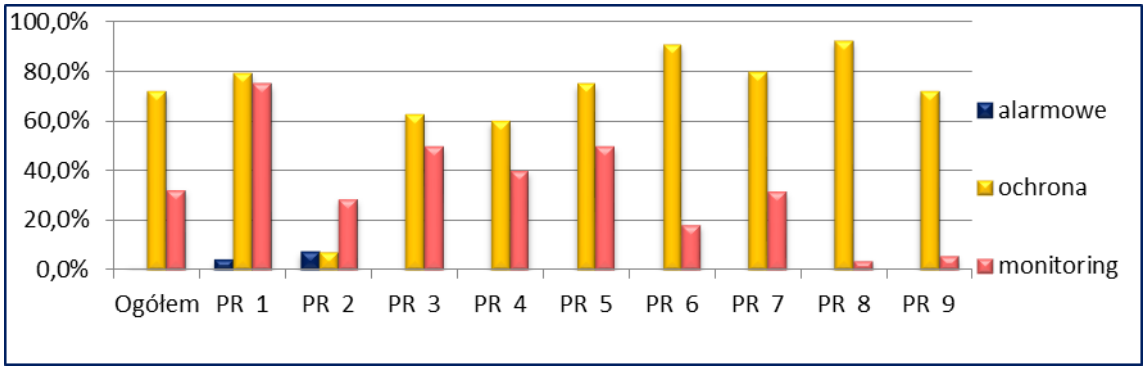


Rysunek 49. Sposób zorganizowania ochrony budynku
Źródło: Opracowanie własne na podstawie badań ankietowych

Analiza stanu aktualnego jest podstawą do wskazania, że w prawie wszystkich organizacjach kontrola dostępu, jest uznawana, jako stosowana ochrona budynku, poprzez zewnętrzne firmy ochroniarskie, które zabezpieczają organizacje. Jednocześnie jednak zastanawiający jest fakt, że mimo zastosowanej kontroli dostępu w dalszym ciągu istnieje możliwość wejścia do PR 1, PR 3, PR 4, i PR 5. W grupie badanych przedsiębiorstw znalazły się osoby, które wskazały na możliwość swobodnego dostępu do organizacji. Odpowiedzi w tym zakresie udzieliła grupa osób pracujących na stanowiskach niekierowniczych, która być może nie posiada wiedzy, związanej z kontrolą i nadzorem osób postronnych po organizacji. Autorytarnie można stwierdzić, iż pomimo występujących procedur, jednak widoczne jest, że goście poruszają się po organizacji bez specjalnego nadzoru. Świadczy to o braku nadzoru w organizacjach.

Na zadane pytanie z ankiety wzorcowo odpowiedziała grupa, pracowników z PR 6, PR 8 (20% odpowiedzi).

Druga część pytania 29 dotyczy analizy zastosowania metod wyboru systemów zabezpieczających, alarmowych oraz monitoringu lub firmy ochroniarskiej. Rysunek 50 nawiązuje do zestawieniowych odpowiedzi.



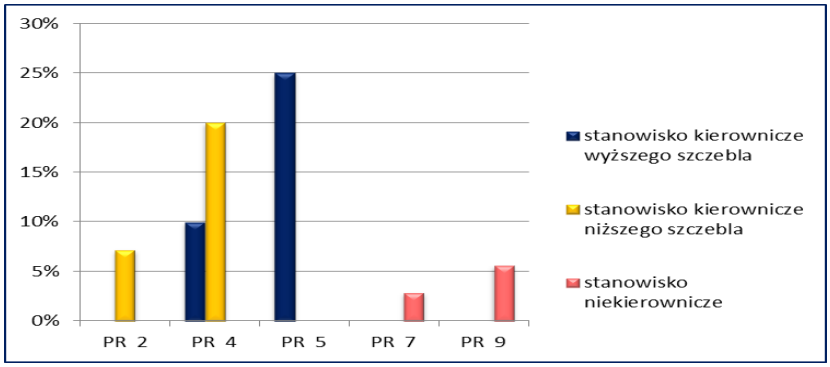
Rysunek 50. Zastosowanie systemów zabezpieczających w celu ochrony budynku
Źródło: Opracowanie własne na podstawie badań ankietowych

Z interpretacji danych przedstawionych na rysunku 50 można stwierdzić, że organizacje korzystają z usług firm ochroniarskich w 72,2%, systemów alarmowych 1,3%, monitoringu wizyjnego 32,3%. Okazuje się, że na ogół najczęściej stosowanymi zabezpieczeniami jest korzystanie z usług firm ochroniarskich.

Zatem analizując otrzymane wyniki można zauważyć, że mimo stosowanych pośrednich zabezpieczeń w organizacjach możliwe jest wejście do budynków na teren organizacji, gdyż swobodne wejście do budynku zadeklarowało 5,1% ogółu przebadanych. W PR 1, PR 3, PR 4, PR 5 ankietowani zwrócili uwagę na swobodny dostęp do budynku, jednocześnie w tych samych organizacjach średnio 65% ankietowanych wskazało na zabezpieczenia budynku poprzez usługi firmy ochroniarskiej. Dowodzi to, że firmy ochroniarskie nie zachowują odpowiedniej ostrożności przy wpuszczaniu osób, gości z zewnątrz (tzw. anonimowych, przypadkowych lub znajomych). Analizując wzorcowe odpowiedzi wykreowano grupę pracowników z PR 7, PR 8, PR 9, którzy uznali, że możliwa jest pełna kontrola osób wchodzących/wychodzących i w pełni zabezpiecza to przedsiębiorstwo przed zagrożeniem utraty bezpieczeństwa informacji.

Skoro omawiane trzy ostatnie organizacje zastosowały monitoring oraz ochronę w postaci firmy zewnętrznej warto dokonać analizy badawczej, jaka grupa pracowników nadal jest zdania, że można wejść swobodnie do organizacji.

Odpowiedzi grupy respondentów wg. zajmowanych stanowisk na pytanie 29.

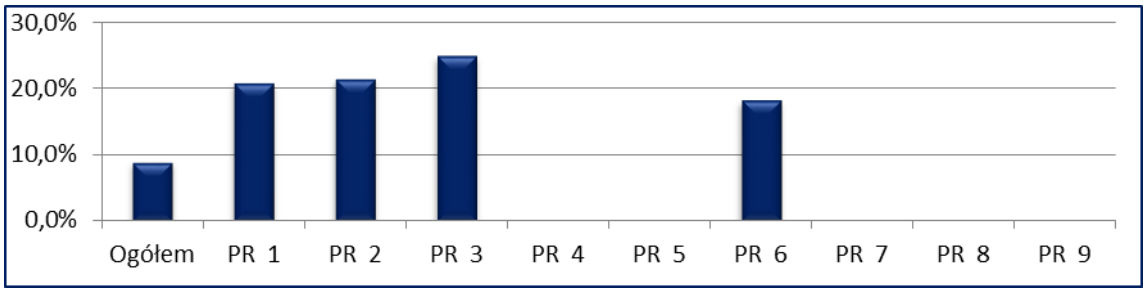


Rysunek 51. Swobodny dostęp do budynku wg. opinii ankietowany
Źródło: Opracowanie własne na podstawie badań ankietowych

Analizując poszczególne odpowiedzi można stwierdzić, że pogląd ten podziela kadra nie kierownicza. Być może taka opinia wynika z braku posiadanej wiedzy na ten temat. Pracownicy ci nie muszą przechodzić przez recepcję i wpisywać się w rejestr gości. Więc wydaje im się, że można swobodnie wejść na teren organizacji.

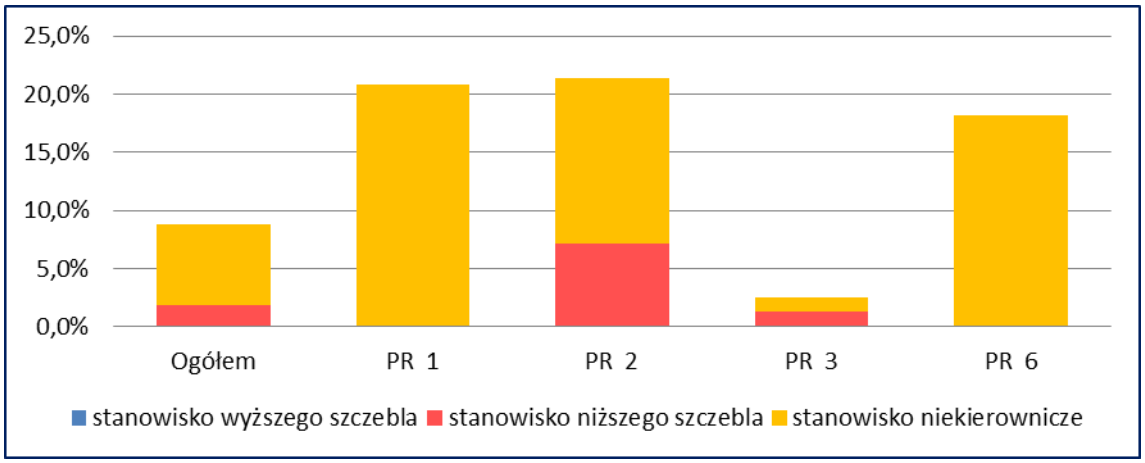
Jednak w podobnym tonie wypowiadają się ci sami respondenci w pytaniu 36 dotyczącym kwestii sposobu przyjmowania gości w organizacji.

Każdego dnia przez organizacje przechodzi wielu interesantów, partnerów, kontrahentów czy gości. Zdarza się też, że są to osoby anonimowe. Bezpośrednio wiązana jest z tym podatność, która zbagatelizowana może uaktywnić zagrożenie.
Pytanie 36 wskazuje na problem swobodnego poruszania się takich osób po terenie organizacji.



Rysunek 52. Odsetek odpowiedzi wskazujących na możliwość swobodnego poruszania, się po terenie firmy
Źródło: Opracowanie własne na podstawie badań ankietowych

Z rysunku 52 wynika, że nie kontroluje się w PR 1, PR 2, PR 3, PR 6 osób odwiedzających organizację. To zarząd oraz kierownictwo wprowadzają procedury obejmujące sposoby postępowanie z gośćmi podczas ich odwiedzin. Kolejny rysunek ujawnia grupy zajmowanych stanowisk, którzy udzielili takiej odpowiedzi.

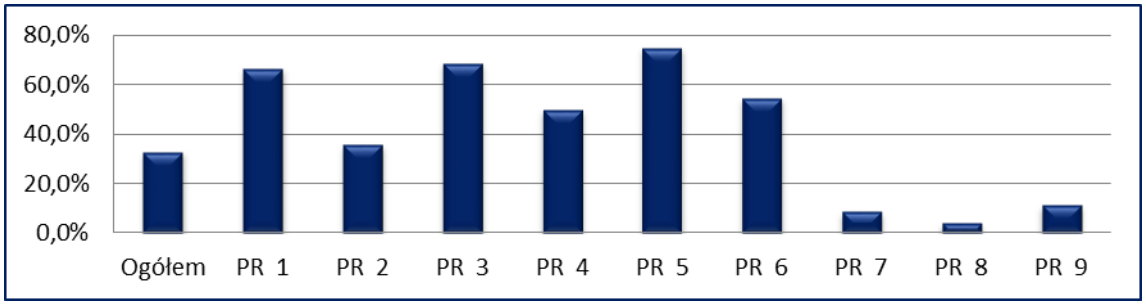


Rysunek 53.Zadeklarowanie swobodnego poruszania, się po budynkach firmy wg. opinii respondentów dla grup stanowiskowych
Źródło: Opracowanie własne na podstawie badań ankietowych

Dane przedstawione na rysunku 53 wskazują, że takiego zdania są osoby, które nie są zatrudnione na stanowiskach kierowniczych, z tego też względu nie posiadają one uprawnień do oprowadzania gości. Natomiast część (1,9%) ogółu kierowników niższego szczebla, którzy odpowiedzieli, że w organizacji swobodnie poruszają się

goście powinna być zaznajomiona z procedurami PBI, w której powinien być opisany sposób przyjmowania osób postronnych. Przestrzeganie procedur PBI to fundament BI a łamanie procedur bezpieczeństwa przez kierownictwo niższego szczebla, może doprowadzić do powstawania nowych zagrożeń.

PBI określa, jak się zachować podczas przyjmowania osób z zewnątrz i określa też, sposób prowadzenia rejestru gości. Czynności kontrolne są niezwykle istotne z punktu widzenia bezpieczeństwa informacji. Wskazane odpowiedzi badanych na pytanie 35 zaprezentowano na rysunku 54.



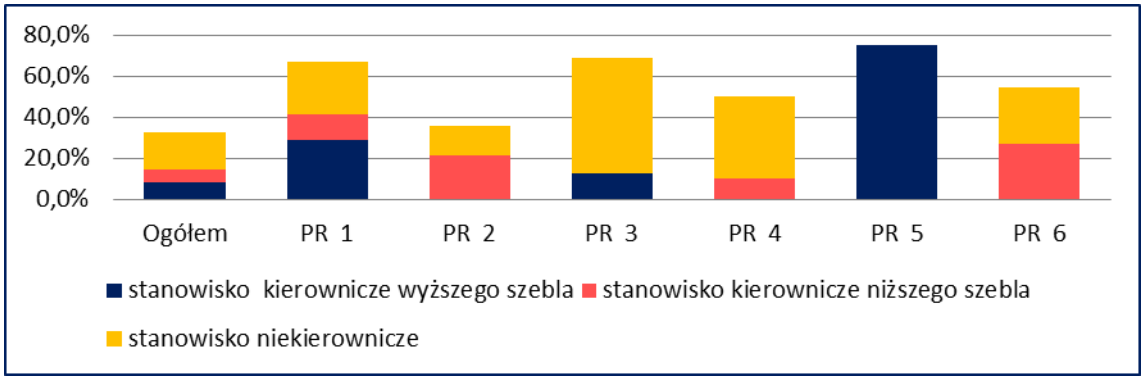
Rysunek 54. Respondenci zwracający uwagę, na brak prowadzenia rejestru osób wchodzących i wychodzących z przedsiębiorstwa
Źródło: badania własne na podstawie badań ankietowych

Z przeprowadzonych badań wynika, że w trzech ostatnich firmach jest większość pracowników świadomych konieczności prowadzenia rejestru odwiedzin gości oraz przestrzegania zapisów PBI, w której to powinna być opisana procedura przyjmowania gości. Dane przedstawione na rysunku 38 dla PR 1(66,7%), PR 2 (35,7%), PR 3 (68,8%), PR 4 (50%), PR 5 (75%), PR 6 (54,5%) świadczą o braku prowadzenia rejestru wejść/wyjść. Średnio zadeklarowało brak prowadzonego takiego rejestru 32,9 % badanych respondentów.

Wskazać należy, że prowadzenie kontroli związanej z odpowiednim postępowaniem podczas wejścia/wyjścia nie gwarantuje poczucia anonimowości, gdyż w każdej chwili można sprawdzić, kto, kiedy, wchodził lub wychodził z organizacji. Jest to pomocne w monitorowaniu ewentualnych nieuprawnionych działań zwolnionych pracowników (wejścia w nocy,

lub po godzinach urzędowania organizacji). Prowadzenie takiego rejestru wejść/wyjść ma kluczowe znaczenie w zapewnieniu wszystkich atrybutów informacji w bezpiecznej organizacji.

Słusznym, więc jest wskazanie grupy pracowników odpowiadających, że nie ma w organizacji rejestru osób w/w. Zestawienie otrzymanych wyników przedstawiono na 55 rysunku.

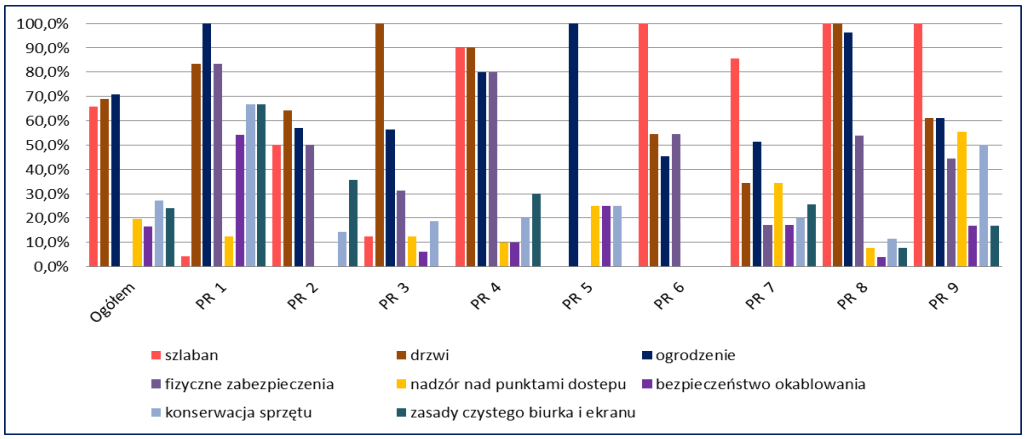


Rysunek 55. Brak prowadzenia rejestru wg. grup stanowiskowych
Źródło: badania własne na podstawie badań ankietowych

Z interpretacji danych przedstawionych na rysunku 55 można stwierdzić, że w pierwszych sześciu przedsiębiorstwach zauważono znaczną nieprawidłowość dotyczącą niewłaściwego zorganizowania ochrony przed wejściem/wyjściem z budynku. Należy zauważyć, że odpowiedzi takich udzieliły głównie osoby na stanowiskach niekierowniczych lub kierowniczych niższego szczebla (oprócz PR 5). Sytuacja taka może wynikać z braku informowania kierowników niższego szczebla o wprowadzeniu rejestru wejść/wyjść lub też zarząd organizacji uznał, że tego typu informacje, są zbędne dla świadomości pracowników niższego szczebla. Zaistniała sytuacja zostanie wyjaśniona w dalszych badaniach podczas wywiadu.

Natomiast na uwagę zasługuje sytuacja w PR 1, PR 5 gdzie nie wprowadzono procedur rejestru w/w i nie przestrzega się zasad wewnętrznych organizacji. Kierownictwo rządzące w wyniku braku kontroli nad osobami odwiedzającymi przedsiębiorstwo nie przykłada do tego szczególnej wagi dając przyzwolenie na swobodne poruszanie się po terenie organizacji. A to nie ma nic wspólnego z zapewnieniem odpowiedniego poziomu zabezpieczeń fizycznych gdzie powinno się ograniczyć potencjalnym intruzom dostęp do organizacji. Ponadto, dopuszczając do takiej sytuacji organizacja może być postrzegana, jako niedbająca o bezpieczeństwo pracowników, powierzonych aktywów oraz samej informacji.

Zbiór konwencjonalnych środków i elementów ochronnych stosowanych w przedsiębiorstwach to zabezpieczenia fizyczne. W celu zbadania czy przedsiębiorstwa korzystają z nich zadano pytanie 30 dotyczące używanych rodzajów zabezpieczeń w przedsiębiorstwach. Przedstawione odpowiedzi zaprezentowano na rysunku 56.



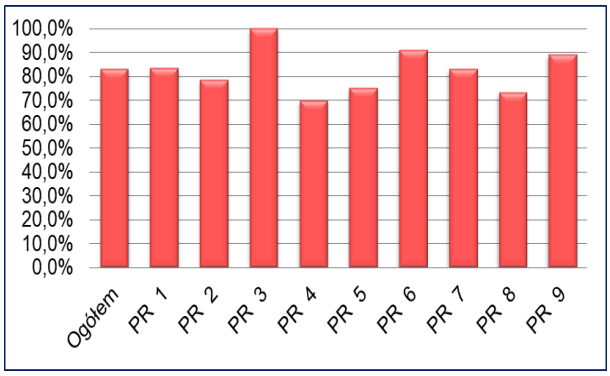
Rysunek 56. Stosowane w przedsiębiorstwach zabezpieczenia

Źródło: Opracowanie własne na podstawie badań ankietowych

Wyniki pokazały, że kluczowymi zabezpieczeniami są: ogrodzenie (70,9%), drzwi (69%) oraz szlaban przy wjeździe (65,8%). Biorąc pod uwagę znaczenie zabezpieczenia, jakim są zasady czystego biurka stosunkowo mało badanych (24,1%) wskazało na tą odpowiedź. Przyjmuje się, więc bagatelizowanie roli i znaczenia, tego działania prewencyjnego.

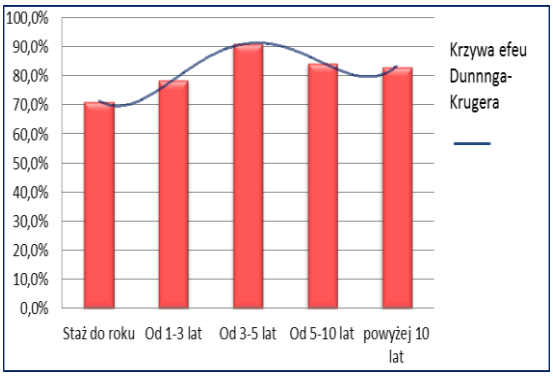
Warto zaznaczyć, że jest to niezwykle istotny element w całym systemie bezpiecznego przechowywania informacji. Dzięki wprowadzeniu polityki czystego biurka omija się wiele sytuacji problemowych, gdzie ktoś może przeczytać poufną wiadomość lub po prostu ukraść dokument. Dlatego najlepiej przechowywać je w zamykanej szafie do tego przeznaczonej.

Często przyczyną utraty informacji jest wykonywanie podczas pracy prywatnych działań. Aby zweryfikować istniejący stan rzeczy zadano pytanie 32. *Czy w godzinach pracy zdarza się Państwu korzystać z innych stron internetowych w celu prywatnych potrzeb (poczta, portale społecznościowe, itp.)* Odpowiedź ankietowanych na to pytanie z punktu widzenia zachowania w organizacji atrybutów bezpieczeństwa jest niezwykle istotna.



Rysunek 57. Ilość osób, które w godzinach pracy korzystają ze stron internetowych

Źródło: Opracowanie własne na podstawie badań ankietowych w organizacjach gospodarczych



Rysunek 58. Korzystam ze stron internetowych wg. stażu pracy

Źródło: Opracowanie własne na podstawie badań ankietowych w organizacjach gospodarczych

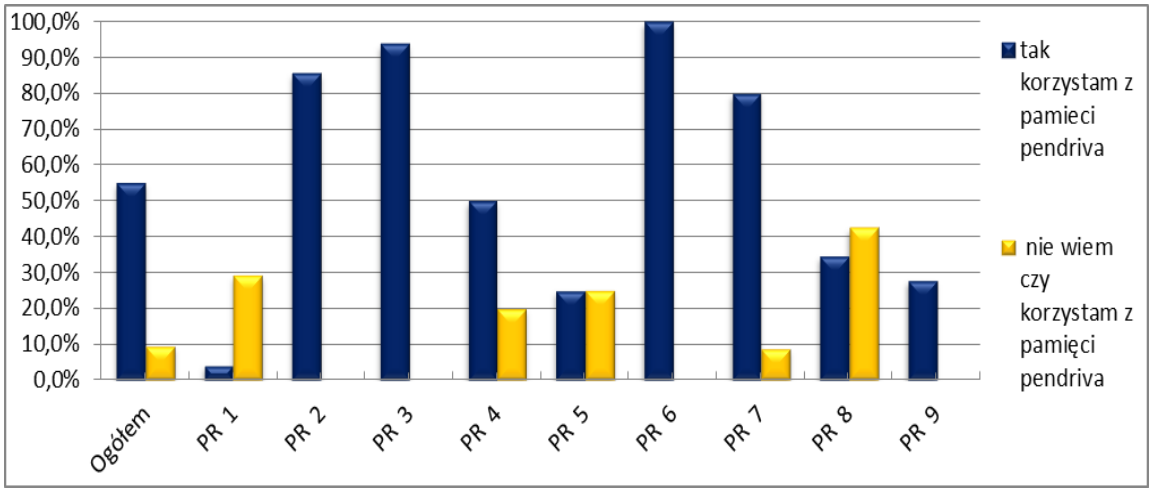
Wyniki badań pokazały, że zdecydowana większość respondentów (82,9%), w godzinach pracy korzysta z Internetu w celach prywatnych. Skoro w organizacjach wyraźną potrzebą jest skuteczniejsza ochrona bezpieczeństwa informacji, to nasuwa się sugestia, że w organizacjach brak jest świadomości w tym obszarze. Zatem, najprawdopodobniej zarządzający nie są świadomi, a tym bardziej przekonani o nieotwieraniu przez pracowników załączników do poczty emaliowej, pochodzących z niewiadomego źródła. W nawiązaniu do odpowiedzi na to pytanie można dodać, że w wyniku przeprowadzonego wywiadu zdiagnozowano problem braku prowadzenia nadzoru nad odpowiedziami na zbędne wiadomości spam.

Są to istotne kwestie, z uwagi na rosnącą ilość zagrożeń spowodowanych różnego rodzaju wirusami uaktywniającymi się podczas przesyłania danych w sieci. Aby takiego stanu nie lekceważyć, kierownictwo organizacji powinno skupić uwagę na działaniach zapobiegających takiemu postępowaniu pracowników.

Zgodnie z danymi zawartymi na rysunku 58 należy uznać, że nie ma różnicy między pracownikami, którzy dopiero zaczynają pracę, a tymi, którzy już od wielu lat pracują w organizacji. Po raz kolejny w analizie otrzymanych wyników można powołać się na krzywą efektu Dunninga-Krugera, gdzie powszechnym zjawiskiem i pułapką staje się po prostu błędne myślenie, co do własnej samooceny. I tak im niższa wiedza tym wyższe wyobrażenie o swoich kompetencjach. Osoby o krótkim stażu, początkujące przeceniają swoje możliwości i zdolności, natomiast znawcy tematu, pracownicy długoletni mocno te umiejętności i wiedzę zaniżają. Wskazuje to na fakt, braku umiejętności dokonania własnej obiektywnej samooceny przez pracowników.

Niezależnie od krzywej efektu Dunninga-Krugera można powiedzieć, że przeglądanie prywatnych stron internetowych w godzinach pracy jest jak najbardziej praktykowane w przedsiębiorstwach.

Kolejnym realnym zagrożeniem bezpieczeństwa danych jest używanie prywatnych nośników pamięci podczas pracy na urządzeniach służbowych. Najczęściej takie przenośne nośniki pamięci nie są zabezpieczone, więc z łatwością może umiejscowić się tam wirusa, który później uaktywni się na urządzeniu służbowym. Ponadto, najczęściej domowe zabezpieczenia nie są na tyle skuteczne i dobrze dobrane, jak programy antywirusowe zakupione i uaktualniane przez przedsiębiorstwo. Zjawisko to nie należy do bezpiecznych, więc i w skutkach też może być zgubne. Pytanie 33 dotyczy też tego tematu *„Czy w czasie pracy można korzystać z prywatnej pamięci flash, pendriva”?* Rysunek 59 prezentuje wynik otrzymanych opinii na omawiany temat.

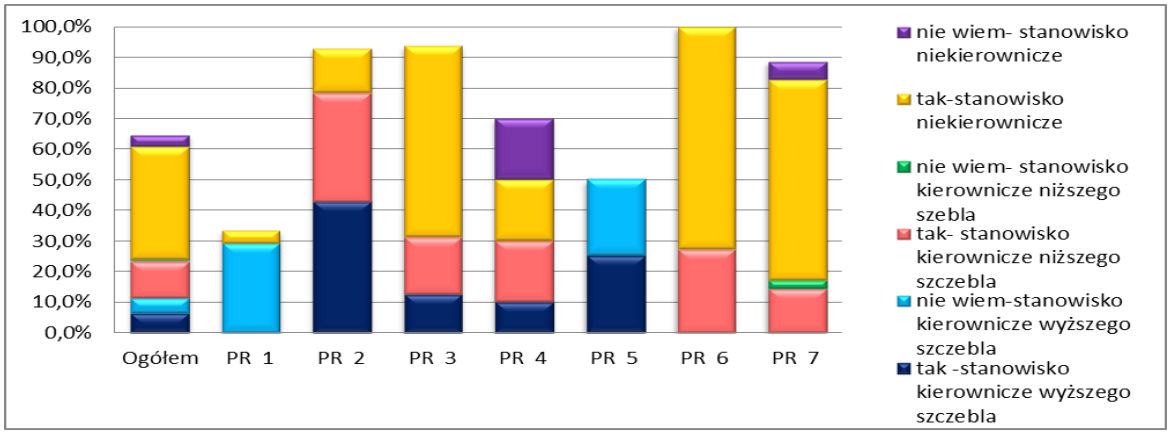


Rysunek 59. Wskazanie odpowiedzi pozytywnej „tak” oraz „nie wiem”, na pytanie o możliwość korzystania z pendrive w czasie pracy
Źródło: badania własne na podstawie badań ankietowych

Badani odpowiadając mogli skorzystać z wielu możliwości. Pod uwagę wzięto dwie odpowiedzi tzn. ”tak” oraz „nie wiem”, które wg. autorki pracy są niedopuszczalne z punktu widzenia bezpiecznego przechowywania informacji w organizacji (w badaniu tym sprawdzono ile osób faktycznie korzysta z pamięci flash pendrive). Rozpatrywanie wskazań odpowiedzi *„nie”* byłoby w tym wypadku bezzasadne. W badaniu skupiono uwagę na odpowiedziach *„tak”* oraz *„nie wiem”* (powyżej wskaźnika 50%). Zaznaczenie opcji „nie wiem” wskazuje na wybranie opcji wymijającej, na którą oddało swoją opinię ogółem 9,5% badanych przypadków. Logicznym wydaje się wskazanie odpowiedzi, czy respondenci korzystają z prywatnej

pamięci pendrive czy też nie. Zatem, obie omawiane odpowiedzi nie są poprawnymi wskazaniami. Ogółem 55,1% pracowników korzysta z takiej formy zapisu nośnika informacji. Zatem z rysunku 59 wynika, że pracownicy powszechnie korzystają w godzinach pracy z dodatkowych pamięci flash czy pendrive. Zaprezentowane wyniki wskazują na skalę podejścia do tego tematu. Jest to bardzo niepokojący fakt, gdyż może on się okazać zgubny w skutkach dla przedsiębiorstwa. Przodującymi organizacjami, którzy dopuszczają do użycia prywatnych nośników pamięci okazali się pracownicy z PR 2, PR 3, PR 4, PR 6, PR 7 (powyżej progu 50%).

Analiza odpowiedzi w grupach stanowiskowych pokazała grupy pracowników: kierowniczych wyższego szczebla, niższego oraz niekierowników, którzy mogą korzystać w czasie pracy z prywatnych nośników informacji w PR 2, PR 3, PR 6, PR 7.



Rysunek 60. Pozytywne odpowiedzi korzystania z prywatnej pamięci flash, pendrive w czasie pracy oraz odpowiedzi nie wiem wg. pracowników wyższego kierownictwa
Źródło: badania własne na podstawie przeprowadzonych badań ankietowych

Niepokój budzą odpowiedzi pracowników w PR 2, PR 3, PR 4, PR 6, PR 7 gdzie widać, że w zarządzie brak kontroli nad używaniem w czasie pracy prywatnych nośników danych. Co prawda, najwięcej odpowiedzi „tak" wskazali niekierownicy w PR 3 (62,5%), PR 6 (72,7%) i PR 7 (65,7%) to jednak, kierownicy niższego szczebla też wyrazili podobną opinię „tak" w PR 3 (18,8%), PR 6 (27,3%), PR 7 (14,3%). Natomiast w PR 4 oprócz omawianych dwóch grup pracowniczych używających nośników informacji pojawili się jeszcze pracownicy wyższego kierownictwa (10%) używający takich nośników w czasie pracy. Z przytoczonych wyników zauważono, że stan w organizacjach PR 3, PR 6, PR 7 jest bardzo zbliżony, mianowicie brak w zachowaniu pracowników ostrożności podczas korzystania w godzinach pracy z prywatnych nośników danych. Zauważa się tutaj lukę w działaniu systemu bezpieczeństwa informacji. Jeśli faktem, jest używanie prywatnych nośników danych to

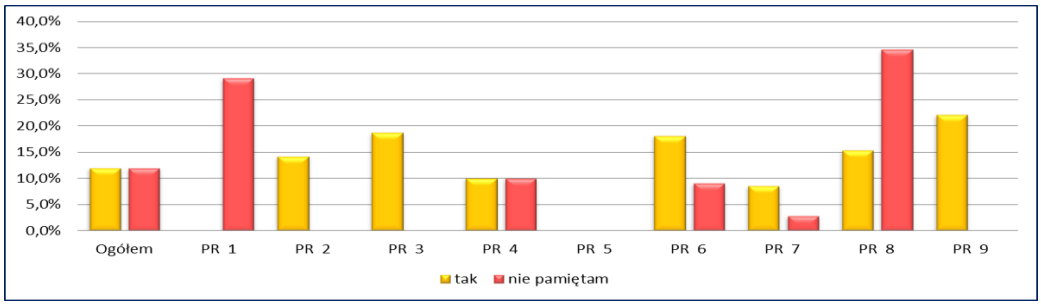
zastanawiające jest to, czy w organizacjach jest osoba odpowiedzialna za kontrolę nad tego typu nośnikami informacji. Ważny jest również sposób i wybór zabezpieczenia takiego prywatnego nośnika oraz gwarancja usunięcia danych podczas utylizacji. Dopuszczając do używania przez pracowników prywatnych nośników danych organizacja jest zobowiązana do nadzorowania ich, aby nie stracić kontroli nad zawartymi na nich informacjami.

Organizacja szanująca swoje zasoby nie powinna dopuścić do tego, aby jej pracownicy używali swojego prywatnego sprzętu w celach służbowych. Należy zauważyć, że pracownicy wiedzą czy używają takich urządzeń czy też nie. Być może z innych względów nie chcą o tym mówić, dlatego skorzystali z odpowiedzi „*nie wiem"*. Należy uwzględnić tutaj opinię badanych z PR 2 (42,9%) i PR 3 (12,5%), gdzie stwierdzono grupę kierowników wyższego szczebla używających swoich prywatnych pamięci flash. Prywatnych nośników informacji nie chroni się w sposób szczególny, a taką podatnością na zagrożenia może być dostęp osób z rodziny, które mogą dopuścić do nieumyślnego lub umyślnego udostępnienia informacji oraz zgubić taką pamięć. Wówczas informacje firmowe mogłyby dostać się w niepowołane ręce. Zatem stan, które te odpowiedzi pokazują budzi niepokój.

Przedsiebiorstwo nr.1 wzorowo podchodzi do stosowania zakazu korzystania z takich urządzeń w czasie pracy, gdyż pracownicy odpowiedzieli negatywnie na to pytanie.

Nieco wcześniej, w pytaniu 15 respondenci wypowiadali się na temat utylizacji sprzętu używanego w przedsiębiorstwie np.: nośników danych. Większość z przebadanych wyraziła wówczas zdanie, że sami je utylizują. Zastanawiające, więc jest, czy prowadzony jest nadzór i kontrola nad likwidacją zużytych nośników w postaci monitoringu lub rejestru zużytego sprzętu? Temat ten zostanie wyjaśniony podczas dalszych badań tj. wywiadu.

Sytuacją wyjątkowo niebezpieczną dla pojawienia się podatności zagrożenia jest zgubienie przez pracownika sprzętu firmowego. Takich zdarzeń dotyczy pytanie 34 *Czy zdarzyło się Pani/Panu zgubić firmowy sprzęt komputerowy lub inne nośniki danych?* Odpowiedzi badanych respondentów prezentuje rysunek 61.

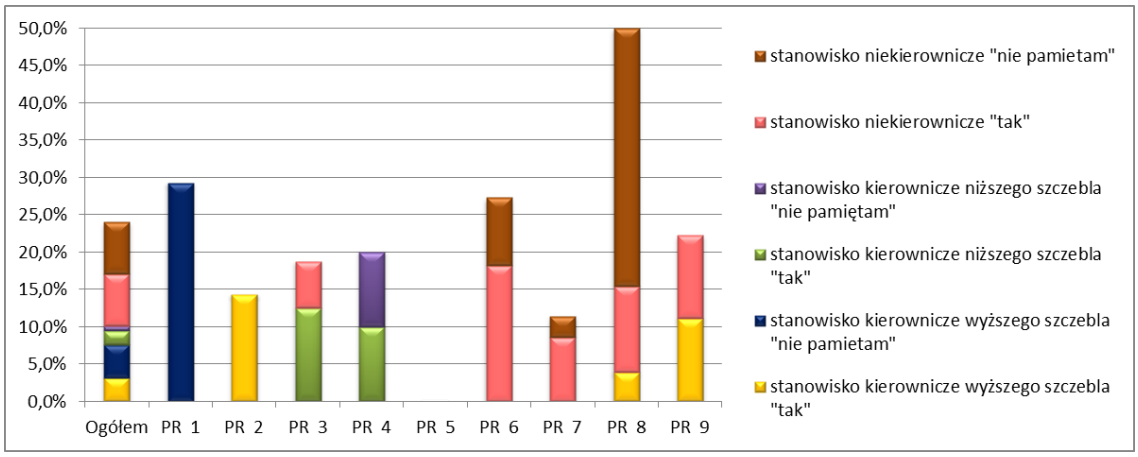


Rysunek 61. Odpowiedzi badanych potwierdzających zgubienie sprzętu firmowego oraz zaznaczenie odpowiedzi „nie pamiętam"
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

Z rysunku 61 wynika, iż zdecydowanej większości przebadanych, zdarzyło się zgubić sprzęt firmowy. Interesujące w badaniu jest to, jak wielu respondentów nie pamięta takiej sytuacji wskazując odpowiedź „nie pamiętam". Ogółem z wszystkich organizacji 12% respondentów nie pamięta takiego incydentu. W pierwszym przedsiębiorstwie wszyscy, którzy wzięli udział w badaniu uznali, że nie pamiętają o takim zdarzeniu.

W toku dalszych badań okazało się, że pracownicy są świadomi, jakie zagrożenia niesie ze sobą niezastosowanie się do podstawowych zasad bezpiecznego przechowywania czy transportowania urządzeń przenośnych. Jednak podczas wywiadu okazało się, że respondenci nie do końca są świadomi działań socjotechnicznych i nielegalnego pozyskiwania sprzętów, czy kradzieży w celu pozyskania strategicznych, tajnych informacji.

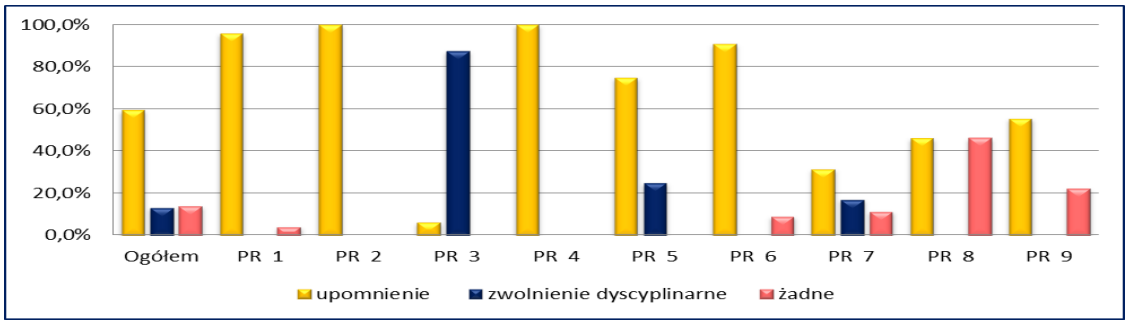
Należy jednak podkreślić istnienie grupy 12% ogółu ankietowanych, którym zdarzył się incydent zgubienia sprzętu komputerowego. Rysunek 62 pokazuje opinię przebadanych, wg. zajmowanego stanowiska w organizacji



Rysunek 62. Zgubienie sprzętu komputerowego oraz wskazanie odpowiedzi „nie pamiętam"
Źródło: Opracowanie własne na podstawie badań ankietowych

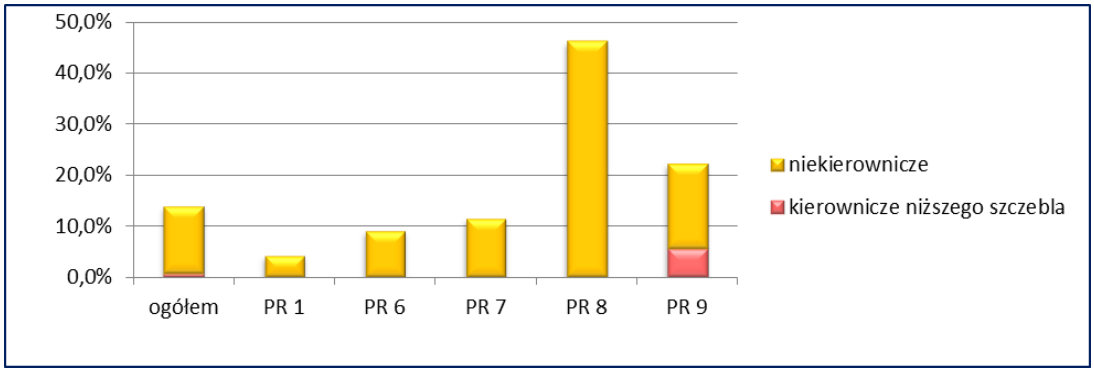
Odpowiedzi są bardzo zróżnicowane, więc nie można zagregować danych. Jednak w PR 5 badani, jako jedyni wzorcowo odpowiedzieli na to pytanie, nikt nie zgubił sprzętu komputerowego. W PR 2 na stanowisku wyższego szczebla, kierownicy zgubili sprzęt firmowy (14,3). W PR 8 (3,8%) i w PR 9 (11,1%) też analogicznie doszło do takiej sytuacji wśród pracowników na tym samym stanowisku. Być może wynika, to z braku poczucia ciągłego zagrożenia kadry kierowniczej i braku zachowania czujności, jaką należy zachowywać podczas przechowywania takich urządzeń.
Wynik odpowiedzi na to pytanie ankietowe wskazuje na istotny problem wynikający z braku poczucia odpowiedzialności za utratę służbowego sprzętu przez pracownika.

Polityka Bezpieczeństwa Informacji reguluje konsekwencje, jakie powinny grozić pracownikom za nieprzestrzeganie zasad bezpieczeństwa informacji. Z tym też związane jest pytanie 37 z kwestionariusza ankiety.



Rysunek 63. Konsekwencje grożące pracownikom, za nieprzestrzeganie zasad BI
Źródło: Opracowanie własne na podstawie przeprowadzonych badań ankietowych

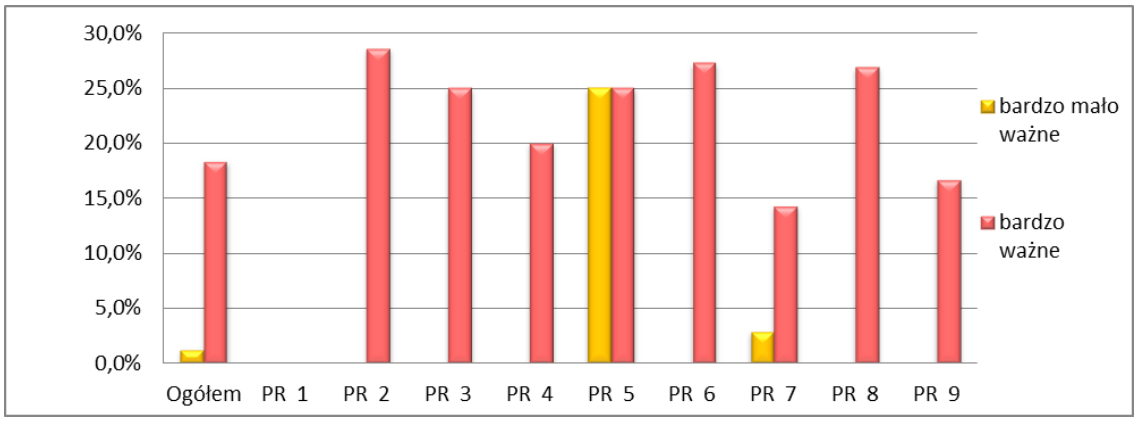
Dzięki przejrzystemu określeniu obowiązków każdego pracownika, nadania mu określonych uprawnień, ogranicza się możliwość nadużyć i wyłudzenia informacji na skutek niestosowania się do poszczególnych zasad bezpieczeństwa. Reguły opisane w PBI sprawdzają się na płaszczyźnie organizacji, a pracownicy zdają sobie sprawę z konsekwencji przekroczenia uprawnień. Aż 13,3% przebadanych z wszystkich organizacji jest świadoma kary *„zwolnienia dyscyplinarnego”* w razie ekstremalnego łamania praw i zasad bezpieczeństwa informacji, a z kolei 59,5% ankietowanych wydaje się być świadoma konsekwencji *„upomnienia”*. Jeszcze inną grupą stanowią ci, którzy wskazali na odpowiedź „żadne” w 13,9%. Wobec tego, można przypuszczać, że kwestia kar jest poważnie traktowana przez przedsiębiorstwa za wyjątkiem PR 8, gdzie wskazań na odpowiedz *„żadne”* jest dużo, mianowicie 46,2%. Należy uznać, że decyzję o nadaniu kary podejmuje sam zarząd organizacji, więc przyjmuje się, że w tym przedsiębiorstwie osoby na stanowiskach niekierowniczych nie są zorientowane, ·co do odpowiedzialności za ujawnienie informacji (rysunek 64).



Rysunek 64. Wskazanie odpowiedzi „żadne konsekwencje" wg. zajmowanych stanowisk pracy
Źródło: Opracowanie własne na podstawie badań ankietowych

Rysunek 64 prezentuje liczbę odpowiedzi *„żadne"* wg. grup stanowiskowych badanych respondentów. Pod uwagę wzięto odpowiedzi kierowników niższego szczebla oraz niekierowników, którzy nie są w posiadaniu wiedzy na temat istotności znaczenia bezpieczeństwa informacji.

Punktem wyjścia zwiększenia świadomości pracowników w organizacji jest ciągłe edukowanie grup pracowniczych szczególnie na szczeblu kierowniczym. Tego tematu dotyczy pytanie, 38 w jakim *stopniu Państwa zdaniem w firmie istnieje potrzeba szkolenia z zakresu bezpieczeństwa informacji?* Odpowiedzi przedstawiają dane zamieszczone na rysunku 65.

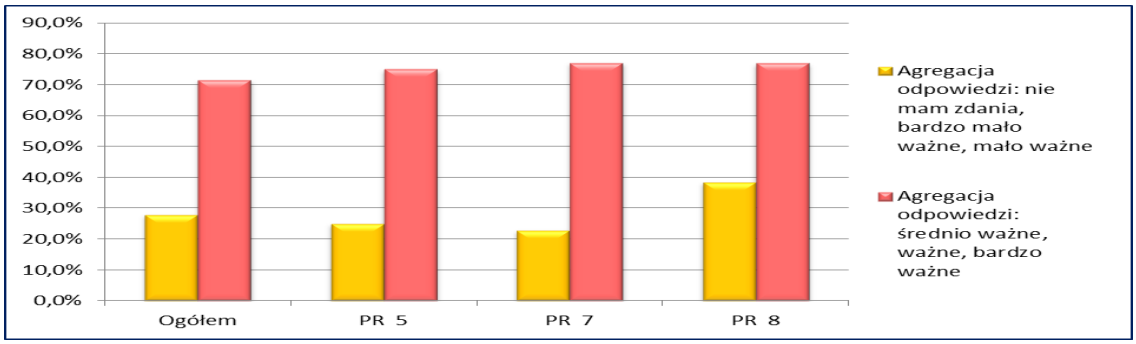


Rysunek 65. Określenie świadomości pracowników, wobec potrzeby szkoleń
Źródło: Opracowanie własne na podstawie badań ankietowych

Badania ujawniły, że ogółem 18,4% respondentów, udzieliło odpowiedzi ze wskazaniem na bardzo ważną potrzebę szkolenia. Poza danymi przedstawionymi na rys. 50 zauważono, że spośród przebadanych 1,3% odpowiedziało, że jest to dla nich bardzo mało ważne. Jest to stan zbieżny we wszystkich organizacjach oprócz PR 5 gdzie aż 25% respondentów uważa szkolenia zarówno za bardzo mało ważne jak i bardzo ważne.

Biorąc pod uwagę, zdiagnozowany we wcześniejszych pytaniach stan wiedzy badanych z zakresu należytego bezpiecznego przetwarzania danych informacji, można domyślać się że jest to związane z brakiem środków finansowych na takie zadania i cele. Niestety oszczędności dotyczą także programu szkoleń, które powinny być dopasowane do potrzeb osób nowo zatrudnionych i tymczasowo oraz pracujących na stałe.

W świetle przeprowadzonych wyników badań, zagregowano przeciwstawne odpowiedzi *„nie mam zdania”*, *„nie istotne”* i *„nieważne”* oraz reprezentujące odmienny pogląd tych rozbieżnych *„średnio ważne”, „ważne” i „bardzo ważne”*. Rysunek 66 prezentuje zagregowane dane.



Rysunek 66. Zagregowane odpowiedzi respondentów wskazujące, na dwa różne wskazania
Źródło: Opracowanie własne na podstawie badań ankietowych

W PR 7 i PR 8 zauważany jest wysoki odsetek respondentów niewiedzących, jaką odpowiedz wybrać. Stan świadomości personelu, które te odpowiedzi pokazują niepokoi, gdyż to właśnie na takich szkoleniach pracownicy nabywają umiejętności odpowiedzialnego przetwarzania, przechowywania danych informacji.

Zatem edukowanie podczas szkoleń jest niezbędnym elementem wpływającym na utrzymanie odpowiedniego poziomu ochrony informacji, a zaznajomienie personelu z potencjalnymi zagrożeniami przygotowuje personel na umiejętne postępowanie z pojawiającym się zagrożeniem.

METRYCZKA

Badania miały na celu wytypowanie grupy osób ze względu na wykształcenie, zajmowane stanowisko oraz staż pracy.

Struktura badanych pod względem wykształcenia jest zróżnicowana, od 32% które posiadają wykształcenie magisterskie wyższe, po 34% o wykształceniu wyższym licencjackim i 29% badanych o wykształceniu średnim. Należy zauważyć też, że 5% ankietowanych nabyło tylko wykształcenie zawodowe.

Badani respondenci w liczbie 60% to personel nie kierowniczy tzw. pracownicy wykonawczy. 19% ankietowanych stanowią pracownicy niższego szczebla, a 21% należy do pracowników wyższego szczebla.

Struktura grupy respondentów pod względem stażu pracy jest mocno zróżnicowana: 9% badanych to osoby zatrudnione w jednostce gospodarczej do 1 roku, 30% jest zatrudnionych w okresie od 1do 3 lat. Kolejną grupę badanych respondentów zajmują ci, którzy pracują od 3-5 lat (25%) oraz 15% to badani zatrudnieni w okresie od 5-10 lat. Natomiast osób, które są zatrudnione powyżej 10 lat jest 15%.

Wobec powyższego stwierdza się silne zróżnicowanie zatrudnionych pod względem stażu pracy.

4.2. Omówienie wyników z przeprowadzonej obserwacji oraz wywiadu

Aby zrealizować zamierzony cel pracy oraz ostatecznie potwierdzić przyjętą hipotezę posłużono się obserwacją naukową (nieuczestniczącą), wywiadem swobodnym, jako metodami badawczymi.

Badania ankietowe były pierwszym etapem zdiagnozowania istniejących stanów niezgodności w zakresie ochrony informacji, występujących w organizacjach.

Drugim zaś etapem była obserwacja nieuczestnicząca, której celem było zidentyfikowanie nieprawidłowości związanych z bezpieczeństwem informacji wskazując na występowanie nowych zagrożeń. Dzięki użyciu tej metody posłużono się wynikami, które uzyskano w badanych organizacjach, aby doprowadzić do uogólnienia wniosków z obserwacji (załącznik 2). Podczas obserwacji koncentrowano uwagę na zaistnieniu nieprawidłowości dotyczących obszarów zabezpieczeń fizycznych, sprzętowo-programowych, organizacyjnych oraz administracyjnych. Ponadto, podczas obserwacji badano sposób postępowania wszystkich grup pracowników w zakresie przestrzegania PBI oraz innych regulacji wewnętrznych w przedsiębiorstwach. Otrzymane wyniki z kwestionariusza obserwacji korelują ze wstępnymi wynikami badań uzyskanymi z ankietowania.

Przeprowadzona na terenie badanych firm obserwacja pozwoliła na sformułowanie następujących stwierdzeń:

- W 60% organizacjach zauważono podobny stan rzeczy, mianowicie dokumenty swobodnie leżące na biurkach, regałach, mimo iż, w pomieszczeniach widoczne

były szafy przeznaczone do ich przechowywania. Stwierdzono stan sprzyjający łatwemu zagubieniu dokumentów.

- W PR 1 zaobserwowano, że w pomieszczeniach, w których przebywają pracownicy tworzący rysunki, projekty prototypów oraz pokojach księgowych nie ma niszczarek oraz kserokopiarek. Sytuacja taka jest szczególnie niebezpieczna, gdyż pracownicy zmuszeni są do przemieszczania się z dokumentami w celu zrobienia kopii. Zwiększa się wtedy ryzyko przypadkowej utraty lub zgubienia kopii dokumentów. Zjawisko to nie jest jednak powszechne, gdyż w pozostałych 8 organizacjach zauważono niszczarki, więc problem ten ich nie dotyczy.
- Podczas obserwacji stanowiska służby ochrony w recepcji zauważono system telewizji dozorowej. System obejmował kamery z obrazami z różnych ujęć tzn. widokiem na zewnątrz oraz wewnątrz organizacji. Obserwacja potwierdza, że większość firm używa instalacji pożarowej oraz korzysta z systemu alarmowego. Stwierdza się jednak, nieprawidłowości w zakresie instalacji systemów alarmowych, gdyż widać było kable, które powinny być umieszczone pod listwami maskującymi.
- We wszystkich przedsiębiorstwach stwierdzono poprawne oznakowanie drogi ewakuacyjnej oraz czujki alarmu pożarowego, jednak nie zauważono systemu sygnalizacji pożarowej w postaci przycisku alarmującego o pożarze.
- Obserwacja wykazała, iż ekrany komputerowe były ustawione tak, że nie chronią widocznej na nich zawartości. Pomimo, że pracownicy są świadomi stosowania odpowiednich zabezpieczeń podczas pracy przy komputerze to jednak poprzez nieostrożność lub nieuwagę nie przykładają do tego zbyt dużej wagi. Na widocznych ekranach komputerów użytkowników zauważono dużą ilość otwartych plików na pulpicie.
- Stwierdzono, że wyznaczone strefy bezpieczeństwa, w których mogą przebywać tylko uprawnieni pracownicy nie są chronione fizycznymi barierami.
- W 6 organizacjach nie zauważono informacji o wdrożeniu Polityki Bezpieczeństwa Informacji. Aby skutecznie zaimplementować rozwiązania przedstawione w tym dokumencie należy zaznajomić innych z mechanizmami kontroli tam zawartymi. W kolejnych organizacjach zauważono na ścianach informacje o wdrożeniu system z PBI. Do dobrych praktyk należy informowanie pracowników o zasadach i regułach obowiązujących w organizacji.

- W siedmiu organizacjach biura są zabezpieczone przed wejściem osób postronnych dzięki zamykaniu drzwi automatycznie, więc chcąc wejść ponownie należy użyć identyfikatora imiennego w systemie kontroli dostępu. Osoba, która takiego identyfikatora nie posiada nie wejdzie do pomieszczenia. Sytuacja mogłaby się wydawać zadawalająca, jednak w kwestionariuszu ankiety ci sami badani w pyt. 36 w 4 organizacjach zadeklarowali, że można swobodnie przemieszczać się po terenie przedsiębiorstwa.
- W pięciu z dziewięciu przebadanych organizacji zauważono zapisane hasła przy monitorze komputera. Sytuacja taka stanowi łamanie podstawowych zasad bezpieczeństwa. Najlepiej zabezpieczonymi pod tym względem okazały się cztery przedsiębiorstwa, które zastosowały zasady PBI, nie umieszczając nigdzie informacji o swoich hasłach.
- Stwierdzono, iż w 8 organizacjach wejście do budynku jest nadzorowane w należyty sposób, przy pomocy służb ochrony. Jednak nie we wszystkich przedsiębiorstwach służby te należycie legitymują gości. Pracownik przyjmujący gościa schodzi do recepcji, jednak ten sposób przyjmowania interesantów budzi kontrowersje. Mimo zastosowanych zabezpieczeń, możliwe jest wykorzystanie chwili oczekiwania na osobę wprowadzającą i wejście na teren przedsiębiorstwa. Ponadto, nie we wszystkich organizacjach zauważono w recepcji księgę gości (6 przed.), w której dokonywane są wpisy osób zewnętrznych i celu wizyty. Po zaanonsowaniu się można swobodnie poruszać się po terenie przedsiębiorstwa.
- Na parkingach należących do 5 przedsiębiorstw zauważono zabezpieczenie techniczne w postaci szlabanu, który wyposażony został w kamerę, dzięki której monitoruje się numery rejestracyjne samochodów pracowników oraz gości.
- W wielu firmach zauważono drukarkę sieciową na korytarzu, w strefie ogólnodostępnej, gdzie przebywają pracownicy. W związku z powyższym istnieje przypuszczenie, że stanowczo wzrasta zagrożenie podczas wydrukowania dokumentów. Ponadto, możliwe jest przypadkowe zabranie dokumentów przez nieupoważnioną osobę. Istotnym jest również fakt korzystania przez większość pracowników do jednej, ogólnodostępnej drukarki, gdzie zupełnie realnym staje się możliwość zostawienia kopii dokumentu.
- Zaobserwowano, że w recepcji wszystkich organizacji nie umieszczono informacji odnoszącej się do zakazu filmowania oraz nagrywania i robienia

zdjęć. W strefach ochronnych wymaga się, aby taka informacja została umieszczona.

- Obserwując oznaczenia pomieszczenia serwerowni zauważono w 2 organizacjach takie oznaczenie. Z kolei w dwóch innych zaobserwowano, że pomieszczenia serwerowni znajdują się tuż przy wejściu do przedsiębiorstwa. Stanowi to realne zagrożenie, gdyż mogą mieć do niego dostęp inni pracownicy. Usytuowanie serwerowni w organizacji jest sprawą niezwykle ważną. W pomieszczeniach serwerowni przechowuje się głównie komputery w oparciu, o które firma prowadzi swą działalność gospodarczą. Takie miejsca, więc nie powinny być oznaczone i nie powinny „rzucać się w oczy" osobom postronnym. Zaleca się odpowiednie zabezpieczenie takich obszarów ze względu na wartość danych tam przechowywanych. W samej serwerowni w środku zaobserwowano wentylatory odprowadzające ciepło i czujki dymu systemu przeciwpożarowego (czujki dymu zależą od konfiguracji pomieszczeń i kluczowych punktów, które zabezpieczają) oraz drzwi wyposażone w zamek magnetyczny. Nie zauważono jednak przycisku pożarowego, niezbędnego podczas alarmowania o rozprzestrzeniającym się pożarze. Serwerownia powinna być zabezpieczona czujkami automatycznymi, które uruchamiają się, gdy np. wzrasta temperatura. Z obserwacji wynika, iż serwerownia mieści się zazwyczaj tam gdzie jest siedziba firmy. Taki stan zaobserwowano w 9 przypadkach. Zbudowany system przeciwpożarowy jest sprawdzonym systemem zabezpieczającym organizacje przed zniszczeniem i utratą danych.

Podsumowując spostrzeżenia można powiedzieć, że zapewnienie wysokiego poziomu bezpieczeństwa informacji nie należy do łatwych rozwiązań i jest procesem ciągłym, a nie jednorazowym. Wiąże się to nieodłącznie z wdrażaniem coraz to nowych zabezpieczeń, adekwatnych do pojawiających się niezidentyfikowanych dotychczas zagrożeń. Ponadto, badania pokazały, że należy stale sprawdzać skuteczność i efektywność tych już zaimplementowanych rozwiązań naprawczych.

Podczas pobytu w jednej z organizacji uwagę obserwatora przykuła sytuacja, przygotowania herbaty w kantynie, gdzie można było zobaczyć dokumenty w rękach pracowników. Co prawda nie wiadomo, jakie zawierały one informacje jednak pracownik nieupoważniony może zwrócić na nie uwagę i je zabrać.

Do dobrych praktyk należy opróżnianie kosza z dokumentów noszących znamiona informacji. Takie dokumenty powinny podlegać od razu zniszczeniu

w niszczarce. Jednak nie zauważono tego w 70% organizacji. Wskazuje to na marginalne postępowanie.

Kolejnym elementem badań było sprawdzenie poprzez technikę badawczą wywiadu, w jaki sposób postrzega się w organizacji PBI oraz jak w rzeczywistości wprowadzone, są zawarte w niej zasady i reguły. Uczyniono to w oparciu o narzędzie, jakim jest, kwestionariusz wywiadu, gdzie celowo przyglądano się zjawiskom występującym w przedsiębiorstwach.

Na podstawie przeprowadzonego wywiadu w organizacjach sformułowano następujące wnioski:

- Badane jednostki doświadczyły wielokrotnie ataków socjotechnicznych. Narażeni na takie ataki byli pracownicy organizacji, przedstawiciele organizacji, przedstawiciele handlowi, którzy spotykają się z innymi partnerami tej samej branży (np. na targach motoryzacyjnych).
- Świadomość zagrożeń socjotechnicznych powinna się kształtować u pracowników podczas ich edukowania. Jednak, brakuje innowacyjnych szkoleń obejmujących metody, techniki wyłudzania informacji, na jakie są narażeni pracownicy organizacji.
- W badanych jednostkach pracownicy nie zawsze reagują na widok nieznanej osoby spoza firmy. Świadczy to o braku przygotowania kadry zarządzającej do nowych sytuacji, w których mogą się znaleźć pracownicy. Pracownicy nie, są odpowiednio przeszkoleni, jak zachować się w sytuacjach z nieznajomymi osobami. Wskazuje to na brak zachowania należytej ostrożności podczas obecności osoby trzeciej, na terenie organizacji.
- Sytuacje typu zagubienia telefonu komórkowego czy identyfikatora miały wcześniej miejsce. Laptopy też zgubiono, choć warto dodać, iż były one zaszyfrowane. Natomiast z telefonów czy tabletów możliwe jest wyczyszczenie informacji na odległość, poprzez wcześniejsze zainstalowanie oprogramowania szpiegowskiego. Brak zainstalowania oprogramowania antywirusowego na urządzeniach przenośnych sprzyja powstaniu podatności ujawnienia informacji.
- W organizacjach nie sprawdza się przy pomocy ewidencji czasu pracy, ile czasu dany pracownik spędzał w danym systemie informatycznym. Jeśli użytkownik zbyt długo korzysta z takiego systemu generuje to źródło zagrożeń, dlatego warto kontrolować i nadzorować czas potrzebny na wykonywanie zadań w systemie.

❖ Weryfikując odpowiedzi na zadane pytanie, czy istnieje potrzeba dalszych szkoleń kadry pracowniczej w obszarze bezpieczeństwa informacji, otrzymano od kierownictwa odpowiedź pozytywną. Jednak od razu wskazano, na problem braku środków na takie cele oraz niedostateczną ilości czasu, na takie szkolenia.

❖ Działania podejmowane w ramach kontroli nad upoważnieniami do przetwarzania informacji, okazują się być nieaktualizowane. Pokazała to sytuacja osoby zwolnionej przed dwoma laty. Były pracownik zdał sprzęt komputerowy, ale hasło i login zatrzymał, dzięki czemu przez cały czas miał dostęp do poczty elektronicznej. Stosowym wydaje się zadać pytanie, czy w organizacji jest osoba odpowiedzialna za uaktualnianie uprawnień? w przedsiębiorstwach zauważa się, że jest taka osoba.

❖ Zmiany poaudytowe w obszarze ochrony osobowej dotyczą wprowadzenia przepisów Rozporządzenia RODO. Jednak zauważono, że zmiany powinny być wprowadzone w innych obszarach funkcjonowania przedsiębiorstw typu: kadrowy, księgowy, techniczno-organizacyjny, administracji, czy marketingu. Okazało się jednak, że organizacje nie nadążają za zmianami w wyniku ograniczenia czasu i środków przeznaczanych na takie cele i z wprowadzania części zaleceń rezygnują. Dotyczy to również zaleceń poaudytowych.

❖ Pracownicy znają zasady korzystania z Internetu w godzinach pracy, jednak nie wszyscy respondenci się do tego stosują, korzystając z niego w celach prywatnych. Ponadto, z rozmowy z grupą pracowników można wyciągnąć wniosek, iż korzystali z portali społecznościowych w celach niezwiązanych z realizacją zadań i obowiązków pracowniczych.

❖ W procesie pozbywania się zużytego sprzętu, pracownicy stosują się do zasad wcześniejszego usuwania zapisów na dyskach. W organizacjach istnieje zakaz przechowywania danych na dyskach lokalnych. Utylizacja sprzętu odbywa się najczęściej na podstawie podpisanych umów z firmami zewnętrznymi. Zajmują się one likwidacją lub dalszą odsprzedażą takich urządzeń. Jest to tożsame z odpowiedziami na pytanie ankietowe nr. 15 z kwestionariusza ankiety, gdzie 39% przebadanych wskazało na utylizację sprzętu za pomocą firmy zewnętrznej, ale jednak zdecydowana większość przedsiębiorstw samodzielnie, sama utylizuje zużyty sprzęt, na co również wskazuje pyt.15 tej samej ankiety. Przeglądając umowy o pracę można było znaleźć informację o potrzebie dbałości o mienie firmy i użytkowanie urządzeń zgodne z ich przeznaczeniem. Można, zatem stwierdzić, że problem utylizacji jest poprawnie rozwiązany.

❖ Poprawnie przeprowadzona analiza ryzyka znacząco wpływa na utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa informacji w jednostkach organizacyjnych. Natomiast jej regularność jest pomocna w identyfikowaniu coraz to nowo powstających zagrożeń, w wyniku, czego można na bieżąco redukować ryzyko. Można jednak odnieść wrażenie, że organizacje mają problem z regularnością dokonywania analizy ryzyka i same nie wiedzą, jak często powinno się ją przeprowadzać. Badania ankietowe pokazały, że jedynie 17,1% przebadanych posiada wiedzę, iż analizę ryzyka należy przeprowadzić raz w roku.

❖ Pracownicy zatrudnieni w organizacjach zdają sobie sprawę z wpływu silnego hasła na poziom wysokiego zabezpieczenia systemu. Dlatego też pytając z ilu znaków składa się Państwa hasło uzyskano odpowiedź od 8 do 10 znaków, dużej i małej litery. Ponadto, system informatyczny, z którego korzystają przedsiębiorstwa wymusza zmianę hasła, nie dłużej niż jeden miesiąc.

❖ Pracownicy uwierzytelniają dostęp do systemu komputerowego dwu poziomowo tzn. loginem i hasłem. W praktyce, w działach finansowo-księgowych dokonując przelewu, nadzoruje transakcję inna osoba, sprawdzająca poprawność wykonanego zadania. Uwierzytelnieniem jest numer karty. Jest to stan zadawalający.

❖ W organizacjach korzysta się z mechanizmu, automatycznego blokowania dostępu do systemu, jeśli dłużej nie korzysta się z systemu.

❖ Na ogół korzysta się z procedur PBI związanych z incydentami naruszeń bezpieczeństwa informacji, jednak nie we wszystkich obszarach organizacji. Zarząd tłumaczy to brakiem funduszy na ten cel we wszystkich obszarach przedsiębiorstwa.

❖ Sprzęt komputerowy jest dobrze zabezpieczony. Natomiast telefonów i tabletów nie zabezpiecza się specjalistycznym oprogramowaniem. Wszyscy pracownicy korzystający z komputerów zobligowani są do wysyłania zaszyfrowanych wiadomości do swoich klientów.

❖ Procedury postępowania w kierunku działań naprawczych dotyczących lepszej ochrony zasobów i informacji tam zawartych są trudne do zrealizowania. W sześciu przedsiębiorstwach PBI jest napisana skomplikowanym językiem i niezbyt przejrzyście oraz jest niezrozumiała dla pracowników, którzy są odpowiedzialni za wdrożenie zmian. Stwierdza się brak przejrzystości tego dokumentu.

❖ Trzy z wymienionych zabezpieczeń tzn.: zakaz nagrywania i fotografowania, wejście tylko upoważnionych osób oraz kontrola dostępu są stosowane w obszarach chronionych badanych organizacji. Nie zauważono jednak, aby pracownicy stosowali

się do zakazu używania telefonów komórkowych. Należy podkreślić, że brak procedur określających korzystanie w czasie pracy z prywatnych telefonów, zwiększa podatność pojawienia się zagrożenia, np. poprzez złamanie nakazu i zrobienie zdjęcia rysunkowi technologii prototypów czy karcie technologicznej produktu. Odpowiedzi badanych są zbieżne, z tymi w pyt. 26 kwestionariusza ankiety.

- W organizacjach jest zabronione pożyczanie kart dostępu do określonych systemów informatycznych. Jednak wywiad dowiódł, że takie sytuacje mają miejsce.
- Podmioty zewnętrzne mają nadawane uprawnienia do określonych obszarów systemów informatycznych, np. do katalogów cen produktów, na podstawie wcześniej zawartych umów. Korespondencja z partnerami jest prowadzona poprzez szyfrowanie wiadomości, natomiast dla partnerów biznesowych wyższej rangi dedykowane są specjalne łącza.
- Pracownikom zwalnianym odbierane są wszelkie uprawnienia. W rejestrze odnotowuje się zwroty powierzonego sprzętu firmowego oraz kluczy, natychmiast po ustaniu stosunku pracy i podpisaniu należytych dokumentów.
- Zdaniem kierowników często zdarzają się awarie dotyczące zabezpieczeń systemu komputerowego w wyniku, którego utracono dane. W ostatnim roku najwięcej, bo 4 przypadki zdarzyły się w 2 organizacjach. W innych z kolei taka awaria zdarzyła się raz w roku (4 organizacje). W pozostałych 3 przed. miało to miejsce raz na dwa lata. Dotyczy to różnych obszarów organizacji, np. w ostatnim czasie awaria spowodowana była wyeksploatowaniem urządzenia w wyniku, którego informacja została ujawniona.
- W organizacjach nie dysponuje się dyskami twardymi, gdyż wszystkie operacje są zapisywane w chmurach obliczeniowych. Jednak nadal siedem przedsiębiorstw, daje możliwość korzystania z pamięci zewnętrznych. Wywiad potwierdził analizę badań ankietowych wyrażoną w pyt.33, gdzie aż 55% ogółu w czasie pracy może korzystać z pamięci flash, pendrive. Przyzwolenia na dopuszczenie do używania prywatnych nośników pamięci jest niedopuszczalnym zjawiskiem i zawsze będzie generować zagrożenia ujawnienia informacji, która przecież powinna być w należyty sposób zabezpieczona.
- W organizacjach za wybór określonych zabezpieczeń odpowiedzialny, jest zarząd organizacji. Rządzący unikają ryzyka, ale jeśli się ono pojawi, to starają się sprowadzić go do minimalnego tzw. akceptowalnego poziomu lub też przenosi się go na innego procesora. W przypadku poniesienia dużych nakładów finansowych na ochronę informacji, zarząd podejmuje decyzje, czy jest to ekonomicznie adekwatne do wartości

aktywu. Takie podejście wpływa na kontrolowanie ryzyka utraty bezpieczeństwa informacji i pomaga w utrzymaniu zadawalającego stanu.

❖ W badanych organizacjach zostały przeprowadzone szkolenia dotyczące korzystania z systemów informatycznych oraz urządzeń współpracujących z komputerami. Szkolenia te są dedykowane uczestnikom pracującym w działach, w których przetwarza się informację. Natomiast inne osoby współpracujące z organizacją nie są zapraszane na takie szkolenia (stażyści, partnerzy, praktykanci). Zauważa się problem w doborze uczestników szkoleń z zakresu bezpieczeństwa informacji. Z treścią szkoleń powinni być zaznajomieni wszyscy pracownicy, od zarządzających, aż po szeregowych. Co prawda personel posiada wiedzę z zakresu skutecznej ochrony informacji oraz wie jak zachowywać się w warunkach zagrażających ujawnieniu kluczowych informacji, to jednak nie należy na tym poprzestawać i prowadzić działania ukierunkowane na systematycznym rezerwowaniu środków na dalsze edukowanie załogi pracowniczej. Bowiem, grupując wyniki badań ankietowych w dalszym ciągu pozostaje 15,2% respondentów, którzy nie wiedzą, jak ustosunkować się do szkoleń, nie mając zdania na ten temat. Uważają to za bardzo mało ważne lub mało ważne (pyt.38 z kwestionariusza ankiety). Nie uczestniczenie w tego typu programach szkoleniowych prowadzi do popełnienia błędu, który jest najpowszechniejszym zagrożeniem dla aktywów organizacji, a pomyłki oznaczają konsekwencje zarówno pieniężne, jak i wizerunkowe dla jednostki gospodarczej.

❖ Kolejną kwestią problemową jest fakt, iż w 6 organizacjach nie została wyznaczona osoba odpowiedzialna za zarządzanie ryzykiem. Podobna opinia została wyrażona w pytaniu ankietowym (pyt.23), gdzie najczęściej wskazywano na Inspektora Ochrony Danych Osobowych, jako osobę odpowiedzialną za wprowadzenie zasad doskonalących SZBI. Jednak do obowiązków IODO takie działania nie należą. To zarząd oraz kierownictwo zarządzające, są odpowiedzialni za wprowadzanie zmian i redukcję ryzyka. W tym też celu tworzy się miejsce pracy dla osoby odpowiedzialnej za zmniejszenie ryzyka. Ponadto, w analizowanych przypadkach stwierdza się brak wiedzy przebadanych na temat potrzeby stworzenia stanowiska dla odpowiednio kompetentnej i wykfalifikowanej osoby. Jej brak powoduje zachwianie kontroli nad ciągłym minimalizowaniem ryzyka.

❖ Działania podejmowane w ramach zabezpieczeń w postaci umów z kontrahentami są w pełni zabezpieczone klauzulą o zachowaniu poufności. Jednak, biorąc pod uwagę opinię respondentów na podstawie pyt.11 z kwestionariusza ankiety

okazuje się, że nie ze wszystkimi taka umowa została podpisana (deklarację podpisania poufności wskazało ogółem tylko 62,7% przebadanych). Brak poczucia odpowiedzialności za przetwarzane, przechowywane informacje doprowadza do ujawnienia ich. Ponadto, jeśli firmy konkurencyjne będą zaznajomione z tajemnicą przedsiębiorstwa będą miały nad nią przewagę. Przedsiębiorstwo musi mieć absolutną pewność, że nie zostanie ujawniona informacja zawarta w umowach.

- Tylko w połowie organizacji istnieje procedura zastępstw (50%). Należy, więc wprowadzić zasady proceduralne, podczas przydzielania i organizowania zastępstw za nieobecnego tak, by uniknąć przypadkowych osób nieznających specyfiki pracy oraz obowiązujących reguł na określonym stanowisku pracy.

4.3. Uogólnione wnioski przeprowadzonej analizy stanu faktycznego poziomu bezpieczeństwa informacji w badanych organizacjach

Ze względu na wartość, jaką można przypisać każdej informacji, jest ona uważana za jeden z najważniejszych aktywów, decydujący w biznesie o zaufaniu potencjalnych kontrahentów, partnerów czy po prostu interesariuszy. Dlatego też przedsiębiorstwa są żywo zainteresowane nie ujawnieniem jej i nie udostępnieniem na zewnątrz. Jednak, aby do tego nie doszło należy odpowiednio zarządzać informacją, poznać jak i gdzie powstaje i chronić ją poprzez sprawdzone skuteczne zabezpieczenia przed potencjalnymi sytuacjami, które mogą wywołać zagrożenie jej utraty.

Pozostałe konkluzje, które wynikają z przeprowadzonych badań zostały po krótce przedstawione poniżej.

- Badania wykazały grupy ankietowanych, którzy nie zawierają w umowach klauzuli dotyczących zachowania poufności informacji. 33,5% badanych z wszystkich organizacjach, wstrzymały się od udzielenia merytorycznej odpowiedzi, wybierając po prostu odpowiedz *„nie mam zdania”* (pyt.11 z kwestionariusza ankiety). Zarządy tych organizacji nie mają świadomości i poczucia zagrożenia, albo nie widzą potrzeby dodatkowego zapisu, który zdecydowanie podniósłby poziom bezpieczeństwa przechowywanej informacji podczas zawierania umów z partnerami biznesowymi. Osoby odpowiedzialne za przygotowanie dokumentów powinny być świadome, że takie zapisy powinny się znajdować w umowach. Warto ten temat poruszyć w programach

przygotowawczych pracowników do pracy, uczulając o konsekwencjach nie przestrzegania zasad poufności informacji.

❖ Nie zauważono wypracowanego jednolitego zdania w temacie uwzględniania w organizacjach zasad bezpiecznego przechowywania informacji zawartych w rozporządzeniach, czy też aktach normatywnych. Jedynie 27% deklaruje wykorzystanie bądź gotowość wykorzystania norm w organizacji (pyt.10 z kwestionariusza ankiety). A przecież w standardach normatywnych zaprezentowane są wskazówki dotyczące budowania i utrzymania systemu zarządzania bezpieczeństwem informacji w sposób całościowy i systemowy, który jest dedykowany typowo organizacjom. Przedstawione wzorce postępowań bezpieczeństwa informacji można zastosować w przedsiębiorstwach o różnego rodzaju, wielkości oraz specyfice.

❖ Analizując kompetencje osób zarządzających, zajmujących stanowiska kierownicze stwierdza się, iż nieodzowną częścią zarządzania poszczególnymi działami jest ciągłe podnoszenie kwalifikacji podczas szkoleń związanych z bezpieczeństwem informacji. Patrząc na otrzymane wyniki stanu faktycznego poziomu bezpieczeństwa informacji w przedsiębiorstwach nasuwa się sugestia, że 15,2 % badanych uznała to za bardzo mało ważne lub mało ważne lub też nie miała zadnia w tej sprawie i nie uznaje potrzeby dalszego zdobywania wiedzy w stopniu ważnym i bardzo ważnym (pyt.38 z kwestionariusza ankiety). Należy być świadomym, iż sytuacje niedostatecznej wiedzy pracowników będą tylko pogłębiać zdarzenia związane z naruszeniami, co przedsiębiorstwom przysporzy tylko dodatkowych sytuacji problemowych.

❖ Badania wskazały, że pracownicy w przedsiębiorstwach są niedoszkoleni, ponadto niekompetentni w zakresie stosowania metod oraz technik zapewniających pożądane atrybuty bezpieczeństwa informacji w organizacji. Wdrażając SZBI to zadaniem zarządu jest uświadamianie pracowników, co do obowiązujących reguł i zasad postępowania wobec powstających zagrożeń. Nie wprowadzono nowego planu szkoleń obejmującego tematy, z którymi bezpośrednio stykają się pracownicy. Sposób przedstawienia tematów nie przykuwa uwagi i nie jest praktyczny. Omawiając zagadnienia związane z bezpieczeństwem informacji brak jest pomocy w zrozumieniu przez personel, jak omawiany materiał może wpłynąć na podejmowane przez nich dalsze decyzje oraz jak mogą wykorzystać praktycznie to, czego się dowiedzieli.

❖ Przedsiębiorstwa nie przywiązują należytej wagi do przeprowadzania szkoleń z zakresu zachowania BI, w szczególności dla: pracowników tymczasowych, stażystów, praktykantów, zespołu sprzątającego oraz firm ochraniających przedsiębiorstwo. W

planach finansowych zawsze powinny znaleźć się środki na programy szkoleniowe (pyt.6 kwestionariusza wywiadu). Nie odpowiednio dobrze dobrana grupa docelowa na programy szkoleń powoduje brak świadomości wśród pracowników.

- Badanie wskazało też na potrzebę kontrolowania czasu, który pracownik spędza w danym systemie (pyt.5 kwestionariusza wywiadu). Jeśli jest to zbyt długi czas warto skontrolować pracę użytkownika.
- Zagrożeniem są również zaniedbania dotyczące aktualizacji uprawnień. Podczas prowadzenia badań odnotowano, iż osobą odpowiedzialną za nadawanie i odbieranie uprawnień jest administrator danych, czyli zarządzający przedsiębiorstwem w opinii większości (pyt.23 kwestionariusza wywiadu oraz pyt.14 kwestionariusza ankiety). Jednak nie wszyscy tak uważają. Jest grupa osób twierdząca, iż odpowiedzialność tę powinno przypisać się działowi kadr (34%) lub po prostu Inspektorowi Ochrony Danych Osobowych. Wskazuje to na niekompetencje w obszarze ZBI i zaistnienie problemu, jakim jest brak upoważnionej osoby do kontroli nadawanych uprawnień. Można domyślać się, iż część z uprawnień wydaje i odbiera najwyższe kierownictwo, a resztę kontroluje dział kadr. Nie jest to jednak pozytywne zjawisko, gdyż ostatecznie nie wiadomo, komu przypisać odpowiedzialność za niedopełnienie obowiązków.
- Do obszarów, w których w ostatnim czasie wprowadzono zmiany należy głównie ochrona osobowa. Podyktowane jest to wymogiem wprowadzenia w Polsce rozporządzenia RODO, mającego zastosowanie od 25 maja 2018r. Uzupełnieniem tego aktu jest Polska Ustawa o Ochronie Danych Osobowych z dnia 10 maja 2018 roku.

Analizując stan bieżący przedsiębiorstw stwierdzono brak zespołu odpowiedzialnego za wprowadzanie zmian korygujących w celu poprawienia efektywności działań systemu. I choć nie ma idealnych zabezpieczeń, to jednak te już istniejące muszą ciągle być doskonalone, uaktualniane zgodnie z zasadą cyklu Deminga Planuj-Wykonuj-Sprawdzaj –Działaj.

- W większości organizacji stwierdzono, iż pracownicy w czasie pracy korzystają z Internetu w celach prywatnych, niezgodnych z realizacja wypełnienia obowiązków pracowniczych. Dotyczy to prywatnej poczty, portali społecznościowych lub innych stron internetowych. Mimo, iż pracownicy znają zasady korzystania z Internetu w czasie pracy, to jednak nie stosują się do nich (pyt.9 z kwestionariusza wywiadu oraz 32 kwestionariusza ankiety). Należy zauważyć, że jeden błąd ludzki może spowodować nie bagatelne straty dla organizacji.

❖ Dokonując analizy badań stwierdza się, że ponad 17,1% przebadanych (pyt.11 kwestionariusza wywiadu oraz pyt.21 kwestionariusza ankiety) jest świadoma działań minimalizujących utratę informacji poprzez dokonywanie regularnej analizy ryzyka. Jednak nie ma w organizacjach osoby odpowiedzialnej za zarządzanie ryzykiem i nadzorowaniem go, powodując jego zmniejszenie. Taka osoba przekazywałaby z kolei wiadomości do zarządu w celu sprowadzenia ryzyka do stanu akceptowalnego. Zdiagnozowano natomiast mnogość obowiązków dedykowanych jednej osobie, w tym i też ograniczanie ryzyka.

❖ Badania ujawniły również mocne zróżnicowanie, opinii na temat częstotliwości przeprowadzania analizy ryzyka (pyt. 20 kwestionariusza ankiety). W części przedsiębiorstw nie wprowadzono zasad przeprowadzania analizy ryzyka raz na rok, mimo iż zalecana jest taka procedura. Wskazuje to na lekceważące podejście kadry zarządzającej. Skoro zarząd nie przykłada do tego zbyt wielkiej wagi to i podobne stanowisko w tej kwestii zajmują pracownicy. Autorka pracy nie zgadza się z opiniami respondentów, którzy są zdania, że analizę ryzyka powinno przeprowadzać raz na kwartał (23,4%), albo raz na pół roku (10,1%).

W ramach wywiadu stwierdzono, iż w 3 organizacjach podczas przeprowadzenia analizy ryzyka niepoprawnie przyjęto metodykę. Ponadto, osoby upoważnione do wykonania tego zadania nie zostały do tego odpowiednio przeszkolone, pod kątem określonych wymagań do odpowiedniego zidentyfikowania zagrożenia oraz właściwego oszacowania skutków występujących zagrożeń. Nieodpowiednio przyjęta metodyka może spowodować nieadekwatne spojrzenie na poziom zagrożenia w organizacji i doprowadzić do złudnego poczucia bezpieczeństwa.

❖ Nie bez znaczenia jest również fakt, nieodpowiedniego przechowywania dokumentów w niektórych organizacjach, co zauważają także sami pracownicy. Stwierdzono, iż w nieodpowiedni sposób postępuje się z dokumentami, pozostawiając je niezabezpieczone na stanowiskach pracy, zamiast chować je w przeznaczonych do tego szafach (17,7% badanych z kwestionariusza ankiety oraz pyt.2 kwestionariusza obserwacji). Takie zaniedbanie organizacyjno-biurowe jest niekorzystne i krytyczne w skutkach i stanowić będzie źródło zagrożenia w zetknięciu np. ze szpiegostwem gospodarczym.

❖ Kadra kierownicza na szczeblu zarządczym powinna mieć świadomość, że w przedsiębiorstwie nie stosuje się zabezpieczeń w postaci urządzeń przeciwdziałających podsłuchowi. Zatem, zarząd organizacji nie może być zupełnie

spokojny, że podczas podejmowania strategicznych decyzji nie zostaną one udostępnione innym osobom.

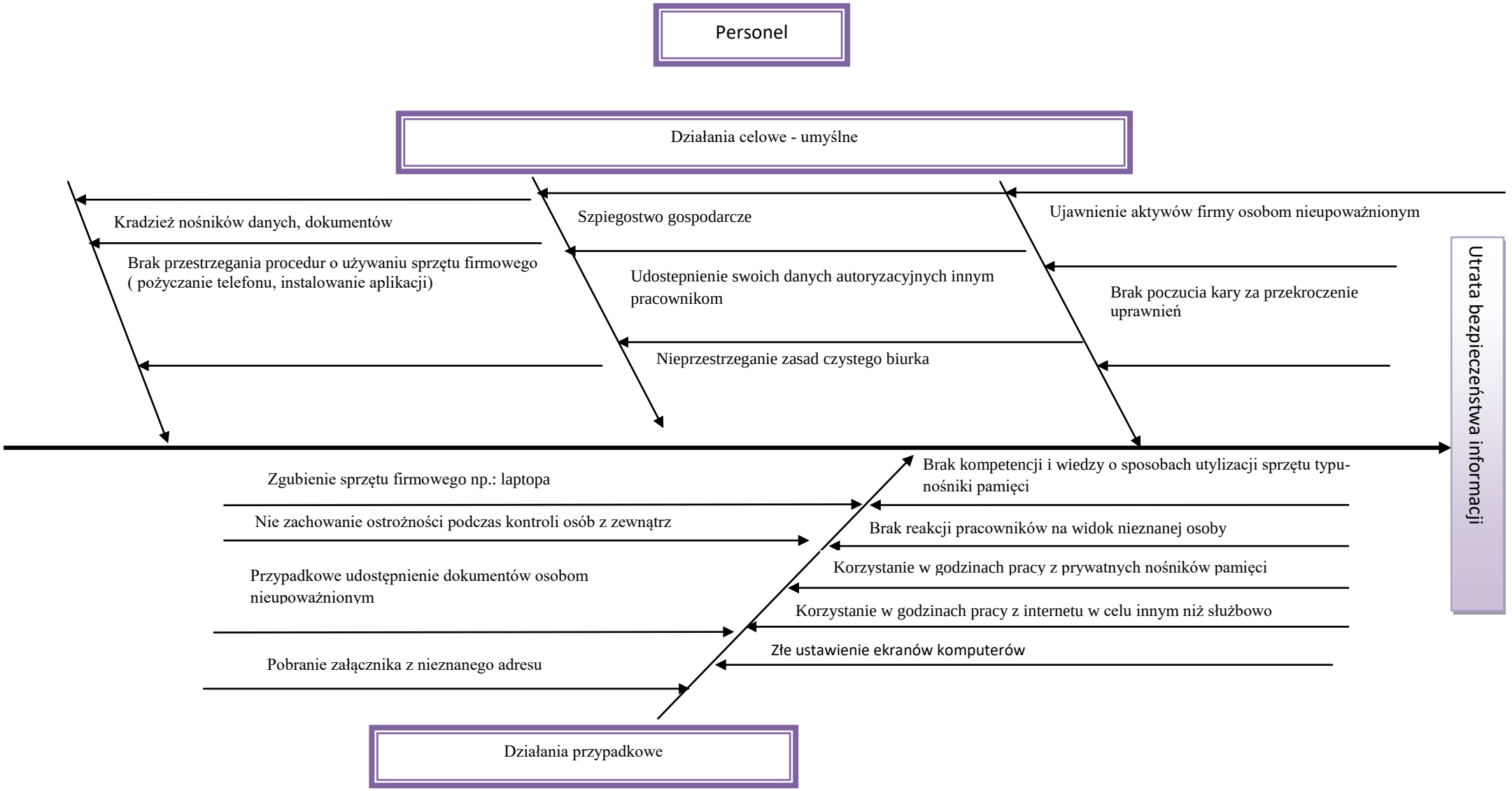
- Ważnym problemem jest również ilość zdarzeń w ciągu roku w wyniku, których mogło dojść do utraty informacji (pyt.4 kwestionariusza ankiety). Dane wskazują, iż przedział od 5 do 10 zdarzeń na rok, wybrało 34 % przebadanych. Pojawienie się tych naruszeń, wskazuje, że system bezpieczeństwa informacji jest niewystarczająco dobrze wprowadzony w obszary organizacji. Ważnym jest, aby skuteczność zabezpieczeń stale kontrolować i dostosowywać ją do coraz to nowych zagrożeń, dotychczas jeszcze niezidentyfikowanych. W wyniku przeprowadzenia analizy ryzyka raz na rok lub też od razu po zidentyfikowaniu zagrożenia organizacja będzie dobierała zabezpieczenia dopasowane do istniejących systemów, ograniczając tym samym ryzyko utraty BI.
- Istotnym zdiagnozowanym problem jest zagubienie sprzętu komputerowego przez personel. Stwierdzono fakt pozostawienia sprzętu służbowego w miejscach publicznych, w prywatnych samochodach czy też w szafkach do przechowywania w sklepie. Co prawda, w organizacjach obowiązuje procedura szyfrowania dysków, jednak stanowi to realne źródło zagrożenia. To właśnie na szkoleniach z odpowiednio dobraną tematyką i grupą odbiorców porusza się tematy sposobu ostrożnego przechowywania służbowych sprzętów komputerowych. Ważnym jest, aby pracownicy wiedzieli, że takie incydenty zazwyczaj kończą się niepożądanymi skutkami, dlatego też nie powinno się dopuszczać do takich sytuacji.
- Zauważa się że aż 12% badanych wyrzuca nośniki pamięci do śmieci. Jest to niepokojące zjawisko. Pracownik niemający doświadczenia może nie świadomie pozostawić zawartości nośnika i go wyrzucić. Brak kontroli nad przestrzeganiem procedur utylizacji nośników informacji sprawia, że nie są one w odpowiednio bezpieczne i nadzorowane. Budzi to realne zagrożenie wystąpienia konsekwencji w postaci utraty informacji.

Zaprezentowany poniżej diagram Ishikawy wskazuje na wytypowane zagrożenia zaistniałe w organizacjach. Na skutek analizy otrzymanych wyników z narzędzi badawczych tj. przeglądu dokumentów, ankietowania, obserwacji oraz wywiadu zidentyfikowano nowe zagrożenia, które w istotny sposób wpływają na poziom bezpieczeństwa organizacji. Takie podejście doprowadziło do zdiagnozowania faktycznego stanu organizacji. Faktem jest, że są organizacje, którym udało się z lepszym skutkiem wdrożyć SZBI w przeciwieństwie do organizacji, które niedomagają pod względem oczekiwanego poziomu BI. Taki obraz sytuacji wskazuje na potrzebę

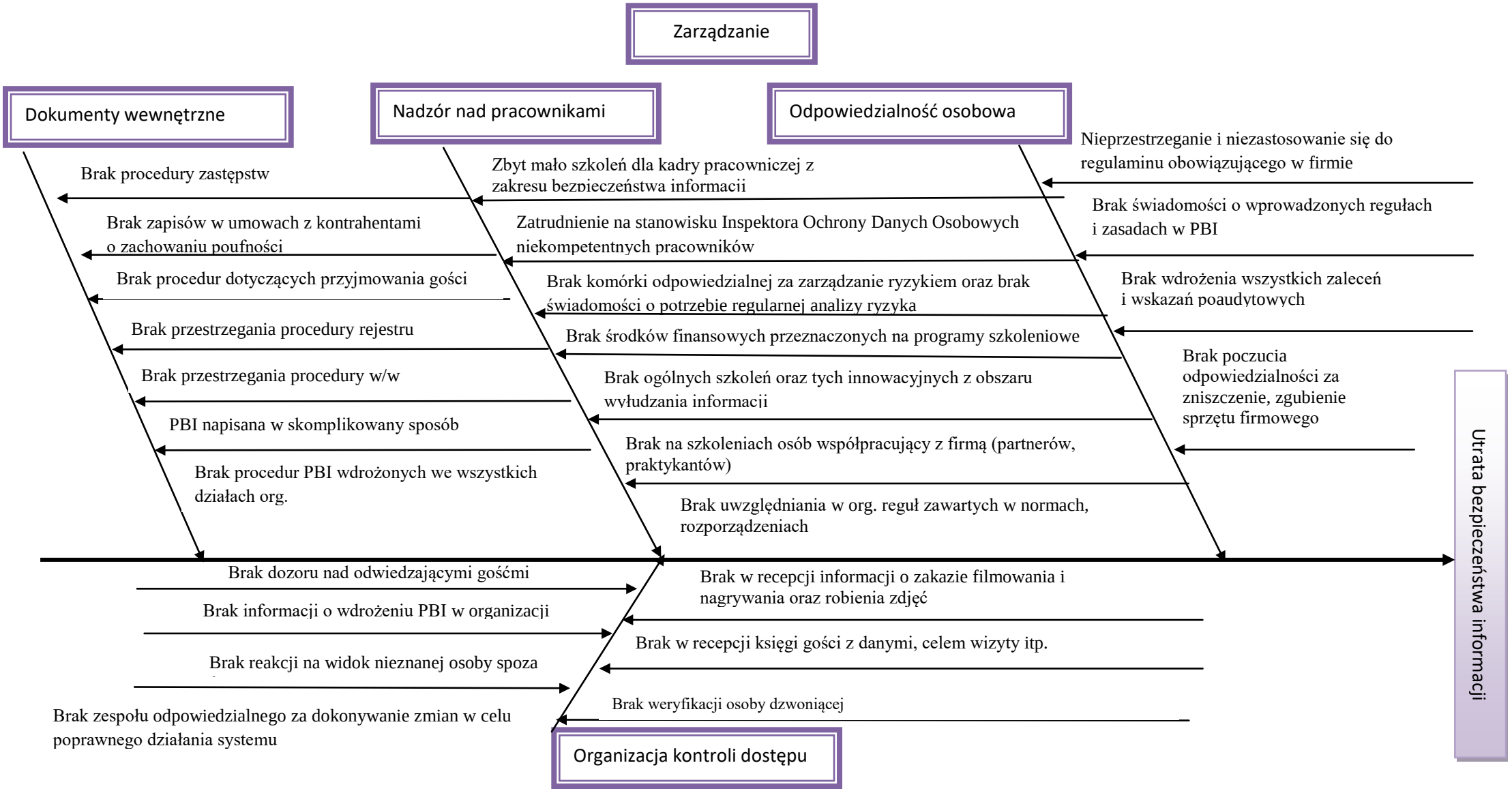
dalszego wprowadzenia i skupienia uwagi czytelnika na czynnikach, które w istotny sposób wpływają na ogólnie rozumiane bezpieczeństwo informacji. Przełoży się to na wskazanie konkretnej pomocy środków ochronno-naprawczych dla tych potrzebujących jej organizacji.

Części diagramu Ishikawy obrazują zjawisko uzyskanych wyników ankietowych, obserwacji i wywiadu, z podziałem na zmodyfikowane gałęzie metody 5M, gdzie wskazano bezpośrednie przyczyny zaistnienia problemu, a później z kolei na ich diagnozę. Do gałęzi tych zaliczono: Personel, Zarządzanie, Systemy Komputerowe, Systemy Bezpieczeństwa, Osoby trzecie, Metoda, starając się zgrupować uzyskane potencjalne zagrożenia wynikłe ze wcześniejszych badań.

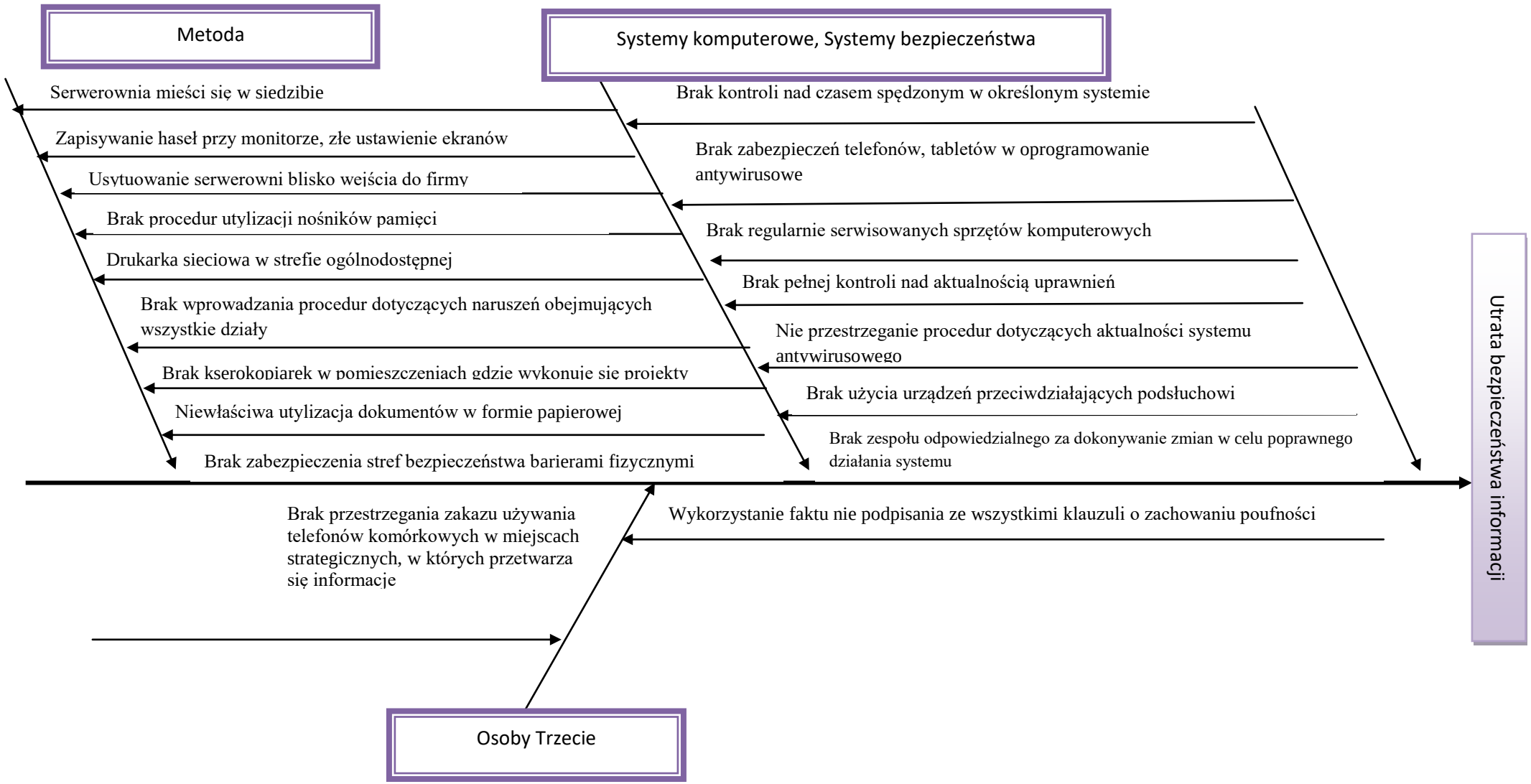
Do każdej z głównych podkategorii przyporządkowano zagrożenia, które w istotny sposób wynikają z głównej przyczyny.



Rysunek 67. Szkielet przyczynowo skutkowy Ishikawy wynikający, z gałęzi Personel
Źródło: Opracowanie własne



Rysunek 68. Szkielet przyczynowo skutkowy Ishikawy wynikający, z grupy zagrożeń zaistniałych, na skutek Zarządzania
Źródło: Opracowanie własne



Rysunek 69. Szkielet przyczynowo skutkowy Ishikawy wynikający, z Systemów komputerowych Systemów bezpieczeństwa, Metody, Osób trzecich oraz Złego Zarządzania Sprzętem *Źródło: Opracowanie własne*

Na szkielecie przyczynowo skutkowym zauważalne jest w niektórych obszarach więcej zagrożeń niż w innych. Główny wpływ na inżynierię bezpieczeństwa mają następujące obszary: Personel, Zarządzanie, Systemy komputerowe i Systemy bezpieczeństwa, Metoda oraz Osoby Trzecie. W przypadku obszaru Personelu diagram wskazał na zagrożenia wynikające z wewnętrza organizacji. Takimi przyczynami celowymi wyłudzenia informacji mogą być m.in.: szpiegostwo gospodarcze, gdzie wykorzystuje się najsłabsze ogniwo, jakim jest człowiek. Motywem działania atakującego włamywacza jest dostanie się do danych kradnąc je w celu przekazania do konkurencji. Brak świadomości pracowników, co do regularności analizy ryzyka, pojawiających się zagrożeń może sprawić, że pracownicy pominą wiele podatności, które ujawniają się jednak nie są dostrzegane. W znacznej mierze przyczynia się do tego stanu brak poczucia kary za przekroczenie uprawnień. Natomiast, jest też wiele działań nieumyślnych pracowników wymienionych na diagramie, które są wynikiem złego zarządzania i nieodpowiedniego nadzoru zarządu nad tym, co się dzieje w organizacji. Ogromne znaczenie ma korzystanie w godzinach pracy z internetu oraz używanie prywatnych nośników pamięci, które zazwyczaj generują zagrożenia. Samo zgubienie sprzętu komputerowego może być często przyczyną ujawnienia zapisanych tam wiadomości, dokumentów wewnętrznych lub sposobu dostania się do samego systemu operacyjnego firmy przez osoby nieuprawnione. W skutek dopuszczenia do takiej sytuacji pracownicy nieświadomie mogą popełnić więcej błędów, niż ci wyszkoleni i dobrze wyedukowani.

Analiza diagramu Ishikawy w kontekście Zarządzania wskazała na wykresie przyczynowo skutkowym potencjalne niebezpieczeństwa i narażające organizacje na utratę BI. Stwierdzono zależność pomiędzy decyzjami zarządu, a postępowaniem pracowników np. tym nieumyślnym lub też celowym. Wygenerowane takim postępowaniem zagrożenia mogą się istotnie zmaterializować i doprowadzić do nieodwracalnych skutków, gdy np. udziela się dostępu osobom nieupoważnionym. Ponadto, brak ewidencji osób uprawnionych do przetwarzania grup informacji powoduje, że przypadkowe osoby w organizacji mają dostęp do poufnych, informacji, co grozi utratą poufności poprzez przekazanie informacji z zasobu nieupoważnionym, postronnym osobom. W ten sposób strategiczne informacje mogą bardzo łatwo zostać udostępnione konkurencji. Na te przyczyny zagrożeń nakłada się brak poczucia odpowiedzialności za popełnione czyny, ponieważ kierownictwo nie reaguje na tego typu sytuacje. Brak nadzoru nad realizacją zasad PBI skutkuje nie przestrzeganiem

wielu przydatnych reguł dotyczących chociażby braku rejestru wejść i wyjść. Taką samą przyczyną ujawnienia informacji może okazać się brak procedury zastępstw, przyjmowania gości lub braku szkoleń. To tylko nieliczne spośród wielu wygenerowanych podatności, które wywołują zagrożenia uwypuklone na diagramie, a sprzyjające urealnieniu się nowych zagrożeń. Brak reakcji zarządzających na tego typu sytuacje, może stanowczo doprowadzić do ujawnienia, zniszczenia, kradzieży strategicznych, poufnych informacji przechowywanych w organizacji.

W obszarze Metody zwrócono m.in. uwagę na: zagrożenie, jakim jest zapisywanie haseł przy ekranie monitora. Jest to czynność niedopuszczalna w organizacji, która chce uchodzić za wiarygodną zaufania organizację, chroniącą swoje aktywa i zasoby. Należy zwrócić również uwagę na niewiedzę pracowników, co do odpowiedniego sposobu utylizowania nośników pamięci. Brak takiej wiedzy może być źródłem wyrzucenia nośnika pamięci do śmieci, a to z kolei stanowiłoby dla organizacji utratę wiarygodności. Innym ważnym zagrożeniem z punktu widzenia zabezpieczeń fizycznych jest umiejscowienie samej serwerowni w pobliżu wejścia/wyjścia, co również sprzyja łatwemu i szybkiemu wejściu intruza. Ponadto, w organizacjach gospodarczych nie wprowadzono procedur operacyjnych dotyczących naruszeń w poszczególnych działach. W związku z powyższym, brak jest pełnego nadzoru nad liczbą naruszeń oraz pojawienia się zagrożeń i ryzyka. Należy nie dopuszczać do takich sytuacji.

Kolejno, w kontekście Systemów komputerowych i Systemów bezpieczeństwa ważne są te podatności, które mogą zostać wykorzystane w wyniku braku stosowania zabezpieczeń urządzeń firmowych. Jest to najczęściej spowodowane nieregularnym serwisem sprzętów firmowych. Należy zwrócić również uwagę na dostęp do systemu osób nieuprawnionych oraz brak nadzoru nad uprawnieniami pracowniczymi. Analiza pokazała, że może dojść do takiego zdarzenia, podczas ataku na system informatyczny, ponieważ pracownicy zupełnie nie są świadomi zagrożeń. Poza tym podatność może się urealnić w wyniku braku odpowiednich zabezpieczeń telefonów komórkowych, czy też tabletów firmowych. Dużym problemem jest również brak urządzeń chroniących przed podsłuchem w miejscach, gdzie zarząd podejmuje strategiczne decyzje. Zagrożenia wywołane takim zjawiskiem mogą powodować ujawnienie informacji poprzez czytanie z ruchu ust i monitorowanie sieci.

W obszarze Osób trzecich wskazano głównie na pojawiające się zagrożenia z zewnątrz, gdzie osoby postronne mogą mieć dostęp do informacji lub grupy

informacji, do których nigdy nie powinny mieć takiego dostępu lub też mogą ujawnić dalej wiadomości, gdyż nie podpisały klauzuli o poufności i przekazują dane innym organizacjom w celu stworzenia kontroferty.

Ponadto, obszar niewłaściwego zarządzania sprzętem, jest przyczyną nieuprawnionego udostepnienia danych. Umiejscowienie drukarki w miejscu ogólno-dostępnym np. w holu organizacji może istotnie wpływać na zgubienie ważnego dokumentu podczas robienia kopii.

Za pomocą diagramu Ishikawy, w sposób jakościowy przeprowadzono ocenę ryzyka. Koniecznym jest jednak przeprowadzenie analizy ryzyka w sposób ilościowy, tak by zaznaczyć wielkość ryzyka, jednocześnie pokazując wygenerowanie najważniejszych zagrożeń, mających wpływ na ryzyko utraty bezpieczeństwa informacji.

5. TESTOWANIE POZIOMU BEZPIECZEŃSTWA INFORMACJI W PRZEDSIEBIORSTWIE

5.1. Wprowadzenie do analizy doświadczalnej

Badania ankietowe, obserwacja oraz wywiad ujawniły problemy związane z zapewnieniem odpowiedniego poziomu atrybutów bezpieczeństwa informacji, z którymi zmagają się przedsiębiorstwa. Analiza stanu poziomu BI ujawniła szereg słabości, które w połączeniu z podatnością mogą uaktywniać zagrożenie. Wpływ podatności ma niebagatelne znaczenie na posiadane aktywa organizacji. Mowa tutaj o:

1. danych osobowych (pracowników, kontrahentów, partnerów, wspólników);
2. tajemnicy przedsiębiorstwa (korespondencja handlowa, lista dostawców, klientów, plany przyszłościowe zakładające rozwój firmy, prognozy sprzedażowe, raporty roczne, miesięczne, strategia pracy w organizacji, treść umów z kontrahentami).

Autorka pracy przeprowadziła kolejne badanie, które miało na celu określenie skuteczności aktualnie istniejących zabezpieczeń w organizacjach.

Ważnym jest, bowiem sprawdzenie czy wprowadzone elementy zabezpieczeń skutecznie działają w życiu organizacji oraz czy pracownicy stosują się do wytycznych zawartych w procedurach SZBI oraz PBI.

Pogląd respondentów został przedstawiony w rozdziale 4 i w wyniku analizy otrzymanych wyników zidentyfikowano występujące niezgodności.

Z przeprowadzonych badań w 9 przedsiębiorstwach jasno wynika, iż organizacje przetwarzają grupy informacji chronionych. Stanowią one tajemnicę zawodową, tajemnicę przedsiębiorstwa, dokumentację wewnętrzną, dane osobowe itp. Wskazane grupy informacji odznaczają się podatnością na zagrożenia, dlatego też należy zastanowić się jak je odpowiednio chronić. Warto przy tym zauważyć, że każda grupa informacji jest narażona na zupełnie innego rodzaju zagrożenia, dlatego powinno się dobierać do każdej z nich indywidualne środki zaradcze. 24% ankietowanych wskazało, że posiada dostęp do informacji związanych z tajemnicą przedsiębiorstwa, przetwarzając informacje technologiczne, techniczne, handlowe oraz organizacyjne. Nie odpowiednie skategoryzowanie takich informacji może wyrządzić nieodwracalne

szkody. Ponadto, zauważono, że 18,4% badanych na stanowiskach niekierowniczych oraz niższego szczebla posiada dostęp do tajemnicy zawodowej. Są to grupy informacji dotyczące tajemnicy bankowej, przedsiębiorstwa, handlowej i innych. Taka tajemnica obowiązuje przez czas odbywania stosunku pracy i później do trzech lat od ustania jego stosunku. W interesie zarządu organizacji leży, więc dokonanie odpowiednich i wyraźnych ustaleń, co do ochrony tajemnicy zawodowej. Obowiązkiem kierownictwa jest również określenie tego, jakie znacznie odgrywają poszczególne kategorie informacji w kontekście prowadzonej działalności gospodarczej.

Z tego też względu, podjęto się przeprowadzenia badań polegających na symulacji realistycznego ataku dotyczącego sprawdzenia stosowania przez pracowników procedur zawartych w PBI oraz wykorzystywania przez nich zaimplementowanych już zabezpieczeń.

Celem przeprowadzenia takiego ataku jest sprawdzenie odporności organizacji na różnego typu scenariusze zdarzeń i określone działania w kierunku ujawnienia informacji.

5.2. Przygotowanie do przeprowadzenia doświadczalnej analizy BI

Przedstawienie informacji na temat doświadczenia: teren, osoby biorące udział w badaniu, termin, czynności do wykonania, zebranie wyników i ich ocena.

W oparciu o plan i scenariusz zostanie przeprowadzona eksperymentalna analiza poziomu bezpieczeństwa w przedsiębiorstwie.

W planie doświadczalnej analizy poziomu bezpieczeństwa w przedsiębiorstwie przewidziano:

I. **Temat: Przeciwdziałanie zagrożeniom występującym w organizacji**

Założenia do eksperymentu: Zakłada się przeprowadzenie ataku na określonej grupie pracowników administracyjno-biurowych, którzy posiadają aktualne upoważnienia do przetwarzania informacji i są odpowiedzialni w organizacji za ich ochronę. Istnieje, bowiem przypuszczenie, że pracownicy bagatelizują niektóre zabezpieczenia, w wyniku, czego nieodpowiednio szacują skutki zagrożeń. Takie zachowanie może wpłynąć na obniżenie ogólnego poziomu bezpieczeństwa w przedsiębiorstwie.

II. **Cel eksperymentu:**

Celem eksperymentu będzie zweryfikowanie faktycznego stanu wiedzy pracowników, co do ochrony informacji, w której są posiadaniu. Czy owa świadomość pozwoli im złamać obowiązujące procedury i zasady postępowania?

Zachowanie pracowników decydująco odpowie na pytanie, czy w organizacji wskazane zabezpieczenia odpowiednio zadziałały czy też nie.

III. **Miejsce przeprowadzenia eksperymentu:**

Doświadczenie zostanie przeprowadzone w jednym z 9 przedsiębiorstw motoryzacyjnych zlokalizowanym w Warszawie. Organizacja jest firmą technologiczną specjalizującą się w produkcji komponentów do samochodów elektrycznych i silników spalinowych oraz pomaga w rozwiązywaniu problemów dotyczących emisji spalin i redukcji zużycia paliwa. Firma świadczy szeroki wachlarz części zamiennych po zaawansowane oprogramowanie diagnostyczne. Obsługuje segment pojazdów osobowych i użytkowych na rynku pojazdów rolniczych, morskich i przemysłowych na całym świecie. Główna siedziba organizacji gospodarczej mieści się w Londynie, natomiast w 24 krajach posiada ośrodki techniczne, zakłady produkcyjne. Autorka pracy decydując o badaniu reprezentatywnym, poddała próbie badawczej 26 osób. Należy do nich kadra administracyjno - biurowa.

Po wcześniejszym ustaleniu strategii postępowania i uzyskaniu zgody od zarządu organizacji przystąpiono do przeprowadzenia eksperymentu.

IV. **Zagadnienia do eksperymentu:**

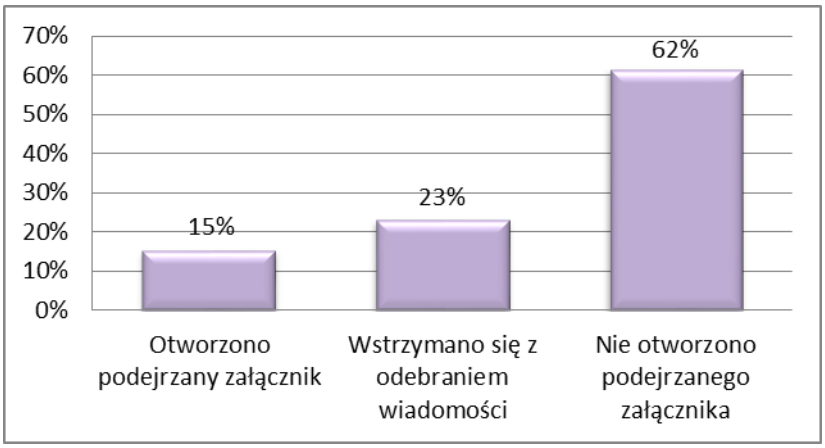
Aby doświadczenie należycie przebiegło przygotowano osiem obszarów, w których, zostaną podjęte działania symulujące atak w celu wydobycia informacji. Należą do nich: przygotowanie wiadomości przeznaczonej do wysłania e-mailem z podejrzanym załącznikiem, próba wejścia na teren przedsiębiorstwa niewylegitymowanym (incognito), próba zrobienia zdjęcia dokumentom leżącym na biurku w przedsiębiorstwie, próba pożyczenia firmowego telefonu komórkowego od kierownika, zasugerowanie zainstalowania ciekawej aplikacji na służbowy telefon kierownika, wydrukowanie dokumentu z pendrive, podejrzenie danych wyświetlonych na monitorze bądź na biurku w wersji papierowej oraz przeprowadzenie ataku telefonicznego w celu pozyskania telefonicznej informacji, co do danych dotyczących przelewu wysłanego przez księgową.

5.3. Wyniki badań z przeprowadzonego eksperymentu

Podjęcie tematu przez autorkę pracy pokazało, na ile system jest odporny i szczelny na symulowane ataki wykrycia informacji.

Diagnoza aktualnego stanu bezpieczeństwa informacji w organizacji ujawniła następująco:

1. Zgodnie z przyjętym planem w pierwszej kolejności przesłano e-mail z załącznikiem z nieznanego adresu. Kryterium oceny podlega czynność pobrania załącznika. I tak się też stało w tym przypadku. Na rys. 70 przedstawiono reakcję osób, które otwarły niniejszy załącznik. Aż 15% pracowników zdecydowała się na otworzenie podejrzanej wiadomości. Jeśli to osoby, które w swojej pracy korzystają systemów informatycznych stanowią realne zagrożenie utraty informacji. Podczas przeprowadzonego badania zaobserwowano zróżnicowane postępowanie wskazujące na otwarcie załącznika znajdującego się w e-mailu.



Rysunek 70. Postępowania pracowników, wobec otwarcia załącznika znajdującego, się w e-mailu
Źródło: Opracowanie własne na podstawie przeprowadzonego eksperymentu

2. W scenariuszu odwiedzin organizacji zaplanowano wejście niezauważonym do środka organizacji. W badaniu ankietowym pracownicy omawianej organizacji zadeklarowali, że służby ochrony monitorują bezpieczeństwo, a goście poruszają się w obecności kogoś trzeciego. Jednak sytuacja w badanym przedsiębiorstwie pokazała, że można wejść niezweryfikowanym przez służby ochrony. Autorce badań udało się również nie wpisywać w rejestr gości. Ponadto, oczekując na kierownika, udało się przejść przez bramki bezpieczeństwa i wejść dalej na teren organizacji, jako osoba postronna, niezauważona przez pracowników i wejść swobodnie nawet na 2 piętro

w jednostce gospodarczej. Procedura kontroli służb ochrony przy wejściu /wyjściu nie jest przestrzegana.

3. Podczas odwiedzin w strefie ochronnej zaplanowano zrobienie zdjęcia lub nagranie filmu dokumentom leżącym na biurku. Autorce udało się zrobić zdjęcie dokumentom leżącym swobodnie na biurku. Warto zaznaczyć, że zrobiono zdjęcie w miejscu, w którym dokumentów nie wolno upubliczniać. Wskazuje to na wyraźny brak reakcji personelu na zaistniały incydent. A przecież ochrona tego typu dokumentów jest obowiązkiem pracowników. Nie zauważono również w pomieszczeniach innych działów, żadnych informacji dotyczących zakazu fotografowania i nagrywania.

4. W ramach eksperymentu pożyczono od kierownika telefon komórkowy. Tym samym zachował się on niezgodnie z obowiązującymi procedurami PBI w zakresie zakazu udostępniania urządzeń firmowych osobom postronnym. Pracownicy nieznający procedur są nieświadomi, że np. szpiedzy przemysłowi atakują, w celu kradzieży lub wyłudzenia danych z organizacji.

5. Doświadczenie ujawniło podejście kierownika do zainstalowania aplikacji na służbowym telefonie. Mimo, iż kierownik odbył szkolenie związane z procedurami użytkowania urządzeń firmowych, to jednak zgodził się na zainstalowanie aplikacji. Nie zachował należytej ostrożności i zlekceważył zasady PBI.

6. Badania pokazały również stosunek pracowników do możliwości wydrukowania dokumentu z pendrive. Stanowisko pracowników było jednoznaczne. Nikt z kierowników nie chciał dokumentu wydrukować, powołując się zasady obowiązujące w organizacji, o zakazie drukowania z obcych nosików pamięci.

7. W ramach doświadczenia postanowiono podejrzeć informacje zawarte w dokumentacji leżącej na biurku. Szczególną uwagę autorki przykuły segregatory, leżące na półkach z napisem „Raporty 2018, 2019". Udało się zrobić zdjęcie w chwili, gdy autorka została sama, na chwilę bez opieki w pomieszczeniu, w którym gdzie przechowuje się dokumentacje. Procedura przechowywania aktywów wskazuje jednoznacznie, na bardzo staranne ich przechowywanie. Można tam znaleźć zapisy odnośnie korzystania z regałów lub szaf zamkniętych w celu ograniczenia dostępu postronnym osobom np. z działu sprzątającego. Na biurku nie mogą leżeć swobodnie dokumenty zawierające ważne dane firmowe. Z kolei komputery użytkowników były zabezpieczone.

8. W wyniku przeprowadzonej rozmowy telefonicznej z księgową, ujawniono osobie niezweryfikowanej tzn. autorce, informacje zwrotną dotyczącą przelewu. Natomiast nie podjęto próby zidentyfikowania instytucji, z której otrzymano połączenie. A przecież zweryfikowanie osoby dzwoniącej pytając o imię, nazwisko, Nip firmy, to oczywistość podczas identyfikacji tożsamości rozmówcy po drugiej stronie. Brak zastosowania się do takiej procedury świadczy o niedopełnieniu obowiązku uwierzytelnienia podmiotu, z którym się współpracuje. Powyższa sytuacja nie napawa optymizmem, ponieważ skutki łamania takich zasad mogą utrudniać prowadzenie działalności gospodarczej.

5.4. Wnioski z przeprowadzonego eksperymentu

Przedsiębiorstwo na podstawie otrzymanych wyników badań, szacując ryzyko i samo decyduje, które informacje z punktu widzenia organizacji są najważniejsze. Decyduje też, gdzie powinny znajdować się aktywa o krytycznym znaczeniu. Mowa tutaj o informacji zapisanej w sposób elektroniczny, jak i przechowywanej w postaci papierowej. Przeprowadzone badania wykazało, że spośród ośmiu zagadnień doświadczalnych, jedynie w jednym przypadku zaobserwowano poprawną reakcję pracowników. Wszystkie inne zdarzenia ujawniły możliwość wyłudzenia, zniszczenia, i modyfikacji informacji.

Badania pozwoliły wyciągnąć następujące spostrzeżenia

- Brak wiedzy kadry pracowniczej, do co zagrożeń wynikających z otwarcia takiego załącznika (mowa o wirusach, makrowirusach, koniach trojańskich, pfishingu, aplikacjach szpiegowskich, złośliwych podzespołach, przechwyceniu transmisji, backdoor, robakach, bakteriach, bombie logicznej DoS i wielu innych przestępczych atakach wykorzystywanych w sieci).
- Przyzwolenie na wejście do środka organizacji niezauważonym oraz niezidentyfikowanym, nie otrzymując przepustki oraz nie wpisując się w rejestr gości jest nie do zaakceptowania.
- Osoby zatrudnione na stanowiskach kierowniczych podatne na manipulacje zrobienia zdjęcia dokumentom.
- Ocenia się, że osoba pożyczająca służbowy telefon, dopuściła się ujawnienia informacji.

- Kierownik zmiany uległ manipulacji socjotechnicznej, instalując aplikację na telefonie służbowym. Jest to bardzo niepokojące zjawisko.
- Przestrzeganie przez pracowników procedury postępowania PBI wobec drukowania dokumentu z pendriva.
- Pracownicy nie przestrzegają zasady należytego przechowywania dokumentów. Zachowanie takie może wynikać z braku świadomości.
- W wyniku braku weryfikacji tożsamości osoby dzwoniącej ujawniono informacje księgową.

Scenariusze potencjalnych wydarzeń odzwierciedlają, na ile system bezpieczeństwa informacji jest odporny na zderzenie z potencjalnym zagrożeniem i wykazują na się dużą słabością w stosunku do podatności.

Według przeprowadzonego doświadczenia pracownicy nie są gotowi na atak socjotechniczny, nie są też edukowani pod kątem umiejętnego manipulowania ludźmi, zmieniającego ich poglądy czy postawę. Zaniedbania te mogą wynikać z nieznajomości katalogu występujących zagrożeń.

Pracownicy zdecydowali się na pobranie załącznika z nieznanego adresu poczty e-mail, ponadto z powodzeniem autorka pracy weszła na teren organizacji niezidentyfikowanym, zrobiła zdjęcie dokumentom, skorzystała z telefonu służbowego kierownika. Oprócz tego zainstalowano na urządzeniu aplikacje, podejrzano informacje zawarte w dokumentach leżące na biurku oraz uzyskano informacje dotyczące przelewu bez weryfikacji osoby dzwoniącej.

Wskazuje to na brak świadomości pracowników wobec ochrony wartości przetwarzanych danych oraz braku znajomości procedur obowiązujących w organizacjach. Po przeprowadzeniu badań ankietowych, obserwacji oraz wywiadu i eksperymentu potwierdza się, że stan w przedsiębiorstwach powinien być zmieniony, gdyż generują się zagrożenia istotne dla utraty atrybutów bezpieczeństwa informacji. Koniecznym jest, zatem przeprowadzenie dalszej dogłębniejszej analizy ryzyka.

6. OCENA POZIOMU BEZPIECZEŃSTWA INFORMACJI WRAZ Z PROJEKTEM ZMNIEJSZAJĄCYM MOŻLIWOŚĆ UTRATY INFORMACJI

Każda organizacja powinna dokonać obiektywnej i rzetelnej oceny w ramach, której stwierdzi, czy przetwarzana informacja jest narażona na ryzyko ujawnienia. Ryzyko należy oszacować obiektywnie oceniając, czy przetwarzana informacja lub grupy informacji są przechowywane w bezpieczny sposób. Ocenę ryzyka należy przeprowadzić dla wszystkich zagrożeń, dynamicznie identyfikowanych przez organizację.

Katalog zagrożeń bezpieczeństwa informacji został ustalony oparciu o przeprowadzone badania dla bezpieczeństwa danych, przedstawionych w kwestionariuszu ankiety, obserwacji i wywiadu. Podczas analizy otrzymanych wyników badań wykazano występowanie zagrożeń w organizacjach. Zagrożenia zostały zidentyfikowane i dobrano do nich zabezpieczenia.

Aby poprawnie przeprowadzić analizę ryzyka niezbędne będzie ustalenie wagi informacji, kwantyfikacji prawdopodobieństwa wystąpienia zagrożenia oraz ustalenie poziomu odziaływania zagrożenia, czyli skutku wpływu zagrożenia. Nie bez znaczenia jest w tym miejscu zidentyfikowanie zagrożeń oraz przypisanie im określonych stosowanych zabezpieczeń. Analiza ryzyka wskaże też poziom skuteczności wykorzystywanej ochrony.

6.1. Ocena poziomu bezpieczeństwa informacji w przedsiębiorstwie

Na początku zapoznano się z posiadanymi przez przedsiębiorstwo zasobami dokonując inwentaryzacji zasobów (informatyczne, techniczne oraz fizyczne zasoby).
Wyniki identyfikacji zasobów przedsiębiorstwa, które powinny podlegać zabezpieczeniu zestawiono w tabeli 12.

Tabela 12. Lista zasobów podlegających zagrożeniom

L.p.	Nazwa zasobu	Opis zasobu
1.	Urządzenia informatyczne służące do przetwarzania danych	Sprzęt używany do przetwarzania danych (stacja robocza, urządzenia współpracujące z komputerem, serwery, drukarki, skanery, tablety, telefony, stacje robocze, elektroniczne nośniki

L.p.	Nazwa zasobu	Opis zasobu
		danych) Wykorzystywane urządzeń do gromadzenia danych, systemy operacyjne
2.	Sieć i przesyłanie danych	Urządzenia do przesyłania danych drogą elektroniczną. Teletransmisja sieci.
3.	Personel	Personel zewnętrzny (np.: usługi firm sprzątających). Personel wewnętrzny - kierownictwo wyższego szczebla oraz niższego szczebla oraz pozostali pracownicy. Wykorzystywanie mechanizmów monitorowania przetwarzanych informacji przez personel. Ogół działań użytkowników dotyczących przetwarzania informacji w przedsiębiorstwie, ich wiedza i doświadczenie
4.	Organizacja	Plany dotyczące ciągłości działania w organizacji. Procedury identyfikowania i szacowania ryzyka. Zapisy odnosząca się do bezpieczeństwa w umowach z klientami. Procedury, nadzór Procedury dotyczące wymiany dokumentów między działami, systemami, podsystemami. Fizyczna ochrona budynków organizacji (okna, drzwi). Fizyczna kontrola dostępu do budynków i pomieszczeń jednostki organizacyjnej.
5.	Dokumentacja	Dokumentacja, w której zawarty jest plan rozwoju organizacji, elementy stosowanej technologii, instrukcje, procedury, projekty. Dokumenty przechowywane w formie papierowej- tradycyjnej. Informacje zapisane na zewnętrznych nośnikach danych, w tym dane osobowe personelu, kontrahentów, bazy danych klientów, zleceniodawców. Sprawozdania finansowe, bilanse, raporty po audytowe, dane w formie papierowej lub elektroniczne.

Katalog zagrożeń bezpieczeństwa informacji powstał w oparciu o przeprowadzone przez autora dysertacji badania obejmujące: ankietowanie, obserwację nieuczestniczącą, wywiad swobodny oraz test odporności na ataki ujawnienia informacji. Stanowi on syntezę otrzymanych wyników badań, a zawarte w nim zagrożenia zostały podzielone wg. zmodyfikowanych kategorii diagramu Ishikawy (tj: metoda, maszyna i technologia, personel, osoby trzecie, zarządzanie).

W tabeli 12 przedstawiono charakterystykę poszczególnych zagrożeń bezpieczeństwa informacji, przyporządkowanych do poszczególnych kategorii diagramu Ishikawy oraz wskazano zasoby, na które one oddziałują.

Częstotliwość ich wystąpienia ocenili badani respondenci w skali 0-5 (gdzie poziomy oznaczają: 1-nie występuje, 2- bardzo rzadko, 3-rzadko, 4-często, 5-bardzo często). Każda organizacja powinna posiadać swój katalog zagrożeń, systematycznie go rozbudowując, o coraz to nowe, dotychczas niezidentyfikowane zagrożenia. Katalog ten powinien być cały czas otwarty i uaktualniany. Również skalę organizacje gospodarcze mogą dowolnie modyfikować pamiętając, że raz ustalona skala powinna obowiązywać już we wszystkich wyliczeniach.

Tabela 13. Lista zagrożeń wybranych z katalogu oraz ich wpływ na wykorzystywane zasoby w organizacji wraz ze wskazaniem skutku wystąpienia

Lp.	Kategorie wg. diagramu Isikawy	Zagrożenie (podatność)/ oznaczenie zagrożenia	Opis/przykład	Zasób
Z.1	**Personel**	Szpiegostwo gospodarcze	Dostęp do danych wynikający z nieuprawnionego dostępu do sieci bezprzewodowej	Urządzenia inf. służące do przetwarzania danych
Z.2	**Personel**	Nieprzestrzeganie i niezastosowanie się do regulaminu obowiązującego w firmie	Używanie sprzętu służbowego w celach prywatnych (laptopów, telefonów) Brak poczucia kary za przekroczenie uprawnień Korzystanie w godzinach pracy z prywatnych nośników pamięci Korzystanie w godzinach pracy niezgodne z zakresem wykonywanych obowiązków Nieprzestrzeganie i niezastosowanie się do regulaminu obowiązującego w firmie Brak świadomości o wprowadzeniu reguł i zasad w PBI. Nieprzestrzeganie zasad czystego biurka	Personel
Z.3	**Personel**	Nieodpowiednie utylizowanie dokumentów papierowych	Nieodpowiednie przechowywanie dokumentów Niewłaściwa utylizacja dokumentów w formie papierowej Ujawnienie aktywów firmy osobom nieupoważnionym Brak przestrzegania procedur używaniu sprzętu służbowego (pożyczanie telefonu, instalowanie aplikacji	Personel
Z.4	**Personel**	Kradzież nośników danych, dokumentów	Brak dostępu do danych ze względu na kradzież urządzeń Zgubienie sprzętu firmowego np.: laptopa	Personel
Z 5	**Personel**	Niewłaściwe korzystanie z poczty e-mailowej	Brak przestrzegania procedur, dotyczących korzystania w czasie pracy z poczty e-mailowej Pobranie załącznika z nieznanego adresu poczty e-mailowej	Personel
Z.6	**Zarządzanie**	Brak utworzonej Polityki Bezpieczeństwa Informacji	Brak stosowania się do reguł i procedur służących ogólnemu stanu bezpieczeństwa w organizacji Brak procedury zastępstw Brak rejestru wejść/wyjść Brak w recepcji księgi dla gości, z danymi uwierzytelniającymi i celem wizyty Brak informacji o wdrożeniu PBI w organizacji PBI napisana w skomplikowany sposób	Personel

			Brak w recepcji informacji o zakazie filmowania i nagrywania oraz robienia zdjęć Brak weryfikacji osoby dzwoniącej	
Z.7	**Zarządzanie**	Brak fizycznej ochrony budynków, drzwi, okien	Niedostatecznie dobra, jakość pracy służb ochrony Brak procedur dotyczących przyjmowania gości Strefy bezpieczeństwa nie są chronione barierami fizycznymi	Dokumentacja
Z.8	**Zarządzanie**	Brak szkoleń dla kadry pracowniczej z zakresu bezpieczeństwa informacji	Brak wiedzy o sposobach utylizacji sprzętu typu nośniki pamięci Brak środków finansowych przeznaczonych na programy szkoleniowe Zbyt mało szkoleń dla kadry pracowniczej dotyczących BI Brak innowacyjnych szkoleń z obszaru wyłudzania informacji Brak na szkoleniach osób współpracujących z firmą Brak poczucia odpowiedzialności za zniszczenie, zgubienie sprzętu firmowego Brak wdrożenia zaleceń po audytowych	Personel Organizacja
Z.9	**Zarządzanie**	Brak reakcji na osoby postronne znajdujące się w budynku	Uzyskanie dostępu do dokumentów poprzez nieostrożność i brak zainteresowania personelu osobami postronnymi Brak dozoru nad odwiedzającymi gośćmi Nie zachowanie ostrożności podczas kontroli osób z zewnątrz Przypadkowe udostepnienie dokumentów	Personel
Z.10	**Zarządzanie**	Brak weryfikacji osoby dzwoniącej	Brak procedury dotyczącej weryfikacji osób dzwoniących z otoczenia organizacji	Personel
Z.11	**Zarządzanie**	Brak w firmie Inspektora Ochrony Danych Osobowych lub zatrudnianie na tym stanowisku niewykwalifikowanych pracowników	Brak zaplanowanego stanowiska w strukturze organizacyjnej dla IODO Zatrudnienie na stanowisku IODO niekompetentnych pracowników Brak komórki odpowiedzialnej za zarządzanie ryzykiem oraz brak świadomości o potrzebie regularnej analizy ryzyka Brak zespołu odpowiedzialnego za dokonywanie zmian w celu poprawy działania systemu	Organizacja
Z.12	**Zarządzanie**	Nieodpowiednie przygotowanie umowy z personelem, kontrahentami i dostawcami	Brak zapisów w umowach z kontrahentami klauzuli o zachowaniu poufności	Personel Dokumentacja
Z.13	**Metoda**	Awaria, utrata zasilania	Uszkodzenie zasobu wynikające z awarii Usytuowanie serwerowni blisko wejścia do firmy	Sieć i przesyłanie danych
Z.14	**Metoda**	Brak mechanizmów monitorowania	Używanie danych firmowych na urządzeniach prywatnych Brak wprowadzania procedur dotyczących naruszeń obejmujących	Personel

			wszystkie działy	
Z.15	**Metoda**	Odtworzenie danych z odnalezionych nośników danych	Brak procedur utylizacji nośników pamięci Przechowywanie danych na urządzeniach niezabezpieczonych i niezaszyfrowanych	Urządzenia inf. służące do przetwarzania danych
Z.16	**Metoda**	Ujawnienie aktywów firmy osobom nieupoważnionym	Użycie nielegalnego oprogramowania do urządzeń Brak weryfikacji pracownika Drukarka sieciowa w strefie ogólno dostępnej Brak kserokopiarek w pomieszczeniach, w których wykonuje się projekty	Sieć i przesyłanie danych
Z.17	**Systemy komputerowe**	Przekroczenie uprawnień poprzez nieuprawniony dostęp do informacji	Brak kontroli nad czasem spędzonym w określonym systemie Brak pełnej kontroli nad aktualnością uprawnień	Personel
Z.18	**Systemy komputerowe**	Podsłuch komputerowy	Dostęp do danych, wynikający z nieuprawnionego dostępu do sieci bezprzewodowej Brak użycia urządzeń przeciwdziałających podsłuchowi	Urządzenia inf. służące do przetwarzania danych
Z.19	**Systemy komputerowe**	Awaria sprzętu komputerowego, ograniczony dostęp do danych	Uniemożliwiony dostęp do danych wynikający z awarii sprzętu Brak regularnie serwisowanych sprzętów komputerowych	Urządzenia inf. służące do przetwarzania danych
Z.20	**Systemy komputerowe**	Nieprawidłowe korzystanie z oprogramowania	Korzystanie z bezpłatnych programów antywirusowych Nie przestrzeganie procedur dot. aktualności systemu antywirusowego	Sieć i przesyłanie danych
Z.21	**Systemy komputerowe**	Włamania do systemu komputerowego, możliwość kradzieży danych	Używanie nielegalnego oprogramowania Brak zabezpieczeń telefonów służbowych, tabletów w oprogramowanie antywirusowe	Urządzenia inf. służące do przetwarzania danych
Z.22	**Osoby trzecie**	Wykorzystanie przez petenta informacji udostępnionych w firmie w celu stworzenia kontroferty	Czytanie, kopiowanie lub fotografowanie dokumentów. Powiązanie fragmentaryczne danych z różnych źródeł informacji	Personel Dokumentacja
Z.23	**Osoby trzecie**	Nieuprawniony dostęp do informacji i jej wykorzystywanie	Nieuprawniony dostęp użytkowników do informacji Wykorzystanie faktu nie podpisania ze wszystkimi klauzuli o zachowaniu poufności. Brak przestrzegania zakazu używania telefonów komórkowych w miejscach strategicznych, w których przetwarza się informacje	Personel Dokumentacja

Po określeniu zasobów w organizacjach oraz wskazaniu pojawienia się zagrożeń koniecznym jest ustalenie, które z wybranych zagrożeń w istotny sposób mogą wpłynąć na ujawnienie, modyfikację uszkodzenie informacji lub też użycie jej w niewłaściwym celu, niezgodnym z jej przeznaczeniem.

Waga znaczenia poufności, integralności oraz dostępności informacji w każdej organizacji będzie przedstawiać się inaczej. Jednak zapewnienie pełnego bezpieczeństwa informacji w przedsiębiorstwie wymaga zagwarantowania wszystkich atrybutów bezpieczeństwa informacji.

Zastosowanie mapowania będzie pomocne w ocenie wdrożonych zabezpieczeń skierowanych na przeciwdziałanie i ochronę zasobów przed zagrożeniami.

Mapowanie będzie niezbędne do określenia w dalszych obliczeniach konkretnej wartości ryzyka.

Procedura mapowania polega na wskazaniu, które z wymienionych zagrożeń istotnie wpływają na utratę poszczególnych atrybuty bezpieczeństwa informacji, tj: poufności, integralności, dostępności, autentyczności i rozliczalności. W wyniku mapowania przyporządkowuje się dla każdego z wymienionych zagrożeń poszczególny atrybut bezpieczeństwa informacji. Kolejnym etapem jest przypisanie dla każdego zagrożenia, atrybutu bezpieczeństwa informacji, wartości liczbowych dla następujących parametrów: zabezpieczenie, prawdopodobieństwo, skutek. Z tego też względu omawiana metoda szacowania ryzyka jest w porównaniu z innymi metodami analizy ryzyka dokładniejsza i bardziej szczegółowa.

Tabela 14. Mapowanie zagrożeń ryzyka powodującego utratę podstawowych atrybutów informacji

Zagrożenia	Poufność	Integralność	Dostę-pność	Nieza-wodność systemu	Autenty-czność systemu	Rozlicza-lność systemu
Szpiegostwo gospodarcze	X	X	X	X	X	X
Nieprzestrzeganie i niezastosowanie się do regulaminu obowiązującego w firmie	X	X	X	X	X	X
Nieodpowiednie utylizowanie dokumentów papierowych	X	X	X			
Kradzież nośników danych, dokumentów	X		X		X	
Niewłaściwe korzystanie z poczty e-mailowej	X	X	X		X	
Brak utworzonej PBI	X	X	X			
Brak fizycznej ochrony budynków, drzwi, okien	X	X	X		X	X
Brak szkoleń dla kadry pracowniczej z zakresu bezpieczeństwa informacji	X	X	X	X	X	X

Zagrożenia	Poufność	Integralność	Dostępność	Niezawodność systemu	Autentyczność systemu	Rozliczalność systemu
Brak reakcji na osoby postronne znajdujące się w budynku	X	X	X		X	
Brak weryfikacji osoby postronnej	X	X	X			
Brak w firmie Inspektora Ochrony Danych Osobowych lub zatrudnianie na tym stanowisku niewykfalifikowanych pracowników	X		X			
Nieodpowiednie przygotowanie umowy z personelem, kontrahentami i dostawcami	X					
Awaria, utrata zasilania		X	X	X		
Brak mechanizmów monitorowania				X		X
Odtworzenie danych z odnalezionych nośników	X				X	
Ujawnienie aktywów firmy osobom nieupoważnionym	X	X				
Przekroczenie uprawnień poprzez nieuprawniony dostęp do informacji	X	X	X		X	X
Podsłuch komputerowy	X		X			
Awaria sprzętu komputerowego			X	X	X	
Nieprawidłowe korzystanie z oprogramowania	X	X	X	X		
Włamania do systemu komputerowego, możliwość kradzieży danych	X	X	X			
Wykorzystanie przez petenta informacji udostępnionych w firmie w celu stworzenia kontroferty	X					
Nieuprawniony dostęp do informacji i jej wykorzystywanie	X	X	X		X	

Do wszystkich zagrożeń przyporządkowano zabezpieczenia wykorzystywane w przedsiębiorstwach tj. fizyczne, techniczne, organizacyjne oraz systemowe. Proponowane zabezpieczenia składają się z różnych jednostkowych, poszczególnych elementów, które stanowią zespół zabezpieczenia ocenianego przez badanych w ankiecie.

Tabela 15. Określenie zabezpieczeń stosowanych w organizacji

L.p. zagrożenia	Zabezpieczenia	Opis
ZAG.1	Procedura korzystania z internetu Informowanie przez służby ochrony o podejrzanych działaniach gości	Czynności zabezpieczające sieć Wi-Fi przed ujawnieniem. Nie pozostawianie komputera, laptopa bez opieki i nadzoru Zakaz prowadzenia rozmów biznesowych w miejscach publicznych. Służby ochrony wyczulone na kontrolowanie wizyty osób odwiedzających organizację oraz ich celu odwiedzin
ZAG.2	Przestrzeganie PBI System kontroli dostępu System ochrony pożarowej System telewizji dozorowej System alarmowy	Ogół procedur służących zapewnieniu wymaganego poziomu bezpieczeństwa pożarowego w poprawne sformułowanej i dopracowanej PBI.
ZAG.3	Doposażenie biur w niszczarki Procedury archiwizacji dokumentów Przechowywanie dokumentów nie dłużej niż to konieczne	Korzystanie z niszczarek o najwyższym poziomie bezpieczeństwa w celu należytego zutylizowania dokumentów, zawierających poufne informacje (cięcie papieru poprzeczne i wzdłużne). Upoważnione osoby do niszczenia tego typu dokumentów. Archiwizowanie dokumentów zgodne z wymaganiami organizacji, nadzorowane elektronicznie. Cyfrowa archiwizacja dokumentów w jednym miejscu (skanowanie dokumentów) Utylizacja dokumentów poprzez uprawnionych pracowników (szkolenia osób odpowiedzialnych za utylizację dokumentów) Protokół zniszczenia z datą utylizacji, formę i sposobem utylizacji.
ZAG.4	Szyfrowanie nośników danych Znaczenie i rola PBI podczas kradzieży dokumentów, nośników Kontrola dostępu	Zaszyfrowanie używanych nośników danych typu: pendrive, dyski twarde, płyty CD/DVD Procedury postępowania podczas stwierdzenia faktu kradzieży dokumentów, nośników W pomieszczeniach, w których przetwarzane są informacje ograniczenie dostępu osób nieupoważnionych do urządzeń firmowych.
ZAG.5	Polityka korzystania z poczty elektronicznej Szyfrowanie wiadomości kluczem publicznym Zgłaszanie przełożonemu pojawienia się incydentu	Procedury postępowania podczas logowania się na pocztę e-mailową Nie otwieranie załączników z nieznanego adresu Sprawdzanie adresu odbiorcy, do którego wysyłana jest korespondencja Wysyłanie zaszyfrowanych wiadomości Określone postępowanie podczas zidentyfikowania zagrożenia
ZAG.6	Audyt bezpieczeństwa (sprawdzenie) PBI dostępna dla wszystkich pracowników Wdrożenie do organizacji systemu DLP (Data Loss Prerention) Szkolenia dotyczące wymogów posiadania w organizacji PBI	Procedury niezbędne do utrzymania i przeglądu zasobów w kierunku wykrycia jego zużycia lub też naprawy, czy potwierdzenia poprawności działania systemu. Zapoznanie wszystkich pracowników z zasadami, wynikającymi z PBI Dzięki oprogramowaniu można ochronić dane przetwarzane w systemie Program szkoleń obejmujący potrzebę wdrożenia w życie organizacji zasad i reguł PBI
ZAG.7	Polityka monitoringu Zapewnienie przeglądów stanu technicznego budynków w tym	Korzystanie z systemu powiadamiania-alarm. System dozoru wizyjnego z przekazaniem informacji do centrali

L.p. zagrożenia	Zabezpieczenia	Opis
	okien i drzwi System sygnalizacji przeciwpożarowej Ogrodzenie wokół budynku Służby ochrony Szafy metalowe, zamki, sejfy	Systematyczna konserwacja okien i drzwi Zainstalowanie czujników wykrycia pożaru Obszar organizacji ogrodzony wraz z bramą i szlabanem przy wjeździe. Kontrola dostępu przez pion ochrony przy wjeździe do organizacji
ZAG.8	Konieczność edukowania pracowników o zasadach bezpieczeństwa informacji Powiększanie kompetencji pracowników o systemie ochrony informacji	Szkolenia wstępne dla nowych pracowników-znając sposoby kradzieży danych łatwiej się przed nimi zabezpieczyć. W wyniku braku wiedzy, możliwe popełnianie błędów przez pracowników.
ZAG.9	Skontrolowanie gościa przez służby ochrony przy wejściu do organizacji Informowanie ochrony o podejrzanych działaniach Lokalizacja stanowisk komputerowych z odpowiednim ustawieniem ekranów komputera Przewodnik bezpieczeństwa dla gościa	Dostęp do organizacji po wylegitymowaniu przez służby ochrony i zidentyfikowaniu gościa. Wyczuleni pracownicy na podejrzane zachowania osób odwiedzających organizację. Odpowiednia lokalizacja stanowisk komputerowych uniemożliwiająca dostęp osób postronnych oraz nieuprawnionych do miejsc, w których przetwarza się informację. W przewodniku bezpieczeństwa znajdują się mapka przedsiębiorstwa oraz informacje dot. zakazu np.: palenia tytoniu
ZAG.10	Zweryfikowanie gości w recepcji Opracowanie procedur dotyczących wpuszczania postronnych osób na teren organizacji Szkolenia	Kontrola odwiedzających gości, celu odwiedzin. Zakaz bagatelizowania dozoru nad osobami odwiedzającymi przedsiębiorstwo. Program szkoleń oparty o tematy skutków wyłudzeń informacji poprzez osoby obce. Określony sposób postępowania wobec odwiedzających gości (gość czeka przy służbach ochrony aż przyjdzie po niego pracownik). Księga wejść/wyjść
ZAG.11	Szkolenia dotyczące roli, zadań i odpowiedzialności IODO Określenie obowiązków wykonywanych przez IODO Rekrutując IODO obowiązkowe doświadczenie i wiedza na temat przetwarzania danych osobowych zgodnie z wymogami RODO	Wyznaczenie Inspektora Danych Osobowych, jako osoby odpowiedzialnej za przetwarzanie danych osobowych Zaplanowanie programu szkoleń spowoduje znajomość osoby odpowiedzialnej za wprowadzanie zasad doskonalących SZBI w organizacji oraz uwzględnienie w postępowaniu pracowników wymogów proponowanych w RODO
ZAG.12	Szkolenia obejmujące znaczenie ochrony tajemnicy handlowej Szkolenia dla osób przygotowujących umowy Podpisanie przez petenta, kontrahenta, partnera biznesowego klauzuli o zachowaniu poufności i tajemnicy Zakaz prowadzenia rozmów o sposobach funkcjonowania organizacji i używanych innych zabezpieczeniach niż te ogólnodostępne	Uświadamianie personelu, co roli i znaczenia strategicznych informacji przechowywanych w organizacji oraz skutków jej utraty. Przygotowanie druku umowy o zachowaniu poufności dopasowanego do organizacji
ZAG.13	Ochrona przed utratą zasilania. UPS-y prądotwórcze Odciążenie sieci zasilających	Własne agregaty o mocy większej niż moc urządzeń podłączonych do UPS-u Zabezpieczenia urządzeń przed przepięciem (listwa

L.p. zagrożenia	Zabezpieczenia	Opis
	Bezpieczeństwo fizyczne systemów informatycznych	przepięciowa) i inne. Ochrona fizyczna systemów informatycznych
ZAG.14	Wprowadzenie zabezpieczeń do systemów informatycznych. Wprowadzenie zabezpieczeń fizycznych pomieszczeń, dokumentów, używanych sprzętów, urządzeń przed wyciekiem informacji. Uświadamianie współpracowników i petentów o wartości informacji. Sprawdzanie i skontrolowanie powodu, dla którego nie działa poprawnie komputer lub czy jest zainfekowany wirusem	Wprowadzenie procedur postępowania opartych o PBI. Zapoznanie pracowników z aktami prawnymi, normami, rozporządzeniami, ramami prywatności obejmującymi temat bezpieczeństwa informacji. Rozmowy z pracownikami na temat sposobów bezpiecznego przechowywania informacji w organizacji.
ZAG.15	Codzienna kontrola operacji wykonywanych wewnątrz organizacji. Rozwiązania organizacyjno-techniczne. Zakaz wynoszenia nośników poza obszar organizacji bez wcześniejszej zgody Administratora. Procedura postępowania ze zgubionym sprzętem służbowym	Monitoring operacji Nie należy wynosić dysków twardych, płyt CD/DVD, pamięci flash poza obszar przedsiębiorstwa. Poinformowanie przełożonego o zaistniałym incydencie i udziale w naruszeniu bezpieczeństwa. Praktykowanie zasady indywidualnych rozmów z pracownikami celem ujawnienia incydentu i bezpośredniego udziału w nim. Praktyka wskazuje na szybką ingerencję ze strony organizacji w celu zminimalizowania skutków utraty informacji.
ZAG.16	Ograniczenie poziomu uprawnień osobom nieprzestrzegającym procedur w organizacji. Blokada portu USB. Wykrywanie poufnych informacji przez programy antywirusowe.	Natychmiastowe odebranie uprawnień osobom, które nie przestrzegają prawa i zasady obowiązujące w organizacji Otrzymywanie powiadomień o podłączeniu urządzenia USB do komputera Zainstalowanie specjalistycznego oprogramowania wykrywającego nadużycia
ZAG.17	Monitoring nadawania uprawnień Postępowanie dyscyplinarne wobec pracowników Polityka haseł	Czynności nadzorujące kontrolę nad nadanymi uprawnieniami. Nakładanie kar na pracowników naruszających obowiązki pracownicze. Hasła zmieniane, z częstotliwością, co 30 dni, dyskretne chowanie haseł.
ZAG.18	Urządzenia antypodsłuchowe dedykowane linii telefonicznej, sieci komputerowej i telewizji przemysłowej Odpowiednie okablowanie	Używanie urządzeń skierowanych na wykrywanie i przeciwdziałanie podsłuchowi (zagłuszacze). Prowadzenie kabli z daleka od obszarów publicznych, pod ziemią.
ZAG.19	Procedura postępowania przy stanowisku komputerowym Kopia zapasowa bezpieczeństwa danych Serwisowanie urządzeń komputerowych	Ogół procedur służących zapewnieniu BI Codzienne tworzenie kopii zapasowej. Prowadzenie regularnej obsługi serwisowej komputerów
ZAG.20	Ochrona antywirusowa przed nielegalnym oprogramowaniem Skanowanie plików z nośników pamięci programem antywirusowym Zgłaszanie incydentu	Kontrolowanie dostępu do danych w celu ograniczenia pojawienia się złośliwego oprogramowania Zakaz wyłączania lub kasowania programu antywirusowego Podczas stwierdzenie pojawienia się zagrożenia należy niezwłocznie zgłosić zdarzenie przełożonemu

L.p. zagrożenia	Zabezpieczenia	Opis
ZAG.21	Płatne programy antywirusowe Zakaz pisania haseł do systemu komputerowego na ekranie monitora Częsta zmiana haseł Procedura postępowania podczas wysyłania wiadomości Przetwarzanie informacji tylko przez użytkowników upoważnionych przez zarząd organizacji	Korzystanie ze sprawdzonych, przetestowanych programów zabezpieczających oprogramowanie komputerowe. Korzystanie z generatora haseł. Zgłaszanie przełożonemu wiadomości e- mailowych o ujawnienie hasła lub identyfikatora. Przetwarzanie informacji zgodnych z klasyfikacją i wydanymi upoważnieniami
ZAG.22	Uświadamianie o wartości informacji współpracowników i petentów Zamykanie drzwi do biur, pomieszczeń, w których przechowuje się dokumenty	Szkolenia dla pracowników Ustawienie monitora komputera, tak by uniemożliwić wgląd nieupoważnionych osób. Kontrola dostępu do pomieszczeń
ZAG.23	Wydzielone miejsca przechowywania dokumentów i nośników danych Kontrola dostępu do pomieszczeń biurowych Informowanie przełożonego o próbie logowania do systemu osoby nieuprawnionej	Stosowanie rozwiązań dotyczących blokowania dostępu do zasobu. Dostęp do pomieszczeń, stref ochronnych poprzez użycie kart dostępowych Zakaz pokazywania identyfikatorów innym pracownikom oraz hasła do systemu Zakaz pracy na wspólnym koncie osób współpracujących

Kolejnym krokiem jest przypisanie wartości liczbowych poszczególnym atrybutom informacji w miejsca, które wynikają z mapowania zagrożeń.

Wartości liczbowe zawarte w tabeli 20, uzyskano z przeprowadzonych wcześniej badań ankietowych, obserwacji nieuczestniczącej, wywiadu swobodnego oraz testu ataków ujawnienia informacji. Dodatkowo zagrożenia te sklasyfikowano zgodnie z kategoriami diagramu Ishikawy.

Odpowiedzi respondentów w pyt.5 *(proszę o wskazanie, które z poniżej wymienionych zagrożeń utraty bezpieczeństwa informacji Pani/Pana zdaniem są prawdopodobne, do wystąpienia w Państwa przedsiębiorstwie określając częstotliwość ich występowania)* uśredniono, a później przedstawiono w skali oceny wystąpienia zagrożenia od 1 do 5. Przykładowo dla zagrożenia (Z.7)- brak fizycznej ochrony budynków, okien i drzwi otrzymano wynik 1,5. Postępowano analogicznie z kolejnymi zagrożeniami i wyliczeniami. Analiza ryzyka utraty bezpieczeństwa informacji uwzględnia parametry poziomu zabezpieczeń oraz prawdopodobieństwa wystąpienia zagrożeń.

Na podstawie odpowiedzi udzielonych w pytaniu 6 kwestionariusza ankiety wskazano na wybór zastosowanych i obowiązujących w organizacjach zabezpieczeń.

Analogicznie jak w przypadku zagrożeń, zidentyfikowanym zabezpieczeniom przypisano wartości liczbowe określające ich skuteczność w skali 1-5. Przykładowo dla zabezpieczenia dedykowanemu zagrożeniu Z.7 (zgodnie z tabelą 19) przypisano wartość 2.7. Jest to średnia wyliczona z odpowiedzi udzielonych przez respondentów.

W tabeli 16. przedstawiono przykładowe wyliczone wartości przypisywane poszczególnym zagrożeniom oraz zabezpieczeniom.

Tabela 16. Średnia wartość prawdopodobieństwa wystąpienia zagrożenia oraz poziomu zabezpieczeń

Zagrożenie	**Średnia wartość z 5 pytania ankietowego dot. prawdopodobieństwa wystąpienia zagrożenia**			**Średnia wartość z 6 pytania ankietowego dot. poziomu zabezpieczeń**		
Brak fizycznej ochrony budynków okien i drzwi	Skala od 0-5	Udział respondentów	Punkty	Skala od 0-5	Udział respondentów	Punkty
	0	0,12	0	0	0,15	0
	1	0,59	0,59	1	0,14	0,14
	2	0,08	0,16	2	0,12	0,24
	3	0,15	0,45	3	0,25	0,75
	4	0,03	0,12	4	0,12	0,48
	5	0,03	0,15	5	0,22	1,1
Suma			1,47			2,71

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Skala oceny prawdopodobieństwa wystąpienia zagrożenia powstała na podstawie wywiadu oraz obserwacji.

Zastosowana w ocenie prawdopodobieństwa skala ma następujące kryteria:

Tabela 17. Kryteria dla wystąpienia prawdopodobieństwa

Skala	Charakterystyka
1	Minimalna szansa wystąpienia zagrożenia
2	Zagrożenie jest mało realne, ale w innych organizacjach wystąpiło
3	Zagrożenie jest realne, miało miejsce w organizacjach
4	Zagrożenie jest wysokie, często występuje w trakcie realizowanych zadań
5	Zagrożenie jest bardzo wysokie

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Kryteria dla zabezpieczenia przedstawione zostały w tabeli 18.

Tabela 18. Kryteria dla zabezpieczenia

Skala	Zabezpieczenie	Charakterystyka
1	Słabe dla zasobu	Niedziałające na zasób lub tez działające sporadycznie
2	Średnie dla zasobu	Działające na zasób w niewielkiej ilości
3	Istotne dla zasobu	Działające na zasób w sposób istotny
4	Dobre dla zasobu	W większości działający zasadnie na zasób
5	Bardzo dobre dla zasobu	Obejmuje całość zasobów, które podlegają ochronione

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Następnie, w celu ustalenia wartości skutku skorzystano z następujących kryteriów, zamieszczonych w tabeli 19.

Tabela 19. Kryteria dla wskaźnika oceny skutku

Skala	Skutek	Charakterystyka
1	Nieważne	Naruszenie wpływające na nieznaczne utrudnienia w systemie bezpieczeństwa
2	Mało istotne	Naruszenie informacji wywołująca małe utrudnienia w systemie bezpieczeństwa
3	Ważne	Naruszenie informacji związane ze szkodą umiarkowaną, wywołującą utrudnienia w systemie bezpieczeństwa
4	Bardzo ważne	Naruszenie informacji wywołane znaczącymi utrudnieniami w systemie bezpieczeństwa oraz związane z tym są szkody finansowe
5	Krytyczne	Naruszenie informacji związane z przerwaniem procesów biznesowych, duża szkoda dla organizacji oraz konsekwencje prawne

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Z kolei ocena skutku obliczona została według opinii respondentów zamieszczona w pytaniu 7.

Przykładowo dla zagrożenia 7. brak fizycznej ochrony budynków, drzwi, okien otrzymano wynik 4,1. Wszystkie otrzymane wyniki z przeprowadzonych badań zawarte zostały w tabeli 20.

Tabela 20. Otrzymane wyniki badań oceny skutku, kwantyfikacji prawdopodobieństwa wystąpienia zagrożenia oraz wskazanie zabezpieczeń zagrożeń bezpieczeństwa informacji

Zagrożenie	Poufność (nieuprawniony dostęp)			Integralność (modyfikacja)			Dostępność (utrata)			Niezawodność systemu			Autentyczność systemu			Rozliczalność systemu		
	Zabezpieczenie	Prawdopodobieństwo	Skutek	Zabezpieczenie	Prawdopodobieństwo	Skutek	Zabezpieczenie	Prawdopodobieństwo	Skutek	Zabezpieczenie	Prawdopodobieństwo	Skutek	Zabezpieczenie	Prawdopodobieństwo	Skutek	Zabezpieczenie	Prawdopodobieństwo	Skutek
Z.1	2,9	1,7	3,1	2,9	1,7	3,1	2,9	1,7	3,1	2,9	1,7	3,1	2,9	1,7	3,1	2,9	1,7	3,1
Z.2	2,4	1,9	3,7	2,4	1,9	3,7	2,4	1,9	3,7	2,4	1,9	3,7	2,4	1,9	3,7	2,4	1,9	3,7
Z.3	3,6	1,2	3,3	2,4	1,9	3,7	2,4	1,9	3,7									
Z.4	3,6	2,1	3,5				3,6	2,1	3,5				3,6	2,1	3,5			
Z.5	3,7	1,5	3,7	3,7	1,5	3,7	3,7	1,5	3,7				3,7	1,5	3,7			
Z.6	3,9	1,1	3,7	3,9	1,1	3,7	3,9	1,1	3,7				3,9	1,1	3,7			
Z.7	2,7	1,5	4,1	2,7	1,5	4,1	2,7	1,5	4,1				2,7	1,5	4,1	2,7	1,5	4,1

Z.8	3,3	2.1	4	3,3	2.1	4	3,3	2.1	4	3,3	2.1	4	3,3	2.1	4	3,3	2.1	4
Z.9	2,9	2,2	3,5	2,9	2,2	3,5	2,9	2,2	3,5				2,9	2,2	3,5			
Z.10	3,7	2,0	4	3,7	2,0	4	3,7	2,0	4									
Z..11	3,4	1,1	3,6				3,4	1,1	3,6									
Z.12	2,9	1,7	3,9															
Z.13				3,2	2,2	3,6	3,2	2,2	3,6	3,2	2,2	3,6						
Z.14										3,2	1,3	3,4				3,2	1,3	3,4
Z.15	3,6	1,5	3,7										3,6	1,5	3,7			
Z.16	2,9	1,7	3,7	2,9	1,7	3,7												
Z.17	3,2	1,9	3,7	3,2	1,9	3,7	3,2	1,9	3,7				3,2	1,9	3,7	3,2	1,9	3,7
Z.18	0,9	1,2	3,3				0,9	1,2	3,3									
Z.19							2,9	2,4	3,8	2,9	2,4	3,8	2,9	2,4	3,8			
Z.20	2,3	1,8	3,4	2,3	1,8	3,4	2,3	1,8	3,4	2,3	1,8	3,4						
Z.21	2,5	1,6	4,1	2,5	1,6	4,1	2,5	1,6	4,1									
Z.22	2,8	1,72	4															
Z.23	2,9	1,8	3,9	2,9	1,8	3,9	2,9	1,8	3,9				2,9	1,8	3,9			
Wartość uśrednionego zagrożenia	3	1,6	3,7	3	1,8	3,7	2,9	1,7	3,7	2,9	1,7	3,7	3,1	1,7	3,7	2,9	1,6	3,7

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Prowadząc dalszą analizę ryzyka przyjęto, za wskaźnik oceny skutku wartość 4 (bardzo ważne), co oznacza, że naruszenie informacji spowoduje znaczące utrudnienia w systemie bezpieczeństwa raz związane z tym szkody finansowe.

Rozpoznany stan w organizacjach wskazuje na istnienie wielu zidentyfikowanych zagrożeń przedstawionych na diagramie Ichikawy, które nie są akceptowalne, ze względu na skutek, jaki mogą wywołać. Zidentyfikowane zagrożenia i ich wpływ na posiadane zasoby powinny podlegać dalszemu monitorowaniu i kontrolowaniu ich wpływu na skutek.

Waga danych

Ważność informacji przetwarzanej w organizacji może być określona wagą danych. Waga jest tworzona na podstawie zespołu czynników wpływających na jej wartość. W celu jej wyznaczenia konieczne jest precyzyjne określenie tych czynników.

Po przeprowadzeniu wywiadu z kierownictwem oraz zarządem w organizacjach dokonano klasyfikacji informacji i na tej podstawie określono wagę informacji dla przedsiębiorstwa. Organizacje są w posiadaniu informacji zawierających dane do projektów, prototypów, stosowanej technologii, karty produktów, czy know-how itp. Ujawnienie którejkolwiek z tych informacji mogłoby doprowadzić do utraty atrybutów bezpieczeństwa informacji.

Do zespołu czynników wagi zaliczono: zakres danych, istotność informacji dla działalności organizacji, stopień złożoności procesu przetwarzania danych, liczba uczestników, która przetwarza dane, liczbę podmiotów, których dane są udostępniane w organizacji. Każdy z tych czynników oceniono w skali 1-5. Przyjętą skalę można dowolnie modyfikować, lecz aby zachować wiarygodność metody warto wiedzieć, że raz przyjęta skala powinna być zachowana dla wszystkich czynników zespołu wagi. Zespół czynników wagi ma charakter szacunkowy, ustalony został przez autorkę pracy w oparciu o informacje zawarte w rejestrach systemowych organizacji. Opis każdego z czynników znajduje się w dalszej części analizy ryzyka.

Wartości liczbowe zespołu czynników wagi zaprezentowano w tabelach 21-25.

„Zakres danych” to zbiór informacji związanych z realizacją czynności przetwarzania informacji, wyrażony liczebnością przetwarzanych poufnych informacji w organizacji. Źródłem danych, z których czerpie się wiadomości o zawartych umowach jest system rejestrowania takich umów. Z przeprowadzonego wywiadu

z dyrektorami organizacji wynika, że przetwarza się ich powyżej 121, o ustalonej wewnętrznej strukturze.

Tabela 21. Kryteria dla wskaźnika „Zakres danych”

Skala	Charakterystyka
1	1 do 30
2	31 do 60
3	61 – 90
4	91 – 120
5	od 121

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

„Istotność informacji” jest to ocena przydatności informacji w kontekście realizowanych procesów w przedsiębiorstwie. Za istotne informacje uznaje się te, których pominięcie lub zmodyfikowanie może znacząco wpłynąć na decyzje podejmowane przez zarząd.

Dla potrzeb wyliczeń przyjęto tą samą skalę oceny stosowaną we wszystkich obliczeniach, a występującą również w kwestionariuszu ankiety, (czyli od 1 do 5). Należy pamiętać, że raz przyjęta skala powinna obowiązywać we wszystkich dalszych analizowanych czynnościach wpływająca na wartość utraty informacji.

Z uwagi na fakt, że badane organizacje są w grupie przedsiębiorstw zajmujących się projektami, patentami, prototypami autorka pracy oszacowała wagę istotności informacji dla organizacji, na poziomie wartości liczbowej 5.

Tabela 22. Kryteria dla wskaźnika „Istotności informacji dla działalności”

Skala	Charakterystyka
1	Informacja nieistotna
2	Informacja o niewielkiej wartości
3	Informacja od średniej do znacznej wartości
4	Informacja bardzo ważna
5	Informacja krytyczna w skutkach

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

„Stopień złożoności procesu przetwarzania danych” określono na podstawie niezbędnych do realizacji procesów w organizacji. Ilość obróbki informacji w poszczególnych procesach wskazuje na nadanie temu czynnikowi wartości 5.

Tabela 23. Kryteria dla wskaźnika „Stopień złożoności procesu przetwarzania danych”

Skala	Charakterystyka
1	Czynność od małoistotnej do niewielkiej, zaprzestanie realizowania nie skutkuje żadnymi konsekwencjami
2	Czynność od niewielkiej do średniej istotności, ograniczony wpływ na działanie przedsiębiorstwa
3	Czynność od średniej do dużej istotności, średni wpływ na działanie przedsiębiorstwa

Skala	Charakterystyka
4	Czynność od dużej do bardzo dużej istotności, duży wpływ na działanie, ograniczenie działania organizacji
5	Czynność od bardzo dużej do krytycznej istotności, krytyczny wpływ na działanie przedsiębiorstwa, zaprzestanie działań biznesowych

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Wskaźnik „Liczba uczestników przetwarzających dane w organizacji" wyraża liczbę osób posiadających dostęp do informacji w przedsiębiorstwie. W wyniku przeprowadzonego wywiadu stwierdzono, że w każdym z badanych przedsiębiorstw dostęp do przetwarzania strategicznych informacji posiada ponad 100 osób, a mniej niż 1000. Stąd też wskaźnikowi temu przypisano wartość 4 zgodnie z klasyfikacja zawartą w tabeli 24.

Tabela 24. Kryteria dla wskaźnika Liczba uczestników, która przetwarza dane w organizacji

Skala	Charakterystyka
1	mniej niż 3
2	Od 4-10
3	od 11 do 100
4	od 101-1000
5	powyżej 1000

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Po przeprowadzeniu wywiadu z kierownictwem w organizacjach wykazano, że w badanych przedsiębiorstwach przetwarza się dane pochodzące z wielu różnych organizacji.

Wskaźnik „liczba podmiotów danych" określa liczbę przedsiębiorstw zewnętrznych, których dane są przetwarzane w badanych dziewięciu przedsiębiorstwach. W wyniku przeprowadzonego wywiadu w zakresie umów z kontrahentami stwierdzono, że w każdym z analizowanych przedsiębiorstw jest zawartych od 21 do 40 umów. Stąd też wskaźnikowi temu przypisano wartość 4 zgodnie z przyjętą klasyfikacja zawartą w tabeli nr.25.

Tabela 25. Kryteria dla wskaźnika Liczba podmiotów danych

Skala	Charakterystyka
1	od 1-5
2	od 6-10
3	od 11-20
4	od 21-40
5	powyżej 40

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Przyjęta wartość na poziomie 4 odzwierciedla stan zawartych umów w wewnętrznym rejestrze organizacji.

Otrzymane wyniki badań pozwoliły na obliczenie średniej wagi informacji. Waga informacji jest parametrem obliczonym o przyjęte założenia, które określono na początku analizy i utrzymywane na tym samym poziomie. Przyjęto średnią arytmetyczną z poszczególnych czynników wagi, na poziomie 4,6. Zestawienie otrzymanych danych zespołu czynników wagi zaprezentowano w tabeli 26.

Tabela 26. Zestawienie otrzymanych wyników

Opis Składnika	Waga składnika
Zakres danych	5
Istotność informacji dla działalności	5
Stopień złożoności	5
Liczba uczestników	4
Liczba podmiotów danych	4
Średnia waga	23:5=4,6

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

W celu przeprowadzenia dalszych obliczeń posłużono się średnią arytmetyczną ze składowych.

Wagę, można przyjąć lub też zmienić w zależności od podjętych wcześniej ustaleń zarządu, co do przyjętej obowiązującej skali.

W niniejszej dysertacji przyjęto wynik średniej wagi na poziomie 4,6

Przeprowadzenie oceny ryzyka

Dzięki wykonaniu analizy ryzyka, diagnozuje się faktyczny stan systemu bezpieczeństwa. Narzędzie to umożliwia zestawienie aktualnych zagrożeń bezpieczeństwa informacji oraz natychmiastowe wprowadzenie zmian w funkcjonującym systemie bezpieczeństwa.

W związku z powyższym, wykorzystano następujący wzór wynikający z przyjętej metodologii szacowania ryzyka.

(3)

$$R = \frac{\mathrm{WxPxS}}{Z}$$

Gdzie:
R-wskaźnik priorytetu ryzyka
W-waga danych
P-prawdopodobieństwo materializacji ryzyka
S-skutek wystąpienia zagrożenia
Z-zastosowanie zabezpieczenia

Po zrealizowaniu kolejnych etapów szacowania ryzyka, w efekcie końcowym dysponuje się kolejno wartościami liczbowymi. Wskaźniki W, Z, P, oceniano w skali od 1 do 5, biorąc pod uwagę kryterium:

W-waga danych, przyjęta w tabeli 26.

Z-ocena stosowanych zabezpieczeń, wartość liczbową przedstawiono w tabeli 20.

P-ocena prawdopodobieństwa wystąpienia zagrożenia, wartość liczbową została przedstawiona w tabeli 20.

S-skutek wystąpienia zagrożenia zaprezentowany w tabeli 20.

Decyzja podjęta przez zarząd organizacji oraz upoważnione do tego osoby dotyczące oceny skutków jest postanowieniem arbitralnym.

Następnie dokuje się oceny ryzyka utraty informacji przy wykorzystaniu w/w wzoru. Dalej przeprowadza się analizę ryzyka poszczególnie dla każdego z atrybutów informacji wymienionych w tabeli 14, obejmującym mapowanie zagrożeń.

Zestawienie wszystkich niezbędnych wartości do oszacowania ryzyka zgodnie z w/w wzorem przedstawia tabela 27.

Tabela 27. Zaprezentowane wyniki z przeprowadzonej analizy ryzyka

Atrybut bezpieczeństwa informacji	Waga	Prawdopodobie-ństwo	Skutek	Zabezpieczenie	Ryzyko	Wskazanie poziomu akceptacji ryzyka
Poufność (nieuprawniony dostęp)	4,6	1,6	3,7	3	4,6x1,6x 3,7:3)= 9,1	Wysokie
Integralność (modyfikacja)	4,6	1,8	3,7	3	10,2	Wysokie
Dostępność (brak dostępności)	4,6	1,7	3,7	2,9	10,0	Wysokie
Niezawodność (awaria systemu)	4,6	1,7	3,7	2,9	10,0	Wysokie
Autentyczność (brak nieuprawionej modyfikacji)	4,6	1,7	3,7	3,1	9,3	Wysokie
Rozliczalność (odpowiedzialność za użytkowanie informacji)	4,6	1,6	3,7	2,9	9,4	Wysokie

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Analiza danych zawartych w tabeli 27 wskazuje na fakt, że największa wartość ryzyka (tj.10,2) związana jest z utratą integralności informacji w systemach, w których przetwarzane są informacje oraz dostępnością i niezawodnością (10,0). Dalej wysoki poziom oceny ryzyka dotyczy: poufności (9,1), i autentyczności (9,3) i rozliczalności

(9,4). Dane zamieszczone w niniejszej analizie wskazują, na problemy związane z dostępnością oraz integralnością informacji przechowywanej i przetwarzanej w organizacji. Zatem, wymaga się od organizacji gospodarczych zastosowania i określenia działań prewencyjnych, ukierowanych na zmniejszenie prawdopodobieństwa pojawienia się tego zagrożenia i zmniejszenia jego skutków. Oszacowany wysoki poziom ryzyka sprzyja powstaniu nowych zagrożeń, w wyniku, których informacja może zostać ujawniona, zniszczona czy też zmodyfikowana lub utracona.

Podsumowując przeprowadzone badania, można stwierdzić, iż wartość ryzyka jest na poziomie nieakceptowalnym. Organizacja gospodarcza, które chce bezpiecznie przetwarzać informacje powinna podjąć działania w kierunku minimalizowania ryzyka do poziomu akceptowalnego.

Rekomendacje

Otrzymując konkretne wartości ryzyka, zaleca się odpowiednie zarządzanie ryzykiem, w zależności od klasyfikacji ryzyka. W tabeli 28 znajdują się kryteria oceny ryzyka wraz ze wskazaniem warunków brzegowych analizy.

Klasyfikację ryzyka przyjęto na podstawie poszczególnych parametrów ryzyka określonych w/w wzorze. Ryzyko niskie, występuje wówczas, gdy waga danych, prawdopodobieństwo wystąpienia zagrożenia oraz skutek zagrożenia są niskie, a wartość zabezpieczenia jest bardzo wysoka. Z kolei ryzyko krytyczne pojawia się gdy waga danych, prawdopodobieństwo wystąpienia zagrożenia oraz skutek są wysokie, a wartość zabezpieczenia jest niska.

Najmniejsze ryzyko 0,2 występuje wówczas, gdy waga danych, prawdopodobieństwo i skutek są minimalne (1), a zabezpieczenia bardzo dobre (5). Z kolei największe ryzyko (125) występuje wówczas, gdy sytuacja jest odwrotna, tzn. waga danych, prawdopodobieństwo i skutek są maksymalne (5), a zabezpieczenia słabe (1).

Tabela 28. Gradacja ryzyka

Wielkość ryzyka	Wartość brzegowa **Ocena min ryzyka**	Wartość brzegowa **Ocena max ryzyka**
Niskie	0,2	0,9
Średnie	1	9
Wysokie	10	26
Bardzo wysokie	27	63
Krytyczne	64	125

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

W zależności od otrzymanego wyniku ustala się wartość ryzyka i sposoby postępowania z nim, rozróżniając, w jakich zakresach klasyfikacji się ono mieści.

Tabela 29. Rodzaje postępowań z ryzykiem

Wielkość ryzyka	Postępowanie z ryzykiem
Niskie	Brak potrzeby wykonywania działań obniżających ryzyko.
Średnie	Brak potrzeby wykonywania działań obniżających ryzyko, ale konieczność monitorowania jego i kontrolowania.
Wysokie	Konieczność skoncentrowania działań obniżających ryzyka do poziomu średniego. Pozostawienie ryzyka na wysokim poziomie grozi utratą lub ujawnieniem informacji, co może być równoznaczne z utratą konkurencyjności. Należy bezwzględnie zmniejszyć ryzyko do wielkości ryzyka średniego lub niskiego. Konieczność wprowadzenia środków redukujących poziom ryzyka. Poinformować zarząd oraz personel o poziomie wysokiego ryzyka. Natychmiast należy wprowadzić działania monitorujące poziom ryzyka.
Bardzo wysokie	Należy ograniczyć zakres przetwarzania informacji w danym obszarze. Ponownie przeprowadzić ewaluację skutków, po redukcji zakresu przetwarzania informacji. Bowiem mniejsza waga danych przekłada się na zmniejszenie skutków materializacji poszczególnego ryzyka. Należy bezwzględnie zmniejszyć ryzyko do wielkości ryzyka średniego lub niskiego ryzyka. Konieczność wdrożenia nowych środków zabezpieczających. Poinformować zarząd oraz personel o poziomie bardzo wysokiego ryzyka.
Krytyczne	Natychmiastowa konieczność zastosowania środków obniżających ryzyko do wielkości średniego lub też niskiego. Należy bezwzględnie zmniejszyć ryzyko do wielkości ryzyka średniego lub niskiego. Konieczność natychmiastowego wdrożenia nowych środków zabezpieczających oraz redukujących ryzyko. Poinformować zarząd oraz personel o poziomie krytycznego ryzyka.

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

W zależności od rodzaju prowadzonej działalności, zaleca się wykonywanie analizy ryzyka, nie rzadziej niż raz na rok. Jednak, dokonując zmian w procedurach, postępowaniu z umowami czy strukturze organizacyjnej, powinno się wykonać ją ponownie. Dokonując jej można przygotować się na sytuacje pojawienia się ryzyka i odpowiednio ochronić, aplikując nowe zabezpieczenia lub też poszerzając zakres już istniejących. Sugeruje się, aby we wszystkich uzyskanych rodzajach zagrożeń zaimplementować nowe środki mające na celu minimalizację powstania skutków zaistniałego zagrożenia, a w szczególności zwrócić uwagę na te ryzyka, które zostały określone mianem bardzo wysokiego, wysokiego i krytycznego, gdyż to one w pierwszej kolejności wymagają uwagi i podjęcia działań z tym związanych.

Dokonując oceny 9 przebadanych przedsiębiorstw można stwierdzić, że grupa zidentyfikowanych zagrożeń jest autentyczna, oparta o uzyskane wyniki badań i wynikające z tego wnioski. Zidentyfikowane luki systemu w wyniku obserwacji oraz wywiadu zgodnie z przyjętą oceną częstotliwości występowania zaobserwowanych zagrożeń i istniejących zabezpieczeń poddano kryterium oceny przyjętym w tabelach

17-19. Zatem przeprowadzenie analizy ryzyka ujawniło listę realnych niebezpieczeństw, na które narażone są organizacje i jej systemy.

6.2. Projekt zarządzania bezpieczeństwem informacji zmniejszający ryzyko utraty informacji

W wyniku przeprowadzonego procesu badawczego zarówno teoretycznego, jak i empirycznego zidentyfikowano zagrożenia, które w istotny sposób wpływają, na zachowanie atrybutów bezpieczeństwa informacji. Dotychczasowe działania organizacji należą do nieefektywnych metod zarządzania bezpieczeństwem informacji.

Analiza istniejącego stanu bezpieczeństwa wskazała, że informacje nie są na odpowiednim poziomie chronione i w związku z tym istnieje realne ryzyko ich utraty. Tymczasem, stosowane dotychczas zabezpieczenia, są niepełne w wyniku, czego powstają błędy, słabe miejsca SZBI i wynikające z tego niedociągnięcia systemowe. Koniecznym jest, zatem skupienie uwagi na podjęciu działań doskonalących.

Po zweryfikowaniu stanu BI w organizacjach opracowano propozycję projektu modernizującego podejmowanie działań związanych z zarządzaniem ryzykiem, wraz z proponowanymi zmianami w tym obszarze opartymi o założenia projektu.

Projekt ma na celu wdrożenie rozwiązań, które w istotny sposób zaważą, na redukcji możliwości pojawienia się zagrożeń i poprawę poziomu BI. Opracowanie projektu wymagało wyodrębnienia: założeń projektu, elementów projektu, koncepcji zmian w obszarach organizacji gospodarczej. Wprowadzenie tego typu systemu powinno w realny sposób wpłynąć na zminimalizowanie ryzyka utraty informacji a w szczególności zmniejszyć powstanie zagrożeń wpływających na atrybuty bezpieczeństwa informacji.

Celem opracowania projektu jest zaproponowanie udoskonalonych przedsięwzięć realizowanych w organizacji. Dzięki wprowadzeniu zmian przedsiębiorcy nie będą zaskoczeni zagrożeniami a raczej przygotowani na ich pojawienie się ponadto umiejąc ograniczyć ich niekorzystny wpływ.

Założenia do projektu

Założenia do projektu systemu ZBI są wynikiem analizy zdiagnozowanego stanu bieżącego przedsiębiorstw i posłużą do skonstruowania projektu, w którym zostaną one uwzględnione.

Założenia przedstawiają się następująco:

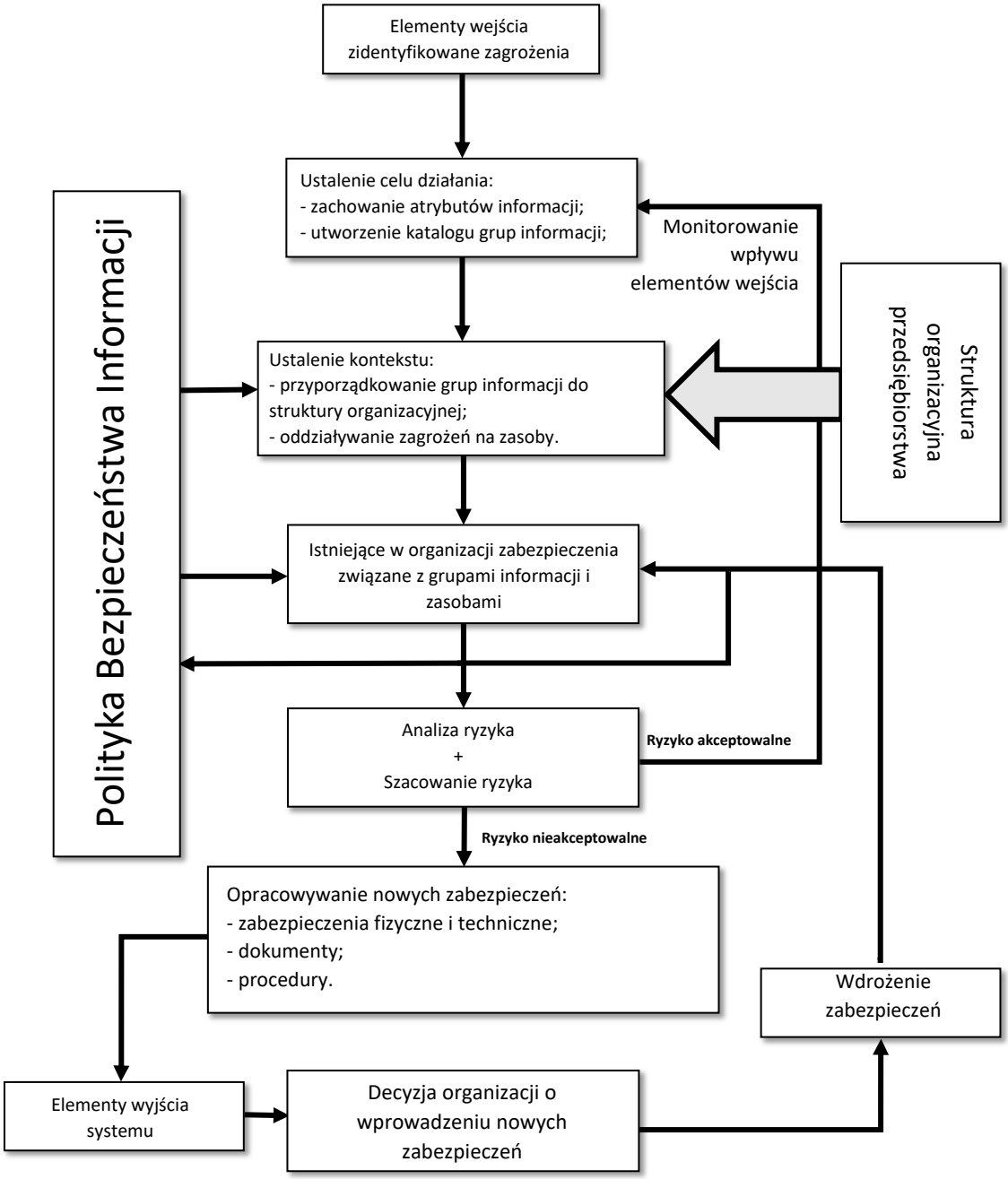
1. uwzględnienie wymagań występujących w aktualnych aktach prawnych, normach, ustawach, rozporządzeniach (rozdział 1.5);
2. dokładne zrozumienie terminologii z zakresu bezpieczeństwa informacji i zarządzania ryzykiem przez pracowników i osoby zarządzające organizacją;
3. zaznajomienie osób zajmujących się zarządzaniem ryzkiem, ze wszystkimi informacjami związanymi z analizą ryzyka;
4. wprowadzenie zabezpieczeń technicznych, organizacyjnych, fizycznych i innych, które należy testować podczas procesu analizy ryzyka;
5. uwzględnienie szkoleń kadry zarządzającej, na temat identyfikowania źródła zagrożenia;
6. utworzenie grup informacji skatalogowanych w katalogu informacji przetwarzanych w przedsiębiorstwie. Zaliczono do nich informacje wewnętrzne, ogólno-dostępne, ściśle chronione;
7. uproszczenie i zwiększenie czytelności PBI obowiązującej, w przedsiębiorstwie (2.3. Polityka Bezpieczeństwa Informacji).

Zakłada się, że komponenty SZBI będą oparte o narzędzia typu regulaminy, procedury i związane z tym działania oraz przedsięwzięcia, które w znaczący sposób oddziałują na ochronę posiadanych aktywów. Dzięki wykorzystaniu poszczególnych komponentów SZBI pracownikowi będzie łatwiej podejmować określone działania stwierdzające podatność na zagrożenia. Istnieje, zatem potrzeba opracowania systemu reagującego na wektor wejściowy (pojawiające się coraz to nowe zagrożenia) tak, aby ich obecność nie powodowała sprowadzenia poziomu ryzyka, do nieakceptowalnego poziomu utraty informacji.

Na podstawie przyjętych założeń opracowano koncepcyjny projekt, przedstawiony na rysunku 71. Budowa systemu ZBI przedstawia się następująco:

1. Koncepcja systemu
2. Etapy budowy systemu
3. Analiza struktury organizacyjnej przedsiębiorstwa
4. Opisanie poszczególnych etapów budowy systemu w odniesieniu do funkcji i zasobów: procedury, odpowiedzialność, przepływ informacji itp.
5. Podsumowanie systemu

Uwzględniając budowę systemu ZBI, na rysunku 71 przedstawiono koncepcyjny projekt zarządzania bezpieczeństwem informacji, redukujący ryzyko utraty informacji.



Rysunek 71. Koncepcyjny projekt zarządzania bezpieczeństwem informacji zmniejszający ryzyko utraty informacji

Źródło: Opracowanie własne

W systemie zaaplikowano sposoby postępowania tak, by ograniczyć pojawienie, się zagrożenia. W tym też, celu powstały procedury, zasady postępowania zawarte w komponentach systemu, które można wykorzystać, wówczas, gdy pojawi się zagrożenie lub już wcześniej podatności na nie. Stworzone procedury będą odznaczać

się uniwersalnością, dzięki czemu można je zaadaptować w każdej organizacji gospodarczej.

Dotychczasowe systemy wykazują się zbyt małym zautomatyzowaniem by móc to robić samodzielnie, zatem istnieje potrzeba ułatwienia pracy systemu tak, by mógł szybko reagować na pojawienie się nowych zagrożeń. W wyniku przedstawionego na rysunku 71 efektu pętli sprężenia zwrotnego analogicznie postępuje, się wg. projektu SZBI zgodnie z pierwotnie przyjętymi procedurami postępowania, określając czas i sposób wprowadzania oraz korzystania z procedur. Tymczasem, poziom określonych zabezpieczeń wynika z przeprowadzonych działań w systemie.

Dlatego też schemat postępowania z zagrożeniem z całą pewnością można powielać, gdy ono się pojawi lub przeprowadzać okresowo. Projekt systemu ZBI wg. przyjętych założeń powinien przynieść pożądany efekt tzn. skuteczność w zapobieganiu utraty podstawowych atrybutów informacji. Działanie SZBI powinno pozwolić na dopasowanie się do panującej sytuacji i określonych warunków pozwalając, na przeprowadzenie powtórnej analizy ryzyka. Dobrze działający system powinien generować odpowiednio dopasowane zabezpieczenia do pojawiających się zagrożeń. W tym też celu, wprowadza się podział obowiązków między poszczególnych pracowników minimalizując, tym samym zjawisko braku poczucia odpowiedzialności za pojawienie się zagrożeń. Wskazane, jest również ustalenie terminu cykliczności działań naprawczych.

Do elementów wejścia projektu zaliczono: zidentyfikowanie występującego zagrożenia w organizacji.

Do ochranianych zasobów organizacji zaliczono:

- odbiorcę (ogół użytkowników korzystający z systemu) decyzyjne osoby w organizacji, pracownicy szeregowi oraz osoby z zewnątrz dostawcy, kontrahenci, partnerzy biznesowi, podwykonawcy, pracownicy ochrony budynków, działy sprzątające, obsługę techniczną;
- systemy operacyjne, wykorzystywane w organizacji. Obejmują specjalistyczne oprogramowanie (skierowane do działów projektowania części zabezpieczające oraz programy antywirusowe) urządzenia sieciowe, i przenośne (smartfony, tablety, laptopy, dyski twarde);
- zaplecze fizyczne w skład, którego wchodzą wszystkie budynki organizacji, wyposażenie biur, komputery, serwery;

- przetwarzane w organizacji zasoby informacyjne bazy danych, archiwa, umowy, dokumenty szkoleniowe, dokumentacja systemowa, plan ciągłości działania, wyniki z przeprowadzonych audytów, pliki, dane cyfrowe, dokumenty, korespondencja, dane dotyczące tajemnicy handlowej, know-how, pozycja organizacji w świecie biznesu, dane badawczo-projektowe, projekty prototypów patenty oraz nie bez znaczenia wiedza i doświadczenie pracowników.

Do elementów wyjścia projektu zaliczono następujące zabezpieczenia w postaci:

- dokumentacji bezpieczeństwa opartej o procedury, dopasowanej do potrzeb i sytuacji organizacji, instrukcji postępowania;
- stosowania znanego słownictwa oraz przyjętych terminów używanych w obszarze bezpieczeństwa informacji w dokumencie PBI;
- określonego, ujednoliconego sposobu postępowania podczas pojawienia się zagrożenia;
- ciągłego edukowania personelu;
- podjęcia przez zarząd decyzji, która w istotny sposób wpłynie na ochronę organizacji przed skutkami wystąpienia zagrożenia.

SZBI opracowano w kolejnych etapach. Etapy to działania ukierunkowane na zmiany BI w zakresie dopasowania do indywidualnych potrzeb organizacji w istniejącym sposobie zarządzania bezpieczeństwem informacji. Warto zaznaczyć, że projekt ma możliwości rozbudowy w zależności od potrzeb i oczekiwań organizacji.
Opracowywanie projektu SZBI obejmuje osiem następujących po sobie etapów.

W etapie pierwszym opracowuje się procedury wykrywania i identyfikowania zagrożeń tych istniejących oraz nowo pojawiających się.
Etap drugi dotyczy opracowania procedury mapowania zagrożeń. Zbudowanie katalogu informacji wg. atrybutów, do których zaliczamy: poufność, dostępność, rozliczalność, autentyczność, niezawodność, niezaprzeczalność, integralność (utworzenie katalogu informacji, jest procesem otwartym i na bieżąco modyfikowalnym w oparciu o wariant pojawienia się nowych zagrożeń).
Etap trzeci bazuje na dostosowaniu stworzonego katalogu informacji do struktury organizacyjnej przedsiębiorstwa. W tym celu ustala się kontekst, obejmujący ocenę wpływu oddziaływania zagrożeń na organizację. Etap ten polega także na opisaniu w procedurach działań oddziaływujących na strukturę organizacji i jej zasoby wraz z uwypukleniem odpowiedzialność za przeprowadzane czynności.

Etap czwarty dotyczy utworzenia tabel stanowiących bazę wiedzy o ujawnionych zagrożeniach oraz dedykowanych im zabezpieczeniach. Tabele powinny zostać wstępnie wypełnione informacjami o wykorzystywanych zabezpieczeniach w organizacji.

Etap piaty polega na zastosowaniu metodologii analizy ryzyka i jego szacowania uwzględniającego parametry: (W) waga danych, (P) prawdopodobieństwo, (S) skutek wystąpienia zagrożenia oraz zabezpieczenia (Z). Wynikiem analizy ryzyka będzie ocena wystąpienia zagrożenia od minimalnej szansy do bardzo wysokiej. Na tym etapie budowy systemu będzie znany poziom ryzyka, czy jest na akceptowalnym poziomie czy też nie.

Etap szósty obejmuje utworzenie nowych procedur generowania potencjalnych rozwiązań zabezpieczających przez osoby odpowiedzialne w danym systemie do tego działania.

Etap siódmy polega na utworzeniu procedur postępowania, związanych z przedstawieniem informacji do zarządu o sposobie zaakceptowania nowych rozwiązań zabezpieczających system.

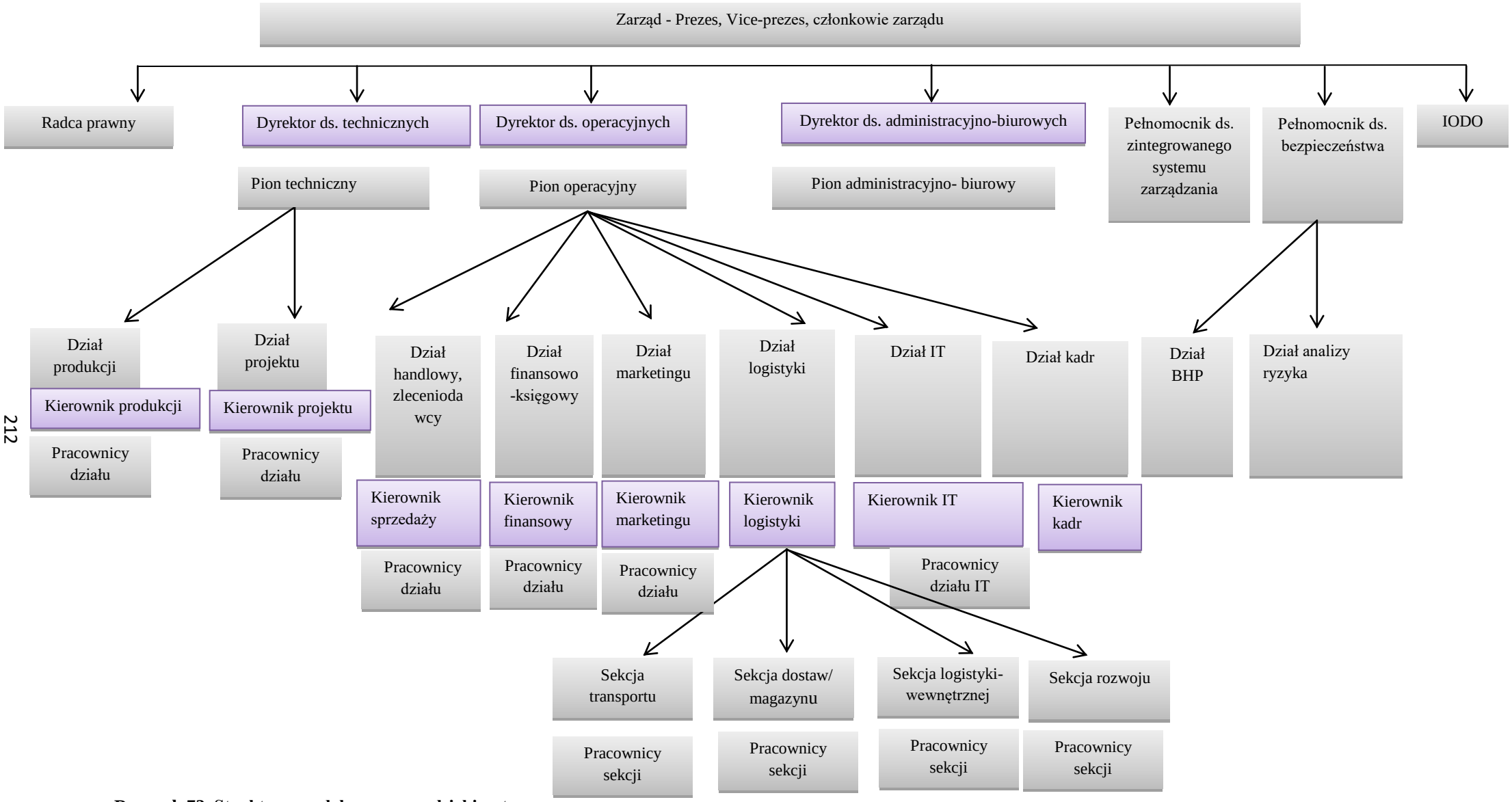
Etap ósmy związany jest z budową procedur związanych z wprowadzaniem zabezpieczeń. Procedura powinna zawierać podział odpowiedzialności za wdrożenie proponowanych zabezpieczeń oraz wpisanie ich do rejestru zabezpieczeń. Wynik oceny ryzyka przed i po wprowadzeniu zabezpieczeń należy wprowadzić do tabeli. Tabele będą wykorzystywane w systemie, który pracuje na wartościach liczbowych poziomu zagrożeń oraz ich zabezpieczeń.

Przedstawienie projektu, ma na celu wyeksponowanie roli i znaczenia wartości informacji w procesie podejmowania decyzji. Procedury, które odnoszą się do każdego z komponentów systemu ZBI będą pomocne w klasyfikowaniu zagrożeń i skutków, ich powstania. Zatem, procedury będą pomagać decydentowi, powziąć strategiczną decyzję, wzbogaconą o wiedzę odnośnie środków zabezpieczających pojawiającej się informacji. Podjęcie właściwych decyzji, będzie sprzyjało podejmowaniu lepszych bardziej trafnych wyborów i stworzeniu warunków, w których to przedsiębiorstwo osiągnie stan bezpieczeństwa i efektywnego zarządzania. Nierozerwalnym elementem SZBI, jest zmodyfikowana Polityka Bezpieczeństwa Informacji, która jako zbiór zasad, procedur jest jednym z ważniejszych elementów przeciwdziałających zagrożeniom (załącznik nr.4).

6.3. Sprawność (praktyczność) projektu zarządzania ryzykiem utraty informacji

Przedsiębiorstwo złożone jest z wielu działów, wzajemnie ze sobą powiązanych przyczyniających się tym samym do osiągnięcia zamierzonych celów. Elementy te można ze sobą łączyć, tworząc różne struktury (techniczną, produkcyjną, organizacyjną oraz inne).

Poniżej znajduje się schemat struktury organizacyjnej modelowego przedsiębiorstwa reprezentatywnego dla badanych organizacji gospodarczych, w którą wpisuje się każda z badanych organizacji, wg. zajmowanych stanowisk pracy z przypisanym zakresem obowiązków i odpowiedzialnością za realizowane obowiązki, na stanowisku pracy.



Rysunek 72. Struktura modelowego przedsiębiorstwa.
Opracowanie własne

To właśnie ludzie związani z działalnością przedsiębiorstwa istotnie wpływają na jego strukturę, decydując o formach zastosowanych zabezpieczeń, a zarząd ostatecznie decyduje o wyborze przyjętej strategii. Na najwyższym szczeblu w hierarchii każdego działu stoi dyrektor wykonawczy/ dyrektor ds. określonego działu, poszczególnego pionu, który kieruje tym działem i ponosi odpowiedzialność za pracowników i prowadzone działania operacyjne. Dalej, odpowiedzialność przechodzi na kierowników określonych komórek. Kierownictwo wyższego szczebla prowadzi nadzór, nad decyzjami podjętymi przez kierowników niższego szczebla.

Funkcjonalność projektowanego systemu ZBI oparto o założenia, elementy projektu i systemu w organizacji powiązanego z podsystemami zarządzania BI. Sposób przepływu informacji w omawianych podsystemach zarządzania BI, został udoskonalony o praktyczne podejście do ochrony informacji, wskazując bezpośrednio odpowiedzialność użytkowników, za przetwarzane informacje. Przyjęto, że poziom odpowiedzialności będzie stanowił o skuteczności opracowanego projektu. Założenia projektu istotnie będą wpływać na poprawienie poziomu BI, ponadto będą bezpośrednio związane z metodami postępowania, ograniczając utratę atrybutów informacji. Proponuje się wprowadzenie do organizacji nowej polityki bezpieczeństwa dedykowanej typowo wszystkim organizacjom z branży motoryzacyjnej. Dokument polityki bezpieczeństwa, jest znany w każdej organizacji, jednak dotychczas skupiano się na elementach zabezpieczeń znanych zagrożeń występujących najczęściej, w przedsiębiorstwach z tej samej branży. Z uwagi na specyfikę informacji, jaka przepływa przez poszczególne elementy systemu w szczególności wymaga się zabezpieczenia informacji w miejscach, w których informacja powinna być ściśle chroniona np. miejscach opracowywania rysunków prototypów.

Przeprowadzone badania i otrzymane wyniki ujawniły problemy dotyczące strategicznych miejsc, w których wymagane, są dodatkowe punkty zabezpieczające.

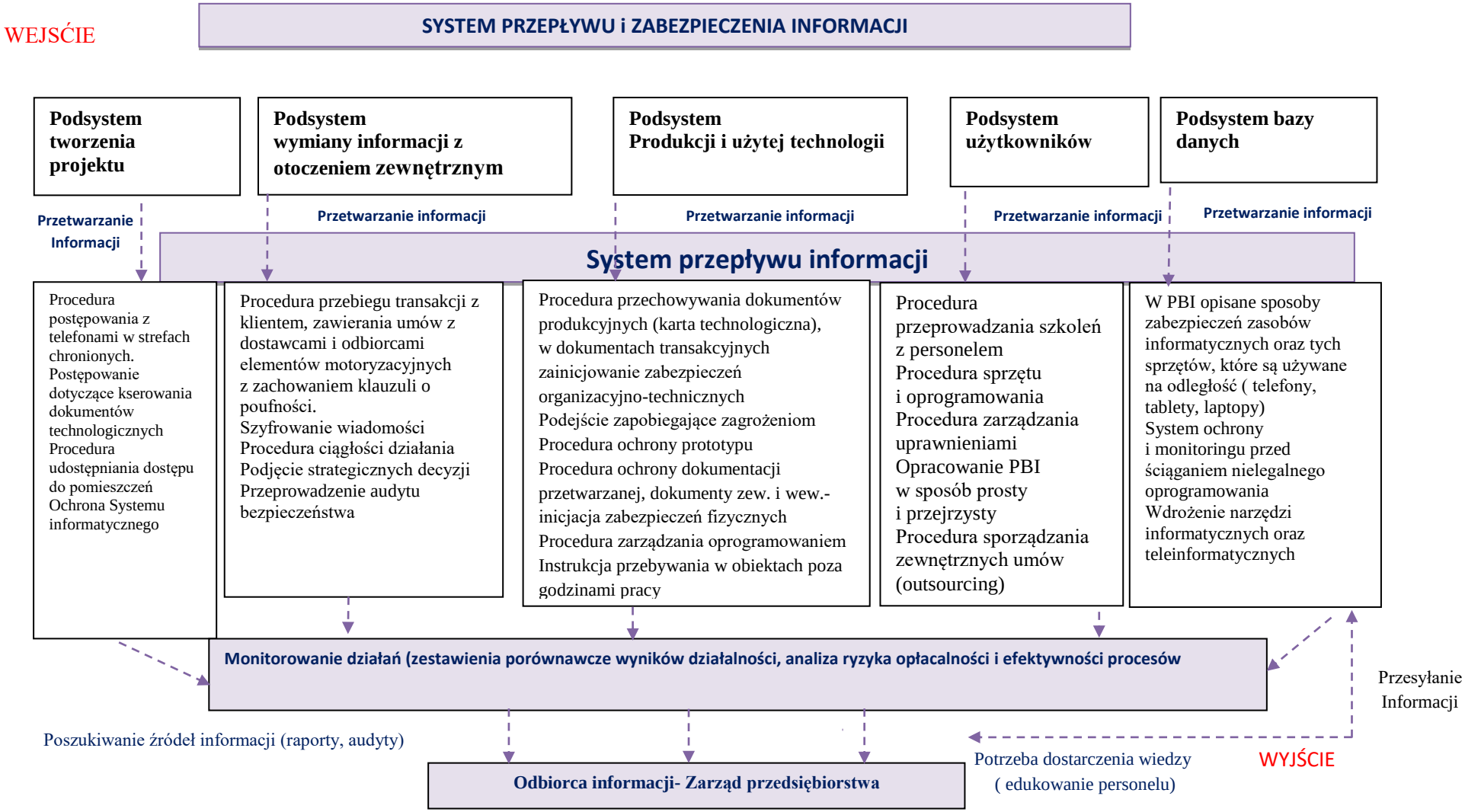
W związku z powyższym, na bazie analizy ryzyka opracowano system ochrony informacji dla branży motoryzacyjnej, który podzielono, na podsystemy powiązane z kategoriami informacji.

W systemie tym informacja występuje w następujących obszarach:

- biura projektowe, które zajmują się tworzeniem projektów prototypów, przechowujących całą dokumentację patentową;

- dostawcy komponentów, w obszarach dotyczących współpracy z dostawcami. Dostawcy przetwarzają informacje o właściwościach danego materiału, z którego zostanie wyprodukowany dany element;
- produkcji wg. stosowanych technologii. Obszar, ten został wyodrębniony z uwagi na informacje zawarte w karcie technologicznej, zawierającej informacje odnośnie danego produktu, jego powstania, aż do zakończenia procesu;
- pracowników administracyjno-biurowych;
- elektronicznych bazy danych- zbiory informacji zawartych w każdym z podsystemów. Zbiory danych, znajdujące się w systemach informatycznych przechowywanych na nośnikach elektronicznych, a zabezpieczone na serwerach własnych lub dzierżawionych. Z, takiej elektronicznej bazy danych mogą korzystać poszczególne działy, w których zawarte są informacje dokumentacyjne konieczne do zabezpieczenia.

Zaprezentowany poniżej schemat przedstawia elementy składowe podsystemów BI, które odpowiedzialne, są za zapewnienie bezpieczeństwa danych dotyczących poszczególnych informacji przetwarzanych w systemie.



Rysunek 73. Proponowany Systemu Przepływu i Zabezpieczenia Informacji

Źródło: Opracowanie własne

Na schemacie przedstawione zostały wydzielone podsystemy przepływu informacji wraz z sposobem zabezpieczenia. W branży motoryzacyjnej niezwykle istotnym czynnikiem jest sprawny obieg informacji oraz, jej przepływ pomiędzy obszarami, w których się nią zarządza. Dzięki wprowadzeniu dodatkowych procedur postępowania, poziom bezpieczeństwa znacznie się podwyższy, co przełoży się na wynik szacowania ryzyka (wykaże się tendencją malejącą). W związku z powyższym, pomocne w podejmowaniu ważnych decyzji przez zarządy będzie wsparcie systemu przepływu i zabezpieczenia informacji.

Podsystem tworzenia projektu

Zadaniem systemu jest stworzenie bezpiecznych warunków podczas tworzenia projektu oraz po jego ukończeniu. Oznacza to, zapobieganie działaniom nieuprawnionego dostępu do pomieszczeń, w których opracowywane i przechowywane są projekty. Ograniczenie dotyczy dostępu pracowników, zgodnie z ich posiadanymi uprawnieniami. Zminimalizuje to możliwość wtargnięcia osoby obcej do pomieszczeń projektowych, w których będą zastosowane zabezpieczenia fizyczne.
W podsystemie zostaną ochronione następujące zasoby materialne i niematerialne:

- rysunki prototypów, stworzone projekty, opracowane założenia do projektów, wyniki analiz i ocena projektu, modele podzespołów

Podsystem zapewni ochronę zasobów w następujących działach:

- technologicznym, badawczo-rozwojowym, zamówień, controlingu działalności badawczo-rozwojowej.

Podsystem tworzenia projektu będzie obejmował pracowników:

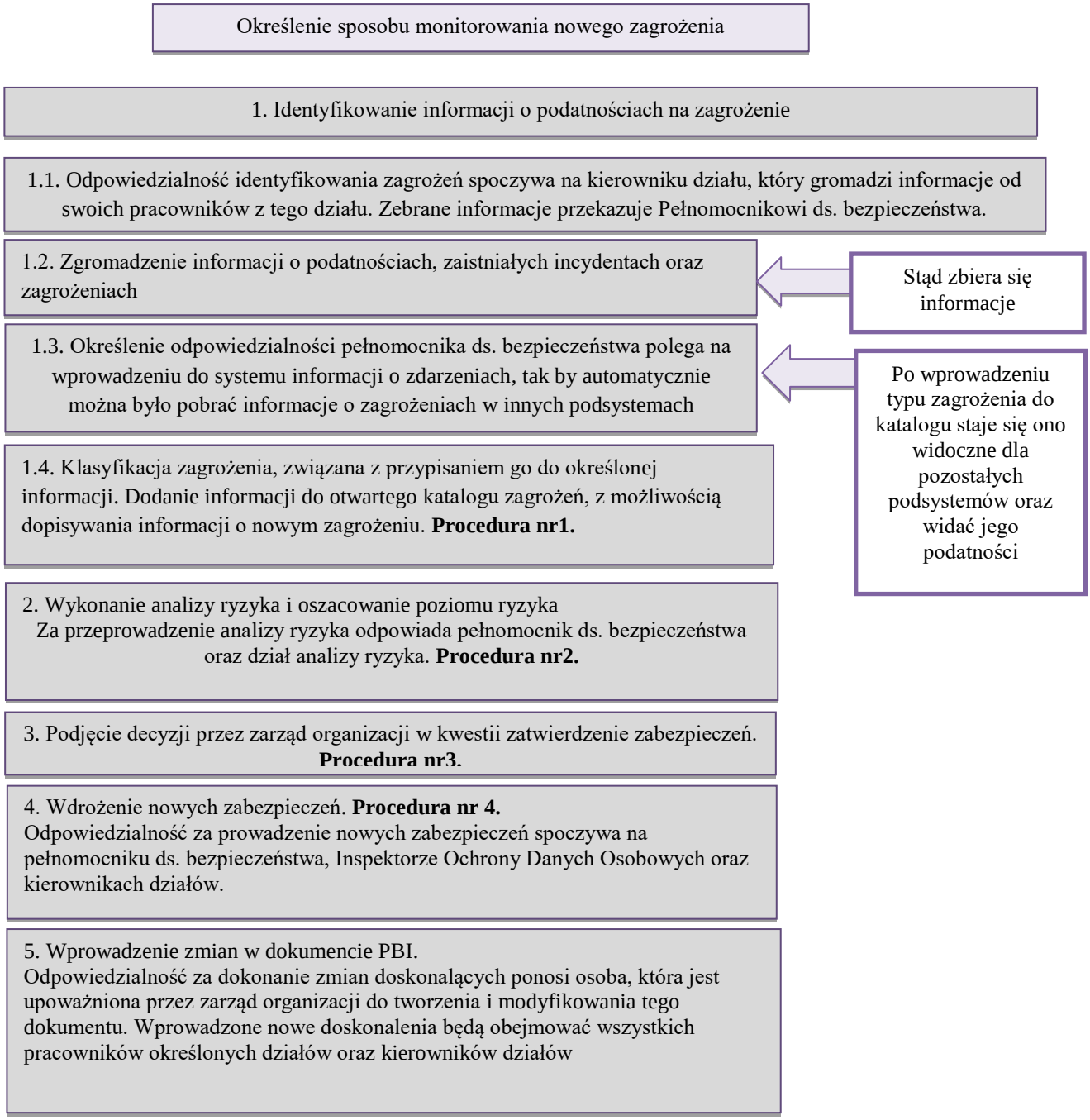
- inżynierów, specjalistów, technologów oraz zatrudnionych w dziale tworzenia projektu.

Odpowiedzialność za wdrożenie procedur podsystemu tworzenia projektu spoczywa na: dyrektorze określonej sekcji/działu/ wydziału (dyrektor wykonawczy).

Podsystem nadzorowany będzie przez dyrektora określonej sekcji /działu/ wydziału. Dział analizy ryzyka powinien przeprowadzać analizę ryzyka, związaną z utratą informacji dotyczącej projektu. Informacje przetwarzane w tym podsystemie będą wymieniane z informacjami z następujących podsystemów: wymiany informacji ze otoczeniem zewnętrznym oraz produkcji i bazy danych.

Każdy z wymienionych na rysunku 73 podsystemów będzie funkcjonował na podobnej zasadzie, jednak będzie obejmował inne grupy informacji oraz inne grupy pracowników obsługujących podsystem, co również jest związane ze zmianą odpowiedzialności za nadzór w określonym podsystemie. Zadaniem podsystemu w wyniku przedstawienia zakresu czynności dla pracowników, jest wygenerowanie nowych zabezpieczeń. System ma charakter adaptacyjny i dopasowuje się do otaczających go warunków w organizacji, posiadanych zasobów i pojawiających się zagrożeń.

Szczegółowy sposób monitorowania zagrożenia w podsystemie tworzenia projektu, oparty o poziomy odpowiedzialności pracowników przedstawiono dla na rysunku 74.



Rysunek 74. Funkcjonowanie systemu ZBI z podziałem, na wskazanie poziomu odpowiedzialności opartego o podsystem tworzenia projektu

Źródło: Opracowanie własne

Na rysunku 74 zaprezentowano schemat, wskazujący na podejście oparte o procedury, uwzględniające pracowników podejmujących decyzje. W przedstawionym systemie podzielono informacje na grupy i związane z tym procedury. Uprawnione osoby wykorzystujące, te grupy informacji przynależne do swoich sekcji zobowiązani, są by je chronić.

Podsystem wymiany informacji z otoczeniem zewnętrznym

W podsystemie chronione będą następujące zasoby typu:

- dokumenty kontraktowania surowców, dokumenty ds. towarów, usług, listy dostawców, dokumentacja techniczna, lista zakupów półproduktów i materiałów niezbędnych do produkcji pożądanego produktu, dokumentacja związana z prowadzonymi badaniami rynkowymi (rozpoznaniem sytuacji gospodarczej zbytu), składane zapytania ofertowe, formy negocjacji z klientem, sposobu magazynowania półproduktów, i wyrobów gotowych, strategie zakupowe, strategie sprzedaży, sposoby wdrażania rozwiązań innowacyjnych, wyniki przeprowadzonych audytów sprzedaży, hurtowe cenniki sprzedaży, formy sprzedaży wyrobów gotowych.

Podsystem wymiany informacji z otoczeniem zewnętrznym realizowany będzie w określonych działach:

- zaopatrzenia podzespołów, magazynu, controllingu, logistyki w obszarze działów związanych z produkcją dotyczących podzespołów, krajowego i zagranicznego, transportu.

Wytycznym podsystemu będą podlegać następujący pracownicy:

- dyrektor zakupów podzespołów, dyrektor logistyki w obszarze działań dotyczących podzespołów, dyrektor controllingu, pracownicy administracyjno-biurowi, osoby pracujące na umowie o dzieło, zlecenie, stażyści, praktykanci, serwisanci sprzętu oraz pracownicy z sekcji rozwoju, kierownicy działów handlowych, przedstawiciele handlowi, specjaliści ds. obsługi klienta.

Część informacji ochranianych w tym systemie, będzie wykorzystywana również w innych podsystemach m.in.: produkcji oraz tworzenia projektu. Zidentyfikowane i scharakteryzowane zagrożenia oraz dedykowane im zabezpieczenia będą widoczne również podczas przetwarzania tej samej grupy informacji w innych podsystemach.

Osobą odpowiedzialną za opracowanie i zastosowanie procedur w podsystemie wymiany informacji z otoczeniem zewnętrznym będzie, dyrektor wykonawczy oraz dyrektor sprzedaży.

Nadzór nad wdrożeniem podsystemu wymiany informacji z otoczeniem zewnętrznym, należy do kompetencji dyrektora ds. sprzedaży oraz jego zastępcy, jak również z-cy dyrektora ds. obsługi klienta natomiast odpowiedzialność za wdrożenie systemu będzie przeniesiona na dyrektora ds. sprzedaży (dyrektor wykonawczy).

Informacje przetwarzane w tym podsystemie będą przetwarzane również w podsystemie tworzenia projektu, produkcji i użytej technologii, użytkowników oraz bazy danych.

Podsystem produkcji i użytej technologii

Podsystem będzie zabezpieczał następujące aktywa:

- dokumenty planowania produkcji, zakup surowców, materiałów, rysunki wykorzystywanej technologii, karta technologiczna, rysunki prototypów, cele operacyjne procesów przygotowujących półprodukt-obróbka wykańczająca, montaż elementów cząsteczkowych.

Podsystem produkcji obejmuje działy:

- zaopatrzenia, controllingu procesu produkcyjnego, zamówienia, sprzedaży, magazynu.

Opracowanie wskazówek podsystemu produkcji i użytej technologii dotyczy m.in.: głównego technologa, osoby mającej dostęp do pełnej wersji szkicu prototypów, pracowników wykańczających produkty gotowe, liderów zespołów, dyrektorów zakładu produkcyjnego, kierowników produkcji.

Za zapewnienie odpowiedniego nadzoru nad wdrożeniem funkcji podsystemu odpowiedzialny jest dyrektor ds. produkcji, z-ca dyrektora ds. produkcji, główny technolog, specjalista ds. koordynacji (dyrektor wykonawczy). Również, za opracowanie i zastosowanie procedur odpowiedzialny jest dyrektor produkcji (dyrektor wykonawczy).

Za ewaluację podsystemu odpowiedzialny, jest dyrektor ds. produkcji, z-ca dyrektora ds. produkcji, główny technolog, specjalista ds. koordynacji (dyrektor wykonawczy).

Informacje przetwarzane w tym podsystemie będą przetwarzane w podsystemie tworzenia projektu, wymiany informacji ze światem zewnętrznym, użytkowników oraz bazy danych.

Podsystem użytkowników

Podsystem użytkowników będzie zabezpieczał aktywa:

- dokumentacja wewnętrzna (umowy z kontrahentami, dokumentacja dot. zastępstw), dokumenty księgowe, raporty płacowe, dokumenty polityki, sprzedażowo-marketingowej organizacji, sposoby strategii sprzedaży, komputery użytkowników, nośniki pamięci.

Podsystemowi będą podlegali pracownicy z następujących obszarów organizacji:

- księgowy, obsługa ekonomiczno- finansowa, marketing, i controlling.

Istnieje wzajemne powiązanie koordynacji zadań wynikłych z przekazywania informacji.

Podsystem użytkowników dedykowany będzie obszarom organizacji

- dział kadr i płacy, BHP, zaopatrzenia, marketingu i sprzedaży.

Za opracowanie i wdrożenie podsystemu będzie odpowiedzialny dyrektor wykonawczy. Istnieje wzajemne powiązanie koordynacji zadań wynikłych z przekazywana informacji między omawianym podsystem, a podsystemem wymiany informacji z otoczeniem zewnętrznym.

Za nadzór wdrożenia podsystemu będzie odpowiadał dyrektor sprzedaży (dyrektor wykonawczy).

Za rozwój systemu jest odpowiedzialny dyrektor sprzedaży (dyrektor wykonawczy).

Podsystem bazy danych

Do obszarów chronionych przez podsystem zaliczono materialne zasoby:

- serwerownia, stacje robocze, sieci komputerowe.

Podsystem zapobiega utracie takich zasobów jak:

- bazy danych (system zarządzania bazą danych), serwer, oprogramowanie pośredniczące, sieci teleinformatyczne, programy wspomagające zarządzanie organizacją.

Podsystem ten jest dedykowany grupie pracowników użytkującym system, w szczególności dotyczy zarówno pracowników administracyjno-biurowych, jak i kierowników wyższego szczebla.
Odpowiedzialnym za opracowanie procedur przed utratą informacji jest dyrektor IT (dyrektor wykonawczy), kierownik IT.
Osobą odpowiedzialną za wdrożenie i utrzymanie podsystemu, jest dyrektor IT oraz kierownik IT.

6.4. Przeprowadzenie ponownej analizy ryzyka

W podrozdziale 6.2. oraz 6.3. przedstawiono założenia SZBI. Dają one możliwość wygenerowania nowych, skuteczniejszych i bardziej efektywnych zabezpieczeń. Przeprowadzenie analizy ryzyka wskazało, które elementy wymagają zwiększonej ochrony, stąd też wynikła propozycja ich zaimplementowania w badanych organizacjach. W dalszej kolejności proponuje się wykonanie ponownej analizy ryzyka, na podstawie przyjętej metodologii, której celem będzie sprawdzenie skuteczności wprowadzonych rozwiązań doskonalących. Wykorzystano tę samą, 5-stopniową skalę oceny, kontynuowaną w części badawczej pracy.

W wyniku dokonania pierwotnej analizy stwierdzono stan nieakceptowalnego poziomu ryzyka występujących zagrożeń. W związku z tym, konieczne jest znalezienie i wprowadzenie działań zabezpieczających oraz dokonanie powtórnie analizy ryzyka w celu oszacowania wartości ryzyka. Należy, więc poszukać zabezpieczeń, które ogranicza wpływ występujących zagrożeń, odnosząc się do poprzednich wyników otrzymanych w wyniku analizy ryzyka.

Wprowadzenie działań doskonalących w celu zredukowania poziomu ryzyka

Przeprowadzona analiza ryzyka pozwoliła na oszacowanie poziomu ryzyka, które jest niebezpieczne dla funkcjonowania organizacji. Aby sprawdzić, czy wytypowane zabezpieczenia przypisane zagrożeniom uległy wzmocnieniu i stały się skuteczniejsze (wynik w kolejnej analizie ryzyka) należy poddać je dokładniejszemu rozważaniu, co uczynione zostanie w ponownej analizie ryzyka. Działanie kontroli i nadzorowania poziomu ryzyka zapewni komfort organizacji.

Tabela 30 prezentuje zaimplementowanie nowych mechanizmów kontroli zapobiegających zidentyfikowanym zagrożeniom. Określając nowe działania prewencyjno doskonalące przypisano w niektórych przypadkach, jedno zabezpieczenie w największym stopniu przeznaczone dla określonego zagrożenia. Wybrane zabezpieczenie w największym stopniu oddziałuje na określone zagrożenie. Spektrum wpływu zabezpieczenia jest jednak większe i w pośredni sposób może wpłynąć również na inne zagrożenia. W niektórych przypadkach do jednego zagrożenia przypisano kilka zabezpieczeń.

Wprowadzając omawiane zmiany w zabezpieczeniach zauważa się korelację między wprowadzonymi zabezpieczeniami a oszacowaniem prawdopodobieństwa wystąpienia danego zagrożenia. Zależność, ta będzie wpływać na wynik, który będzie się zmniejszał relatywnie do sposobu płynnego zainicjowania działań asekuracyjnych. W każdym przedsiębiorstwie, inaczej przebiegał będzie proces wdrożenia i będzie on uzależniony, od ilości skutecznego wprowadzenia zmian oraz reorganizacji pracy ludzi i systemów.

Analizując możliwości wprowadzenia nowych zabezpieczeń autorka pracy uwzględniła skuteczność nowych zabezpieczeń oraz ich koszty (przedsiębiorcy nie są zainteresowani nieekonomicznymi rozwiązaniami), starając się tym samym uzyskać wyraźną poprawę ochrony przed występującymi zagrożeniami, przy uwzględnieniu niskich kosztów zabezpieczenia. Tabela 30 przedstawia proponowane rozwiązania zabezpieczeń dla zidentyfikowanych zagrożeń.

Tabela 30. Określenie nowych działań prewencyjnych zmniejszających ryzyko utraty atrybutów informacji wzmacniających zabezpieczenia organizacji

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
Z.1	Ogół działań związanych z zachowaniem informacji wewnątrz przedsiębiorstwa i przeciwdziałanie ujawnieniu jej na zewnątrz.	Procedura korzystania z napędów USB. Zabezpieczanie danych poprzez blokowanie dostępu do komputera. Nawyk niszczenia dokumentów i materiałów niewykorzystywanych do pracy. Zamontowane urządzeń antypodsłuchowych w miejscach gdzie prowadzone są rozmowy biznesowe Odłączanie komputera od sieci internet, jeśli nie jest to konieczne takie połączenie. Zabezpieczenie telefonów komórkowych przed inwigilacją. Okablowanie aparatów telefonicznych pod kątem zniszczeń i przyłączeń innych urządzeń. Analizatory widma częstotliwości radiowych (pluskwy). Informacje sklasyfikowane, jako najważniejsze przechowywane w komputerach niepodłączonych do internetu.	Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem użytkowników Podsystem produkcji i użytej technologii Podsystem tworzenia projektu
Z.2	Program szkoleniowy dopasowany do wykonywanych działań w organizacji. Zwolnienia dyscyplinarne. Legalne oprogramowanie. Monitoring komputera, serwera.	Szkolenia wzbogacone o program realnych sytuacji wyłudzenia informacji, w których mogą się znaleźć pracownicy. Program szkoleń oparty o podział obowiązków oraz poczucie odpowiedzialności pracowników wobec przetwarzanych informacji i realizowanych planów bezpieczeństwa. Zaproszenie do przedsiębiorstwa socjotechnika, który w praktyczny sposób pokaże metody i techniki wykorzystywane w celu ujawnienia informacji i praktyki manipulowania zachowaniem, a w rezultacie postępowaniem pracownika. Kary dla pracowników nieprzestrzegających reguł i zasad obowiązujących w organizacji oraz pozbawienie możliwości wykonywania prac. Aktualizacja oprogramowania na urządzeniach zdalnych używanych przez pracowników. Monitorowanie pracy serwera.	Podsystem produkcji i użytej technologii Podsystem tworzenia projektu Podsystem bazy danych Podsystem użytkowników Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.3	Zlecenie usługi niszczenia dokumentów firmie zewnętrznej specjalizującej się tego typu pracami.	Zabezpieczenie dokumentacji zanim zostanie zutylizowana. Możliwość uczestnictwa podczas procesu niszczenia dokumentów. Możliwość otrzymania kopii filmu oraz protokołu zniszczenia dokumentów	Podsystem użytkowników Podsystem tworzenia projektu Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem produkcji i użytej technologii

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
Z.4	Zabezpieczenia sprzętowo-programowe.	W pomieszczeniach używanie zamków biometrycznych, posiadanie przez pracowników dokumentów lub kart magnetycznych. Automatyczne blokowanie ekranu komputera, zawsze wpisywanie hasła użytkownika. Nie pozostawianie otwartych drzwi do pomieszczeń, w których przetwarzane są informacje. Przechowywanie dysków, pendrive w sejfach, szafach metalowych.	Podsystem użytkowników Podsystem produkcji i użytej technologii
Z.5	Zakaz otwierania załączników typu zip, exe, xlsm z niewiadomego pochodzenia	W tego typu załącznikach znajdują się wirusy infekujące komputery. Wysyłając wiadomości do wielu użytkowników należy stosować opcję ukrytej wiadomości. Kasowanie nie potrzebnych wiadomości (wymagany okres przechowywania e-maili to 1 rok. E-maile z poufnymi danymi należy archaizować w innym pliku). E-mail służbowy służy wyłącznie do celów służbowych a nigdy prywatnych. Zakaz wysyłania poufnych informacji z prywatnej skrzynki pocztowej. Sprawdzanie adresu odbiorcy w celu uniknięcia pomyłki adresata.	Podsystem użytkowników Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.6	Stworzenie Polityki Bezpieczeństwa Informacji gdzie w sposób zrozumiały i jasny będą przedstawione procedury postępowania.	Opracowanie rozwiązań obejmujących całość zasad dotyczących obiegu dokumentów, szybkiej identyfikacji osób, dostępu do pomieszczeń, reagowania na incydenty, itp. Wprowadzenie zapisów odpowiedzialności powiązanych z kompetencjami pracowników. Cykliczne aktualizowanie dokumentu PBI, dopasowując zmiany do potrzeb organizacji.	Podsystem użytkowników Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem tworzenia projektu Podsystem produkcji i użytej technologii
Z.7	Podejmowanie działań służących zapewnieniu zabezpieczenia fizycznego budynku (system włamania i napadu).	Zainstalowanie czujników ruchu, otwierania okien i drzwi, wykrywające poruszanie się. Zamontowanie dodatkowych zabezpieczeń w miejscach strategicznych, w których przetwarzane są informacje (okna z zamontowanymi kratami) Drzwi antywłamaniowe klasy 5,6 wyposażone w zamek centralny, antywłamaniowy, stalowa ościeżnica). W miejscach, w których można podejrzeć informacje stosuje się żaluzje, szyby matowe, rolety. Oświetlenie chronionego obszaru przedsiębiorstwa. Mechanizmy zabezpieczające powinny ze sobą współpracować i uzupełniać się. Szyby o zwiększonej odporności na rozbicie (01-02 P1-P8).	Podsystem produkcji i użytej technologii Podsystem użytkowników
Z.8	Polityka zapewnienia kompetencji i wiedzy pracowników, co do	Czynniki skoncentrowane na zapewnieniu ciągłości wiedzy, co do zasobów, które pozostają pod kontrolą użytkowników. W budżecie organizacji przeznaczanie środków finansowych na programy szkoleniowe.	Podsystem produkcji i użytej technologii Podsystem tworzenia

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
	gromadzonych zasobów w organizacji oraz wskazywania na poczucie współodpowiedzialności za powierzone aktywa informacyjne i zrealizowanie wytycznych w PBI. Ciągłe podtrzymywanie świadomości personelu, rozwijając motywację wewnętrzną.	Cykliczne edukowanie pracowników fizycznych, biurowych, stażystów, doktorantów, członków zarządu, dyrektorów, kierowników niższego szczebla, i nie kierowników, partnerów, kontrahentów, nie zapominając o tych czasowo pracujących, nie rzadziej niż raz na pół roku. Tematyczne programy szkoleń. System weryfikujący wiedzę pracowników.	projektu Podsystem bazy danych Podsystem użytkowników Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.9	Rejestr pobrań kluczy. Obecność na szkoleniach.	Opracowanie nowych procedur i zaleceń dotyczących dostępu osób postronnych do budynku, pomieszczeń biurowych. Opracowanie zaleceń postępowania wobec nowych osób w organizacji. Eskortowanie ich po organizacji zmniejszyłoby prawdopodobieństwo wystąpienia zagrożenia. Podczas szkoleń warto wprowadzić ewidencje obecności w celu nadzoru czy wszystkie grupy pracownicze uczestniczyły w programie edukacyjnym.	Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.10	Kontrola dostępu do systemu.	Uwierzytelnienie SYK, SYH, SYA, SYD,	Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.11	Wskazanie w organizacji na jedną osobę, odpowiedzialną za obowiązki Inspektora Ochrony Danych Osobowych lub korzystanie z firmy zewnętrznej świadczącej usługi w tym zakresie.	Osoba wykonująca obowiązki Inspektora Ochrony Danych Osobowych nie może wykonywać innych czynności związanych z czynnościami etatowymi. Zadaniem IODO jest pilnowanie porządku w dokumentacji RODO, przestrzeganie reguł i zasad bezpieczeństwa przechowywanych danych osobowych.	Podsystem użytkowników
Z.12	Opracowanie ogółu procedur służących ochronie tajemnicy przedsiębiorstwa	Wdrożenie postępowania karnego dla osoby, która ujawni tajemnicę przedsiębiorstwa (określając wysokość kary). W umowach należy ustalić okres ochrony tajemnicy (czas nieokreślony czy określony), jakie informacje należy chronić, kategorie informacji. Określenie,	Podsystem wymiany informacji z otoczeniem zewnętrznym

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
	zapewniając tym samym poufność informacji. Wytyczne i reguły do opracowania umowy o zachowaniu poufności.	w jakim zakresie i na jakich zasadach informacje poufne mogą być ujawnione innym. Określenie postępowania, kiedy już umowa przestanie obowiązywać, (w jaki sposób zniszczyć dokumenty lub też jak je zwrócić). Zbyt ogólnie napisana umowa utrudnia przestrzeganie jej reguł. Ciągłe szkolenia znacznie podnoszą świadomość pracowników w kierunku odpowiedniego sporządzania umów. Zaplanowanie programu szkoleń spowoduje poznanie osoby odpowiedzialnej za wprowadzanie zasad doskonalących SZBI w organizacji oraz uwzględnienie w postępowaniu wymogów proponowanych w RODO.	Podsystem użytkowników
Z.13	Procedury utrzymania generatorów sieciowych. Zakup UPS-u potwierdzonych certyfikatem.	Sprawdzenie czy urządzenia produkujące prąd są na bieżąco ładowane i zawsze gotowe do pracy. Czas reakcji urządzenia po włączeniu powinien być jak najkrótszy. Odłączenie komputera od sieci internetu, jeśli go nie potrzebujemy. Takim działaniem skraca się czas, w którym komputer jest narażony na ryzyko utraty informacji lub zainfekowanie wirusem.	Podsystem bazy danych Podsystem użytkowników Podsystem produkcji i użytej technologii Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem tworzenia projektu
Z.14	Czynniki obejmujące bezpieczeństwo przeciwpożarowe. Monitorowanie pracy firm zewnętrznych, z którymi jest nawiązana współpraca.	Plan postępowania odnośnie zniszczenia zasobu wynikającego z jego spalenia czy zalania. Plan postępowania w sytuacji bezpośredniego zagrożenia organizacji. Pomocny monitoring wizyjny. Kontrolowanie pracy firm outsourcingowych wykonujących zlecenie informatyczne, dostawcy oprogramowania na serwerach i komputerach organizacji.	Podsystem bazy danych Podsystem użytkowników Podsystem produkcji i użytej technologii Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem tworzenia projektu
Z.15	System szyfrowania.	Szyfrowanie urządzeń przenośnych. W czasie podróży należy zapewnić bezpieczeństwo dyskom twardym, pamięci flash, pendrive, płytom CD/DVD, laptopom i telefonom. Szyfrowanie programowe typu McAffee, Sophos –w wyniku oprogramowania szyfrującego nie można uzyskać dostępu do danych, jak tylko przez komputer oryginalnie został zaszyfrowany.	Podsystem bazy danych Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem użytkowników

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
Z.16	Ograniczenie uprawnień pracownikom (którym należy stopniowo zwiększać uprawnienia i przywileje).	Zbyt wysokie poziomy uprawnień nadane użytkownikom, którzy nie powinni mieć dostępu do ogółu informacji. Nadawanie uprawnień stosownych do nabytej wiedzy i koniecznych potrzeb w celu pełnienia obowiązków służbowych (weryfikowanie statusu pracownika).	Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem użytkowników
Z.17	Fizyczne i programowe mechanizmy blokowania dostępu do pomieszczeń, a w nich urządzeń osobom nieuprawnionym.	Ogół rozwiązań blokowania dostępu do zasobów. Pracownik zobowiązany jest do nie ujawniania informacji osobom trzecim tzn. klientom, użytkownikom z innych działów. Po zakończeniu pracy należy wylogować się z systemu. Nie należy instalować żadnych aplikacji, programów bez zgody zarządu czy działu IT.	Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.18	Stworzenie w organizacji stref ochronnych, do których ma dostęp tylko dyrekcja i zarząd. Monitoring aktualnych uprawnień.	Podejmowanie strategicznych decyzji w przeznaczonych do tego strefach ochronnych. W strefach ochronnych powinny być bariery fizyczne ograniczające dostęp tylko dla upoważnionych osób. Natychmiastowe blokowanie dostępu użytkownikom, którzy nie posiadają aktualnych uprawnień. Wdrożenie procedury dotyczącej ewidencjonowania aktualnych uprawnień dla pracowników oraz już tych utraconych. Takie działanie wspomaga kontrolę nad bieżącą sytuacją w firmie.	Podsystem produkcji i użytej technologii Podsystem tworzenia projektu Podsystem bazy danych Podsystem wymiany informacji z otoczeniem zewnętrznym
Z.19	Procedury serwisowania sprzętu. Zabezpieczenie komputera przed wirusami, aktualizowanie oprogramowania.	Warunki serwisowania sprzętu przez podmioty zewnętrzne tak, aby nie utracić poufności danych zawartych w powierzonym urządzeniu. Urządzenia teleinformatyczne podlegające konserwacji tylko przez uprawnionych pracowników (informatyków) lub komórki organizacyjne. Jeśli na urządzeniu znajdują się informacje wrażliwe sprzęt taki powinien być naprawiony pod nadzorem osoby posiadającej uprawnienia do takich operacji. Prowadzenie rejestru zasobów w celu identyfikacji historii urządzenia. Archiwizowanie informacji w komputerach, które stanowią integralną część urządzeń teleinformatycznych przekazywanych do konserwacji. Korzystanie z urządzeń komputerowych potwierdzonych certyfikatem i atestem. Unikanie korzystania ze stron z nielegalnym oprogramowaniem (filmy, muzyki). Używanie bezpiecznych przeglądarek.	Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem tworzenia projektu
Z.20	Procedury serwisowania i utrzymania	Procedury serwisowania oprogramowania przez podmioty zewnętrzne tak, aby nie utracić poufności dokumentów zapisanych na dyskach oraz zapewnić ciągłość działania w organizacji.	Podsystem wymiany informacji z otoczeniem

L.p. zagrożenia	Propozycja nowych środków ochronno - zapobiegawczych	Opis	Podsystem zarządzania BI
	oprogramowania Zabezpieczenia IT (programy do monitoringu i kontroli komputerów oraz serwerów)	Programy do monitorowania aktywności komputerów i serwerów, dzięki którym zabezpieczone są informacje firmowe (oprogramowanie pomaga w monitorowaniu i nagrywaniu pracy użytkownika w systemie, zarządza urządzeniami USB, przerywa sesje niebezpieczne oraz blokuje system w momencie próby wyłudzenia informacji). Dział IT ma wgląd w działania prowadzone na komputerze użytkownika. Kryptograficzna ochrona danych przez szyfrowanie oddzielne nośnika (Mcafee, Sophos).	zewnętrznym Podsystem tworzenia projektu Podsystem bazy danych
Z.21	Możliwie jak najszybsze alarmowanie o zagrożeniach Narzędzia monitorujące kluczowe parametry oprogramowania ds. wielkości przesyłanych plików, zużycia zasobów, wielkości bazy danych.	Zachęca się pracowników do przezwyciężania strachu, przed ujawnieniem swojego udziału w naruszeniu i jak najszybsze zgłoszenie incydentu przełożonemu (kierownikowi, dyrektorowi). Fizyczne, programowe mechanizmy blokowania dostępu do przetwarzanych treści. Działania niedopuszczające do skanowania. Śledzenie przesyłanych, masowych treści. Zakaz samodzielnego przyłączania się do komputerów, modemów, telefonów. Zakaz łączenia tych urządzeń z internetem. Zakaz ujawniania haseł innym osobom. Zablokowanie pracy użytkownika bez możliwości ponownego zalogowania się.	Podsystem tworzenia projektu Podsystem bazy danych Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem produkcji i użytej technologii Podsystem użytkowników
Z.22	Certyfikaty bezpieczeństwa	Wymagania dotyczące certyfikatów bezpieczeństwa od dostawców usług oraz certyfikaty urządzeń, na których pracują dostawcy. Zaleca się, aby osoby sporządzające umowy znały przepisy obowiązującego prawa, ustaw i rozporządzeń regulujące status prowadzenia działalności gospodarczej. Przedsiębiorstwa, które nie wdrożyły wszystkich standardów tracą czas na opracowanie zasad postępowania, podczas gdy należy skupić uwagę na czynnikach przyczyniających się do bezpiecznego rozwoju organizacji. Zaleca się prowadzenie rejestru organizacji, z którymi zawarte zostały umowy (program do monitorowania komputera i serwera).	Podsystem tworzenia projektu Podsystem bazy danych Podsystem wymiany informacji z otoczeniem zewnętrznym Podsystem produkcji i użytej technologii Podsystem użytkowników
Z.23	System szyfrowania (zabezpieczenia IT) Kontrolowanie pracy firm outsourcingowych, z którymi jest podpisana współpraca	Szyfrowanie dokumentów, aby zawartość ich była nieczytelna dla nieuprawnionych osób. Telefony, smartfony, tablety zabezpieczone hasłem, PIN-em, kodem autoryzującymi dostęp do zawartych informacji. Sprawdzanie działań firm zewnętrznych, z którymi organizacja współpracuje na serwerach i komputerach.	Podsystem bazy danych Podsystem wymiany informacji z otoczeniem zewnętrznym

W celach badawczych przyjęto założenie, zmniejszenia wpływu zagrożeń, poprzez wdrożenie nowych działań korygujących oraz rozszerzenie już tych sprawnych o dodatkowe spektrum działania ochraniającego organizację. Takie działanie powoduje wzrost zabezpieczenia oraz jego wartości liczbowej.

W celu procesu inicjacji środków doskonalących, należy skorzystać z możliwych do wprowadzenia zabezpieczeń, które dotychczas nie zostały wdrożone. Zatem powiększy się ich ilość, dzięki czemu będzie można oszacować poziom zabezpieczeń.

Dla przykładu podano schemat wyliczenia wartości numerycznych przypisanych poszczególnym zagrożeniom oraz ich asekuracyjnym zabezpieczeniom.
Dla 7-go zagrożenia w katalogu zagrożeń wstępuje 7 różnych zabezpieczeń. Dotychczas skorzystano z 6-ciu możliwych opcji, co stanowi 86% pełnego katalogu zabezpieczeń. Dodając jeszcze jedno zabezpieczenie (podejmowanie działań służących zapewnieniu zabezpieczenia fizycznego budynku, wartość zabezpieczenia wzrosła o 14%. Dzięki, takiemu działaniu skorzystano z 7-miu zabezpieczeń, wykorzystując 100% z możliwych dostępnych opcji. W pierwotnej analizie ryzyka zabezpieczenie uzyskało wartość 2,7. Zatem korzystając z nowego zabezpieczenia, uzyskujemy wartość 4,1. Taki też wynik wpisano w tabelę 31.

W celach badawczych autorka pracy zmitygowała wpływ zagrożeń, poprzez wdrożenie nowych działań korygująco-doskonalących oraz rozszerzenia, już tych sprawnych o dodatkowe spektrum działania zabezpieczającego organizację, zmniejszając tym samym prawdopodobieństwo, którego wartość liczbowa dotychczas wynosiła 1,5. Powiększając wynik o wartość wprowadzonego zabezpieczenia (14%) do wartości wykorzystywanych dotychczas zabezpieczeń (86%) uzyskano wartość prawdopodobieństwa 0,2. Po wprowadzeniu nowych zabezpieczeń wartość prawdopodobieństwa zmalała o 0,2 i wyniosła 1,3. Taką, też wartość zastała wprowadzona. Natomiast ocenę parametru skutku stanu bezpieczeństwa informacji w badanych organizacjach pozostawiono bez zmian, gdyż efekt wystąpienia zagrożenia będzie taki sam, jak pierwotnie, (czyli wartość 4,1 utrzymuje się). Dla skorygowanych otrzymanych wartości liczbowych zabezpieczeń dokonano powtórnej analizy ryzyka. Wartości liczbowe zabezpieczeń umieszczono w miejsca mapowania zagrożeń wg. kolejności przyjętej w analizie ryzyka.

Waga danych ma charakter szacunkowy ustalony przez autorkę pracy, który wynosił 4,6. Wynika, to z rozmów z pracownikami w przeprowadzonym wywiadzie oraz obserwacji warunków panujących w organizacji. Przyjęta waga oraz kryteria nie ulegają zmianie w stosunku do pierwotnie przeprowadzonej analizy ryzyka.

Wyniki z ponownej analizy ryzyka zaprezentowano w tabeli 31.

Tabela 31. Uzyskane wyniki badań z powtórnej analizy ryzyka

Ryzyko	Waga	Prawdopodo-bieństwo	Skutek	Ocena zabezpieczeń	Ocena ryzyka	Wskazanie poziomu akceptacji ryzyka
Poufność((nieuprawniony dostęp)	4,6	1,2	3,7	4,1	5,0 (4,6x1,2x3,7 :4,1)	Średnie
Integralność (modyfikacja)	4,6	1,2	3,7	3,9	5,2	Średnie
Dostępność (utrata)	4,6	1,2	3,7	4,3	4,7	Średnie
Niezawodność	4,6	1,5	3,7	5,2	4,9	Średnie
Autentyczność (ujawnienie)	4,6	1,3	3,7	4,5	4,9	Średnie
Rozliczalność (zniszczenie)	4,6	1,1	3,7	4,3	4,3	Średnie

Źródło: Opracowanie własne na podstawie przeprowadzonych badań

Dokonanie analizy porównawczej wskazuje na znaczne zmiany wartości parametrów zabezpieczenia oraz prawdopodobieństwa wystąpienia zagrożenia. Zauważając obniżenie wartości ryzyka w stosunku do bieżącego stanu w organizacjach zmieniła się jego akceptacja we wszystkich atrybutach bezpieczeństwa informacji z wartości wysokiego ryzyka do poziomu średniego (wg. kryteriów przyjętych w tabeli 28. Gradacja ryzyka). Zmiana poziomu ryzyka wysokiego do poziomu średniego w istotny sposób wpłynie na zachowanie bezpieczeństwa w organizacjach. W tym miejscu należy zauważyć, iż analiza ryzyka wskazuje na dalsze działania w kierunku obniżenia poziomu, do stanu akceptowalnego. Wymaga to wprowadzania dalszych zmian ukierunkowanych, na reorganizowanie działań pracowników oraz wspomagania informatycznego, powiązanego ze szkoleniem kadry zarządzającej. Rekomenduje się systematyczne podejmowanie działań w kierunku obniżenia wartości ryzyka do poziomu niskiego.

Rysunek 75. Określenie korelacji między danymi liczbowymi z przed i po wprowadzeniu działań ochronno - naprawczych skutkujących redukcją ryzyka
Źródło: Opracowanie własne

Z przeprowadzonych badań oraz otrzymanych wyników przedstawionych w tabelach 27 oraz 31, wynikają znaczne różnice w ocenie ryzyka, gdzie zauważono faktyczne i znaczące zmiany. Rysunek nr 75 wskazuje zmiany we wszystkich przypadkach atrybutów bezpieczeństwa. Uściślając, zauważono redukcje ryzyka dla poziomu poufności z wartości 9,1 na 5, integralności z 10,2 na 5,2, dostępności z 10 na 4,7. Niewątpliwie zaobserwowano również tendencję zmiany ryzyka dla niezawodności z 10,0 na 4,9, autentyczności z 9,3 na 4,9 oraz rozliczalności z 9,4 na 4,3. Analiza ryzyka została przeprowadzona przy poprawnie przyjętej metodyce i odpowiednim oszacowaniu skutków zagrożeń. Z tego też powodu, zaproponowana skuteczność elementów doskonaląco- naprawczych będzie zadawalać przedsiębiorców.

Przedstawiona propozycja zabezpieczeń nie musi być w pełni wprowadzona, jednak w zaistniałej sytuacji, wdrażając do organizacji wybrane asekuracyjne działania, które znacząco wpłyną na zmitygowanie ryzyka do poziomu akceptowalnego.

PODSUMOWANIE

Z uwagi na to, że zasoby informacyjne przedstawiają wartość dla przedsiębiorstwa wymagają zapewnienia im należytej ochrony. Nie jest to związane z jednorazowym zabiegiem, lecz ciągłymi staraniami opartymi o nowoczesne techniki, metody, narzędzia w pełni odpowiadające potencjalnym zagrożeniom. Zatem, wymaga się wprowadzenia działań wspomagających bezpieczeństwo informacji oraz systematyczne i dokładne monitorowanie pojawiających się coraz to nowszych form zagrożeń.

Wzrost świadomości znaczenia informacji i sposobów i jej ochrony ma swoje odzwierciedlenie w rozwoju standardów normatywnych, dedykowanych systemom zarządzania bezpieczeństwem informacji. W normach określone zostały zabezpieczenia fizyczne, techniczne, teleinformatyczne, prawne, organizacyjno-administracyjne, lecz nie określono szczegółowych rozwiązań postępowania z ryzykiem, a później zarządzania nim. Obfitość różnych standardów, rozporządzeń, ram prywatności, ustaw, aktów normatywnych powoduje, że przedsiębiorcy nie wiedzą, gdzie ich szukać oraz czy dane wymagania prawne są jeszcze aktualne, czy już wycofane i zastąpione innymi. Ze względu na dynamikę powstawania nowych zagrożeń w krótkim czasie, dezaktywują się wymagania normatywne i konieczne jest ich uzupełnianie.

W wyniku przeprowadzenia analizy literatury oraz badań empirycznych zrealizowano cel dysertacji, poprzez wskazanie nowych zagrożeń i koncepcji postępowania w systemie zarządzania bezpieczeństwem informacji. Wyeksponowano znaczenie i rolę informacji w przedsiębiorstwach, pokazano sposób jej ochrony, z uwzględnieniem wyników analizy ryzyka. W pracy wskazano podsystemy przepływu i zabezpieczenia informacji oraz zaproponowano projekt systemu zmniejszenia ryzyka wdrażający działania doskonalące.

Skorzystanie z narzędzi analizy (badanie ankietowe, wywiad, obserwacja oraz eksperyment) pozwoliło na wskazanie wielu luk w systemie bezpieczeństwa informacji. Dokonano taksonomii źródeł zagrożeń z zgodnie z metodą 5M, która obejmowała następujące kryteria: człowiek (personel), kierownictwo (zarządzanie), otoczenie (osoby trzecie), maszyna (systemy komputerowe, systemy bezpieczeństwa) oraz materiał (metodę). Zastosowany podział wskazał miejsca w organizacjach, w których niewystarczający sposób zabezpieczono informacje oraz w szczególny sposób podatne na urzeczywistnienie się zagrożenia.

Elementy wpływające na zmaterializowanie się zagrożenia i pojawienie się go w organizacjach mogą być w bardzo różne. Jednak do najważniejszych z nich zaliczono: niezabezpieczone dokumenty, brak regularności w dokonywaniu analizy ryzyka, nikły poziom wiedzy w kierunku samego procesu jej przeprowadzania. Ponadto, badania wskazały, że organizacje nie wyznaczają osób odpowiedzialnych za zarządzanie ryzykiem, tak by utrzymywać poziom ryzyka utraty bądź ujawnienia informacji. Również w części z badanych organizacji zauważa, się niedbałe podejście do zabezpieczeń fizycznych m.in.: brak barier fizycznych, które są potrzebne w celu wydzielenia ochranianych stref bezpieczeństwa. Nie bez znaczenia jest też brak umieszczenia informacji o zakazie filmowania oraz robienia zdjęć w omawianych strefach. Ktokolwiek w sposób nieświadomy dokonuje nadużycia, może ujawnić informacje przechowywane w organizacjach.

Również w zachowaniu pracowników nie zauważono ostrożności, np. podczas przyjmowania osób postronnych w organizacji. Zatem, niewystarczające jest nabycie wiedzy o zasadach postępowania podczas przyjmowania gości, lecz kształtowanie świadomości w programach szkoleń, co do zagrożeń, jakie mogą powodować tego rodzaju sytuacje. Poważnym ujawnionym problemem jest też użytkowanie internetu w czasie pracy w celach innych niż tego wymagają obowiązki służbowe (np. korzystanie z portali społecznościowych) oraz wykorzystywanie telefonów służbowych w celach prywatnych lub też pożyczanie urządzeń innym pracownikom. Takie sytuacje mogą utrudniać prowadzenie działalności gospodarczej, lecz zapewniają ochronę informacji oraz utrzymanie ryzyka na odpowiednio niskim poziomie.

Dopuszczenie do wystąpienia sytuacji, w której zostaje ukradziony sprzęt komputerowy, telefon służbowy stanowi istotne źródło zagrożenia ujawnienia informacji.

Uwagę przykuwają również urządzenia takie jak: drukarka, tablet, telefon służbowy niezabezpieczone odpowiednim specjalistycznym oprogramowaniem. Działania takie, są przejawem nieznajomości zasad ochrony informacji oraz brakiem świadomości kadry zarządzającej o możliwości pojawienia się nieodwracalnych skutków. Kolejnym źródłem zagrożeń jest brak klauzul o zachowaniu poufności w umowach z partnerami handlowymi.

Zauważyć można, zatem że znajomość reguł bezpieczeństwa i procedur postępowania, nie idzie w parze z ich zastosowaniem. Eksperyment wykazał przypadek ujawnienia przez pracownika firmy istotnych informacji osobnie niezweryfikowanej.

Ponadto, inną sytuacją wywołującą podatność ujawnienia informacji było pobranie załącznika z poczty e-mailowej od podejrzanego nadawcy. 15% respondentów pobrało i otworzyło załącznik umieszczony w wiadomości e-mailowej. Zdarzenie takie, świadczy o braku skuteczności proponowanych szkoleń dla pracowników.

Innym elementem, potwierdzającym słabe miejsce w organizacji, jest brak dopasowanego programu szkoleń w zakresie bezpieczeństwa informacji do zleconych obowiązków pracowników. Ponadto organizacje nie przywiązują wagi, do zatrudniania na stanowisku Inspektora Ochrony Danych Osobowych odpowiednio wyszkolonych osób. Często zdarza się, że funkcje IODO powierza się przypadkowemu pracownikowi. Zidentyfikowanie tak dużej ilości newralgicznych słabych miejsc, w organizacjach doprowadziło do przeanalizowania ich wpływu na pożądany i wymagany akceptowalny poziom bezpieczeństwa informacji.

W wyniku weryfikacji istniejącego stanu faktycznego w badanych przedsiębiorstwach okazało się, że poziom ryzyka utrzymywał się na wysokim poziomie, co wymagało wprowadzenia działań korygujących.

To zarządy organizacji powinny zabiegać, o to żeby kadra pracownicza otrzymała wszelką wiedzę dotyczącą należytego przechowywania informacji w organizacji. Ważnym jest, aby program szkoleń dopasowany był do potrzeb pracowników i w praktyczny sposób przedstawiał metody, techniki oraz narzędzia wykorzystywane do wyłudzania informacji przez socjotechników. Niezwykle istotną kwestią w podnoszeniu świadomości pracowników, jest objęcie takim programem wszystkich osób w organizacji, od członków zarządu po pracowników produkcji. Takie podejście może zapewnić większy poziom ochrony podczas wystąpienia zagrożenia. Wymienione elementy, są kluczowe z punktu widzenia ochrony organizacji przed wpływem zagrożenia, jednak badając organizacje takiego podejścia nie zauważono.

Na bazie, tak zidentyfikowanych zagrożeń i ich wpływu na poszczególne obszary przetwarzania informacji oszacowano wartość ryzyka oraz przedstawiono sposoby postępowania z nim. Wyprzedzenie wystąpienia zagrożenia, w znacznym stopniu przełoży się na odpowiednie przygotowanie organizacji na jego pojawienie i kompleksową ochronę. Stwierdzono zależność między stanem obecnym w przedsiębiorstwach, a możliwością jego poprawy poprzez wprowadzenie nowych środków naprawczych. Zależność pomiędzy czynnikiem prawdopodobieństwa wystąpienia zagrożenia, a wartością zabezpieczenia okazała się kluczem do zbadania skuteczności zabezpieczeń.

Skrupulatna i wnikliwa analiza ryzyka wpływa na zapewnienie odpowiednio wysokiego poziomu bezpieczeństwa informacji.

Wartość ryzyka oszacowana, na podstawie analizy ryzyka oparto o zaimplementowanie kluczowych atrybutów bezpieczeństwa informacji, jakimi są: poufność, integralność, dostępność, rozliczalność, autentyczność, niezawodność (rekomendowane przez standard ISO/IEC 27002:2017). W metodzie analizy ryzyka uwzględniono wagę informacji, która w istotny sposób przełożyła się na poziom ryzyka. Użyta metodyka wpłynęła na obiektywizm, wiarygodność i rzetelność otrzymanych wyników obliczeń, co ma swoje odzwierciedlenie w lepszym, bardziej dopasowanym doborze proponowanych zabezpieczeń. Dzięki oszacowaniu wartości ryzyka stwierdzono, na których zabezpieczeniach należy się koncentrować, obserwując zależności wagi informacji do wzrostu poziomu zabezpieczeń.

Nie każdą informację traktuje się jednakowo. Jedna informacja ma większą wagę od innej. Na podstawie przyjętej klasyfikacji informacji rozpoznaje się, do której grupy powinna ona przynależeć. Zatem, przekłada się to na ilość zastosowanych zabezpieczeń, a w konsekwencji na poziom ryzyka. Ponadto dzięki temu, że w analizie ryzyka wydzielono wagę informacji bardziej kompleksowo można ocenić skutek wystąpienia zagrożenia, co z kolei ma kluczowe znaczenie dla świadomości przedsiębiorców.

W pracy określono, które informacje są najważniejsze z punktu widzenia przedsiębiorstwa wskazując, na obszary z katalogu informacji. Pozwoliło to na skatalogowanie informacji w obszarach podsystemów, w których generowane są kluczowe informacje. Zwrócono uwagę, na rozróżnienie informacji, gdzie szczególną ochroną należy objąć te, odznaczające się większą podatnością na ujawnienie i to właśnie one są kluczowe ze względu na rodzaj i charakter prowadzonej działalności. Takie nowatorskie podejście, nabiera szczególnego znaczenia podczas dokładnego klasyfikowania informacji i dobrania odpowiednio skutecznych zabezpieczeń. Szczególnie istotnym z punktu widzenia BI, jest podsystem tworzenia projektu oraz produkcji i użytej technologii, gdzie informacje tam występujące powinny być chroniona bardziej niż w innych miejscach. Omawiane podsystemy, są najbardziej związane z branżą motoryzacyjną i niosą największą nowość z punktu bezpieczeństwa informacji.

Wysoki priorytet ochrony powinny mieć rysunki prototypu, które podlegać będą większej ochronie niż inne grupy informacji.

Bezpieczeństwo informacji również wpływa, na jakość gotowego produktu i bezpieczeństwo użytkowników. Jakość informacji nie może być dostępna i nie może ulec modyfikacji poprzez nieuprawniony dostęp. Taka manipulacja może wypływać na proces produkcyjny lub tworzenia prototypu.

W procesie analizy ryzyka stworzono nowy katalog zgrupowanych zagrożeń, który istotnie wpływa na przedsiębiorstwo i kreuje wartość ryzyka. Katalog ten jest uniwersalny i nadal otwarty, a występujące w nim zagrożenia mogą również pojawić się w innych przedsiębiorstwach. Przyjęta w ten sposób metodologia sprowadza się do określenia czy poziom ryzyka jest akceptowalny, czy też nie oraz dalszego sposobu postępowania z nim.

W tym względzie ważnym jest zwrócenie uwagi na zaaplikowanie systemu zmniejszenia ryzyka utraty informacji, opartego o uwarunkowania i strukturę organizacji. Ten zbiór dokładnych, starannych i czytelnych zasad postępowania, zgodnych z aktualnym prawem daje możliwość zarządzania systemem, procesami, dokumentami, operacjami, podsystemami tak by wspomagać rozwój zarządzania przedsiębiorstwem.

Uwzględniając budowę systemu zarządzania bezpieczeństwem informacji, w pracy przedstawiono projekt, redukujący ryzyko utraty informacji. Koncepcja projektu będzie pomocą w szybszym identyfikowaniu zagrożeń oraz sytuacji potencjalnie zagrażających organizacji. Ponadto, wskazanie zakresu odpowiedzialności za przetwarzanie i przechowywanie informacji spowoduje określenie osób współodpowiedzialnych za jej ochronę. Przedstawiony w pracy projekt, składa się z następujących podsystemów: bezpieczeństwa tworzenia projektu, wymiany informacji z otoczeniem zewnętrznym, produkcji i użytej technologii, użytkowników oraz bazy danych. Pomimo, że badania były przeprowadzone w dziewięciu przedsiębiorstwach z branży motoryzacyjnej, to jednak projekt jest na tyle uniwersalny, że może być wykorzystywany w innych przedsiębiorstwach, o podobnej strukturze i wielkości. Dzięki wprowadzeniu zbioru procedur postępowania, zarządy organizacji będą mogły podejmować strategiczne decyzje, stwarzające warunki efektywniejszego zarządzania procesami biznesowymi, bez obawy o ujawnienie swoich aktywów. W pracy odwzorowano schematy systemowego postępowania w postaci procedur, tak by ułatwić identyfikowanie zagrożeń i szybsze reagowanie na pojawiające się incydenty.

W pracy przeprowadzono powtórną analizę ryzyka, zwracając szczególną uwagę, na zagrożenia o najwyższym poziomie ryzyka. Określając nową grupę zabezpieczeń,

ryzyko utraty informacji zmieniło się w istotny sposób. Biorąc szczególnie pod uwagę, te zagrożenia z wysokim poziomem ryzyka zauważa się redukcję ich wartości ryzyka. W ten sposób uzyskano wyniki, które dały jasny i przejrzysty obraz, w których obszarach zaproponować zabezpieczenia, tak by działania były produktywne i wydajne.

BIBLIOGRAFIA

[1] F. Wołowski i J. Zawiła- Niedźwiecki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polski i międzynarodowymi, Kraków: edu-Libri, 2012.

[2] S. Katsikeas, P. Johnson, M. Ekstedt, R. Lagerström „Research communities in cyber security: A comprehensive literature revie" *Computer Science Review Open Access* Volume 42 November 2021

[3] www.darkreading.com (data dostepu 6.12.2019).

[4] P. Bączek., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruń: Wydawnictwo Adam Marszałek, 2005.

[5] T. Muliński., Zagrożenia Bezpieczeństwa dla systemów informatycznych E-Administaracji, Warszawa: CeDeWu, 2015.

[6] P. Tyrała., Zagrożenia kryzysowe. Ryzyko-bezpieczenstwo-obronność, Toruń: Wydawnictwo Adam Marszałek, 2001.

[7] E. Nowak i M. Nowak, Zarys teorii bezpieczeństwa narodowego, Warszawa: Difin, 2011.

[8] ISO 17799-1:2000 Information security management-Code of practice for information security management.

[9] S. W. Nowak A., Zarządzanie bezpieczeństwem informacyjnym, Warszawa: AON, 2010.

[10] J. Łuczak, Zarządzanie bezpieczeństwem informacji. Praca zbiorowa, Poznań: Oficyna Współczesna, 2004.

[11] I. Staniec i J. Zawiła- Niedźwiecki (red.), Ryzyko operacyjne w naukach o zarządzaniu, Warszawa: C.H.Beck, 2015.

[12] W. Bral., Obieg i ochrona dokumentów w zarządzniu jakością, środowiskiem i bezpieczeństwem informacji, Warszawa: Difin, 2008.

[13] K. Liderman., Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa: PWN, 2009.

[14] Ustawa z dn. 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).

[15] M. Wrzosek i A. Nowak, Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego. Praca naukowo-badawcza, Warszawa, 2009.

[16] S. Forlicz., Informacja w biznesie, Warszawa: Polskie Wydawnictwo Ekonomiczne, 2008.

[17] Ł. Łuczak i M. Trybulski, Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań: Wydawnictwo Uniwersytetu Ekonomicznego , 2010.

[18] P. Sienkiewicz., 10 wykładów, Warszawa: AON, 2005.

[19] M. Strzoda., Zarządzanie informacjami w organizacji, Warszawa: AON, 2004.

[20] W. Góralczyk (red.), Prawo informacji, Warszawa: Wyższa Szkoła Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, 2006.

[21] PN-ISO/IEC 27002:2017-06 Praktyczne zasady zabezpieczenia informacji.

[22] T. Kifner., Polityka bezpieczeństwa i ochrony informacji, Gliwice: Helion, 1999.

[23] PN-ISO/IEC 27000:2020-07 Technika informatyczna- Techniki bezpieczeństwa-Systemy zarządzania bezpieczeństwem informacji-Przegląd i technologia.

[24] K. Krzysztofek i Szczepański M.S., Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych. Podręcznik socjologii rozwoju społecznego dla studentów socjologii nauk politycznych i ekonomii. Wydanie2, Katowice: UŚ, 2005.

[25] B. Fischer i W. Świerczyńska-Głowinia, Dostęp do informacji ustawowo chronionych, zarządzanie informacją. Zagadnienia dla dziennikarzy, Kraków: Uniwersytet Jagielloński, 2006.

[26] T. Lech i G. Podgórski , Bezpieczeństwo w sieci[w]J.Papińska-Kacperek (red.) Społeczeństwo informacyjne, Warszawa: PWN, 2008.

[27] Wielki Słownik Poprawnej Polszczyzny, Warszawa, PWN, 2010.

[28] W. Lidwa., Zarządzanie w sytuacjach kryzysowych, AON, 2010.

[29] K. Ficoń., Inżynieria zarządzania kryzysowego. Podejście systemowe," Bel Studio sp.zo.o., Warszawa, 2007.

[30] T. Kaczmarek., „Ryzyko i zarządzanie ryzykiem," Difin, Warszawa, 2008.

[31] „PN-ISO 31000:2018-08 Zarządzanie ryzykiem-wytyczne".

[32] B. Stawnicka., R. Winiewski i Socha (red.), Zarządzanie kryzysowe Teoria, praktyka, konteksty, badania," WiPWSP, Szczytno, 2011.

[33] D. Mąka, M. Skawina i W. Dragoń , Jak chronić informację?, Bellona, Warszawa, 2004.

[34] l. Kiełtyka., Komunikacja w zarządzaniu. Techniki, narzędzia i formy przekazu informacji, Placet, Warszawa, 2002.

[35] PN-ISO/IEC 29134:2018-11 Technika informatyczna-techniki bezpieczeństwa-wytyczne dotyczące oceny skutków dla prywatności

[36] tvn24bis.plz -kraju,74/inter-cars-po ataku-hakerskim-odzyskuje-sprawność, 753763.html (data dostępu 6.12.2019).

[37] Wielki Słownik Wyrazów Obcych, PWN, Warszawa, 2018.

[38] Ustawa z dn. 15 marca 2019r. o ochronie informacji niejawnych.

[39] A. Korombel., Apetyt na ryzyko w zarządzaniu przedsiębiorstwami, Politechnika Częstochowska, Częstochowa, 2013.

[40] P. Białas., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2007.

[41] A. Małachowski (red.), Internet w zarządzaniu przedsiębiorstwem, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław, 2003.

[42] D. Wojtyto., Zarządzanie ryzykiem na szczeblach administracji samorządowej w aspekcie zarządzania kryzysowego. Rozprawa doktorska, AON, Warszawa, 2015.

[43] A. Barczak i T. Sydoruk, Bezpieczeństwo systemów informatycznych zarządzania, Bellona, Warszawa, 2003.

[44] ISO/IEC 27005:2014-01 Technika informatyczna-techniki bezpieczeństwa-Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN, 2013.

[45] A. Nowicki (red.), Komputerowe wspomaganie biznesu, Placet, Warszawa, 2006.

[46] Poradnik Jak stosować podejście oparte na ryzyku Poradnik RODO Podejście oparte na ryzyku, UODO, Warszawa, 2018.

[47] C. Hadnagy., Socjotechnika Sztuka zdobywania władzy nad umysłami, Helion, Gliwice, 2017.

[48] T. Trejderowski, „Socjotechnika podstawy manipulacji w praktyce," Eneteia, Warszawa, 2009.

[49] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku2011, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, Warszawa, 2012.

[50] F. Pierzchalski i J. Golinowski (red.), Socjotechnika lęku w polityce, Uniwersytet Kazimierza Wielkiego, Bydgoszcz, 2016.

[51] W. Stelmach., Socjologia i Socjotechnika Kierowania,Wyższa Szkoła Menadzerska , Warszawa, 2014.

[52] K. Mitnick i W. Simon, Sztuka podstępu, Helion, Gliwice, 2011.

[53] Raport Sociał-Engineer.org z 2010r.

[54] A. Kura., Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku, Sztafeta, Stalowa Wola , 2016.

[55] https://wiadomości. dziennik.pl/świat/artykuły/79159, hakerzy-poszli-na wojne-z gruzja.html (data dotepu 6.12.2019).

[56] https://wiadomości.onet.pl/tylko - w-onecie/estonia-pierwsza-ofiara-cybernetycznej-wojny/t3czdh5 (6.12.2019).

[57] Ustawa z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczenstwa (Dz.U.2018 poz.1560).

[58] J. Jańczak i A. Nowak, Bezpieczeństwo informacyjne Wybrane problemy, Warszawa , 2013.

[59] A. Nowicki i T. Turek , Technologie informacyjne dla ekonomistów. Narzędzia zastosowania, UE, Wrocław, 2010.

[60] www.cert.pl 22.12.2020.

[61] A. Nowicki i M. Sita., Procesy informacyjne, Uniwersytet Ekonomii , Wrocław, 2016.

[62] Ustawa z dnia 17 stycznia 2019r. o rachunkowości (DZ.U.2019 poz.351).

[63] Ustawa z dnia 16 maja 2019 (Dz.U.2019 poz.1010) o zwalczaniu nieuczciewj konkurencji.

[64] Kodeks pracy z dnia 18 czerwca 2020r.

[65] Ustawa z dnia 15 lipca 2020r Kodeks Karny (Dz.U.2020 poz.1444).

[66] Ustawa z dnia 10 maja 2018r. o o ochronie danych osobowych (Dz.U.2019 poz.1781).

[67] Ustawa o prawie telekomunikacyjnym z dnia 15 marca 2019 (Dz.U.z 2019 poz.643).

[68] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r (Art47, 49, 51).

[69] Ustawa z dnia 6 września 2001r. o dostepie do informacji publicznej (Dz.U.2001 nr112 poz.1198).

[70] Ustawa z dnia 21 sierpnia 1997r. prawo o publicznym obrocie papierami wartościowymi (Dz.U. 1997 nr. 118 poz. 754).

[71] Ustawa z dnia 29 lipca 2005 o nadzorze nad rynkiem kapitałowym (Dz.U.2005 nr.183 poz.1537)”

[72] „Ustawa z dnia 29 sierpnia 1997 prawo bankowe (Dz.U. 1997 nr.140 poz.939)”.

[73] Ustawa z dnia 29 lipca 2005 o obrocie instrumentami finansowymi (Dz.U. 2005 nr183 poz.1538).

[74] Ustawa z dnia 16 lipca 2004 prawo telekomunikacyjne (Dz.U 2004 nr171 poz.1800).

[75] Ustawa z dnia 29 lipca 2005 o ofercie publicznej i warunkach wprowadzenia instrumentów do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U.2005 nr.184 poz.1539).

[76] Obwieszczenie Marszałka Sejmu Rzeczypospolitej z dnia 18 października 2019r. w sprawie ustawy o ochronie baz danych (Dz.U.2019 poz.2134).

[77] Ustawa o podpisie elektronicznym 18 września 2001 (Dz.U. 2001 nr.130 poz.1450).

[78] Ustawa o zmianie ustawy o prawie autorskim i prawach pokrewnych oraz ustawy o ochronie baz danych z dnia 22 lipca 2018.

[79] Ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018r.

[80] RODO najważniejsze zmiany i nowości. Bezpieczeństwo ponad wszystko. Materiały szkoleniowe Forsafe, Forsafe, Łódź, 2081.

[81] M. Byczkowski., Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i operacyjnego wymaganego w RODO. Wdrażanie ogólnego rozporzadzenia o ochronie danych. Aktualne problemy prawnej ochony danych osobowych 2017. Nr20/2017, C.H. Beck, Warszawa, 2017.

[82] J. Burdulak i P. Sobczak (red.), „Wybrane problemy zarządzania bezpieczeństwem informacji," Szkoła Główna Handlowa, Warszawa, 2014.

[83] E. Dobrodziej., Ochrona tajemnicy-przepisy, komentarze, wyjśnienia. Zeszyt 158/2000, Oficyna Wydawnicza Ośrodka Postępu Organizcyjnego, Bygdoszcz, 2000.

[84] S. Sołtyński (red.), System Prawa Prywatnego Tom 17A, C.H. Back, Warszawa, 2010.

[85] S. Wojciechowska-Filipek i Z. Ciekanowski, Bezpieczeństwo w cyberprzestrzeni. Jednostki-Organizacja-Państwa, CeDeWu, Warszawa, 2016.

[86] PN-ISO/IEC 27001:2017-06 Systemy Zarządzania Bezpieczeństwem Informacji-wymagania.

[87] PN-ISO/IEC 27018:2020-11 Technika informatyczna- Techniki bezpieczeństwa- Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających, jako przetwarzający PII.

[88] www.pkn.pl/informacje/2018/09/nowelizacja- normy-isoiec-270052018 (data dostępu 6.12.2019).

[89] PN-EN IEC 31010: 2020-01 Zarządzanie ryzykiem-Techniki oceny ryzyka.

[90] PN-EN ISO/IEC 29100:2020-11Technika informatyczna-Technika bezpieczenstwa-Ramy prywatności, wersja angielska.

[91] 29100:2017-07/ A1: 2019-09 Technika informatyczna-Techniki bezpieczeństwa-Ramy prywatności.

[92] PN-ISO/IEC 2900:2017-07 Technika informatyczna- Techniki bezpieczeństwa- Ramy prywatności.

[93] PN-EN ISO/IEC 29134:2020-09,Technika informatyczna- Techniki bezpieczeństwa -Wytyczne dotyczące oceny skutków dla prywatności- wersja angielska.

[94] PN-I-13335-2:2003 Technika informacyjna- Wytyczne zarządzania bezpieczeństwem systemów informatycznych.

[95] NIST Special Publication 800-34 RE. V.1 Contingency Guidefor Information Technology Systems, 2010.

[96] G. Michniewicz., Szpiegostwo gospodarcze -jak zapobiegać. Magazyn Zarządzających Bezpieczeństwem, 3/2006.

[97] E. Pietras., Zagadnienia zarządzania bezpieczeństwem informacji w organizacji. Zarządzanie Przedsiębiorstwem, Polskie Towarzystwo Zarządzania Produkcją, Opole, 1/2016.

[98] D. Pipkin., Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, Wydawnictwo

Naukowo-Techniczne, Warszawa, 2002.

[99] M. Pałęga i M. Knapiński , System zarządzania bezpieczeństwem informacji ISO/IEC 27001:2013 jako narzędzie diagnozy i doskonalenia systemu zarządzania bezpieczeństwem informacji w przedsiebiorstwie. Innowacje w Zarządzaniu i Inżynierii Produkcji 2017, T.2. pod red. R. Knosali, Oficyna Wydawnicza PTZP, Opole, 2017.

[100] PN-EN ISO 19011:2018-08 Wytyczne dotyczące audytowania systemów zarządzania.

[101] T. Polaczek., Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice, 2006.

[102] M. Sekuła., Jaka jest różnica między audytorem a kontrolą. Gazeta prawna z dn.23czerwca 2004.

[103] T. Peltier., Information security policies and procedures. A practioners s.2ed, Auerbach Publication, 2004.

[104] A. Adamczyk, Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania, ITTI, Kościelisko, 2005.

[105] K. Liderman., Bezpieczeństwo Informacyjne. Nowe wyzwania. Wyd.II, PWN, Warszawa , 2017.

[106] Rozporządzenie MSWIA z dn.29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[107] J. Krawiec i K. Stefaniak, System Zarządzania Bezpieczeństwem Informacji w praktyce. Zasady wyboru zabezpieczeń, Warszawa, 2011.

[108] D. Denning., Wojna informacyjna i bezpieczeństwo informacji, Wydawnictow Naukowo-Techniczne, Warszawa, 2010.

[109] M. Pałęga, M. Knapiński i D. Rydz, Identyfikacja i ocena zagrożeń bezpieczeństwa informacji za pomocą wybranych instrumentów zarządzania jakością, Oficyna Wydawnicza Polskiego Towarzystwa Produkcji, Opole, 2018.

[110] T. Lech, G. Podgórski i P. Czerwonka, Chmura obliczeniowa [w] Acta Universitatis Lodziensis Folia Oeconomica, 2011, vol. 3, nr 261.

[111] D. Wróblewski., Zarządzanie ryzykiem-przegląd wybranych metodyk, CNBOP-PIB, Józefów, 2015.

[112] M. Molski i S. Opala, Elementarz bezpieczeństwa systemów informatycznych, Mikom, 2002.

[113] D. Rydz, M. Krakowiak i T. Bajor, Systemy biometryczne jako metoda zapobiegania zagrożeniom bezpieczeństwa publicznego,, Częstochowa: Centralna Szkoła Państwowej Straży Pożarniczej w Częstochowie, 2013.

[114] M. Pałęga., System zarządzania bezpieczeństwem informacji ISO/IEC 27001 w działalności logistycznej, Logistyka, 2/2014.

[115] M. Molski i M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice, 2007.

[116] T. Kaczmarek., Podstawowe zasady interdyscyplinarnego zarządzania ryzkiem. Myśl ekonomiczna i Polityczna, 2011.

[117] M. Pałęga., Rola czynnika ludzkiego w systemie bezpieczeństwa informacji w przedsiębiorstwie, Politechnika Częstochowska Wydział Inzynierii Produkcji i Technologii Materiałów Rozprawa Doktorska, Częstochowa, 2015.

[118] P. Jatkiewicz., Uwarunkowania zarządzania systemem bezpieczeństwa informacji w jednostkach samorządu terytorialnego, Uniwersytet Gdański Wydziała Zarządzania, Gdańsk, 2012.

[119] M.P. Novaes, L.F. Carvalho, J. Lioret, M.L. Proenca, Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments *Future Generation Computer Systems* Volume 125, 2021.

[120] D. Rydz, M. Krakowiak i T. Bajor, Zapewnienie bezpieczeństwa informacji w przedsiębiorstwach. Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa, Akademia im. Jana Długosza , Częstochowa, 2013.

[121] A. Veiga, L. Astakhowa, A. Botha i M. Herselman, Defining organisational information security culture—Perspectives from academia and industry. Computer&Secirity, 2020.

[122] L. Dahabiyeh., Factors affecting organizational adoption and acceptance of computer-based security awareness training tools.
Information and *Computer* Security Volume 29, Issue 5, 2021.

SPIS RYSUNKÓW

SPIS TABEL

ZAŁĄCZNIKI

Mgr inż. Estera Pietras

Politechnika Częstochowska, Wydział Inżynierii Produkcji i Technologii Materiałów,
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa.
al. Armii Krajowej 19, 42-200 Częstochowa
adres e-mail: estera.pietras@wp.pl

KWESTIONARIUSZ ANKIETY BADAWCZEJ

Szanowni Państwo,

Jestem doktorantką Instytutu Przeróbki Plastycznej i Inżynierii Bezpieczeństwa Wydziału Inżynierii Produkcji i Technologii Materiałów Politechniki Częstochowskiej. Przygotowuję pracę doktorką na temat: „*Teoretyczno-doświadczalna analiza poziomu bezpieczeństwa informacji w przedsiębiorstwie wraz z systemem zmniejszenia ryzyka utraty informacji”,* do której zbieram materiał badawczy dotyczący analizy i oceny aktualnego stanu bezpieczeństwa informacji w przedsiębiorstwie. Dlatego też, przekazuję Państwu ankietę w formie papierowej, prosząc o udzielenie odpowiedzi na pytania zamieszczone w niniejszym kwestionariuszu.
Nadmieniam, że ankieta jest anonimowa, a zawarte w niej udzielone odpowiedzi posłużą wyłącznie do celów badawczych i nie będą nikomu ujawnione. Opracowane wnioski będą wykorzystane do badań naukowych. Jednocześnie nadmieniam, że każde pytanie opatrzone zostało instrukcją udzielenia odpowiedzi.

Bardzo dziękuję za wyrozumiałość i udzielenie szczerych odpowiedzi na zadane pytania.

Z wyrazami szacunku
Estera Pietras

1. Czy w Państwa firmie jest wdrożona norma ISO 27001 (dotycząca bezpieczeństwa informacji)?
(Proszę o wstawienie znaku „x" przy wybranej odpowiedzi)

Tak	
Nie	
Nic o tym nie wiem	

2. Czy w Państwa firmie została opracowana i wdrożona Polityka Bezpieczeństwa Informacji?
(Proszę o wstawienie znaku „x" przy wybranej odpowiedzi)

Tak	
Nie	
Nie wiem	

3. Co dla Pani/Pana oznacza bezpieczeństwo informacji, czy jest to zachowanie…?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi lub więcej)

Poufności (informacja nie jest udostępniana nieupoważnionym osobom lub podmiotom)	
Rozliczalności (wiąże się z jednoznacznym przypisaniem zakresu działań jednemu podmiotowi)	
Integralności (zapewnienie, że dane nie zostały zmienione w sposób nieautoryzowany)	
Dostępności (właściwość bycia dostępnym)	
Niezawodności (poprawność działania systemu)	
Autentyczności (zapewnienie, że tożsamość podmiotu jest zgodna z zadeklarowaną)	

4. Proszę określić przypuszczalną liczbę zdarzeń, które w ostatnim roku mogły spowodować utratę bezpieczeństwa informacji w przedsiębiorstwie.
(Wstaw znak „x" przy wybranej odpowiedzi)

Mniej niż 2	
Od 2 do 4	
Od 5 do 6	
Od 7 do 9	
Powyżej 10	
Nigdy nie odnotowano incydentu	
Nie wiem	

5. Proszę o wskazanie, które z poniżej wymienionych zagrożeń utraty bezpieczeństwa informacji Pani/Pana zdaniem są prawdopodobne, do wystąpienia w Państwa przedsiębiorstwie określając częstotliwość ich występowania.

Oceń pojedyncze zagrożenia w skali 0-5 (gdzie poziomy oznaczają: 0-nie mam zdania 1-nie występuje, 2-bardzo rzadko, 3-rzadko, 4-często, 5-bardzo często).

Lp.	Zagrożenia	Prawdopodobieństwo występowania zagrożenia					
		0	1	2	3	4	5
1.	Szpiegostwo gospodarcze						
2.	Nieprzestrzeganie i niezastosowanie się do regulaminu obowiązującego w firmie						
3.	Nieodpowiednie utylizowanie dokumentów papierowych						
4.	Kradzież nośników danych, dokumentów						
5.	Niewłaściwe korzystanie z poczty e-mailowej						
6.	Brak utworzonej PBI						
7.	Brak fizycznej ochrony budynków, drzwi, okien						
8.	Brak szkoleń dla kadry pracowniczej z zakresu bezpieczeństwa informacji						
9.	Brak reakcji na osoby postronne znajdujące się w budynku						
10.	Brak weryfikacji osoby postronnej						
11.	Brak w firmie Inspektora Ochrony Danych Osobowych lub zatrudnianie na tym stanowisku niewykfalifikowanych pracowników						
12.	Nieodpowiednie przygotowanie umowy z personelem, kontrahentami i dostawcami						
13.	Awaria, utrata zasilania						
14.	Brak mechanizmów monitorowania						
15.	Odtworzenie danych z odnalezionych nośników						
16.	Ujawnienie aktywów firmy osobom nieupoważnionym						
17.	Przekroczenie uprawnień poprzez nieuprawniony dostęp do informacji						
18.	Podsłuch komputerowy						
19	Awaria sprzętu komputerowego						
20.	Nieprawidłowe korzystanie z oprogramowania						
21	Włamania do systemu komputerowego, możliwość kradzieży danych						
22.	Wykorzystanie przez petenta informacji udostępnionych w firmie w celu stworzenia kontroferty						
23.	Nieuprawniony dostęp do informacji i jej wykorzystywanie						

6. Proszę wskazać Pani/Pana zdaniem, możliwe zabezpieczenia dla wymienionych w pytaniu 5 zagrożeń bezpieczeństwa informacji?
Wstaw znak „x" przy wybranej odpowiedzi
Skala 0-5 (gdzie poziom: 0- nie mam zdania, 1-nieważne, 2-mało istotne, 3-umiarkowanie istotne, 4-ważne, 5-bardzo ważne).

Lp.	Proponowane zabezpieczenia	Ocena					
		0	**1**	**2**	**3**	**4**	**5**
1.	Procedura korzystania z Internetu						
2.	Przestrzeganie zasad Polityki Bezpieczeństwa Informacji						
3.	Niszczarki						
4.	Szyfrowanie nośników danych						
5.	Polityka korzystania z poczty elektronicznej						
6.	Audyt bezpieczeństwa						
7.	Polityka monitoringu						
8.	Konieczność edukowania pracowników o zasadach bezpieczeństwa informacji						
9.	Służby pionu ochrony przy wejściu do organizacji						
10.	Weryfikacja gości w recepcji						
11.	Szkolenia dot. roli i zadań oraz odpowiedzialności Inspektora Ochrony Danych Osobowych						
12.	Szkolenia dotyczące znaczenia i roli tajemnicy handlowej						
13.	Ochrona przed zanikaniem zasilania, UPS-y prądotwórcze						
14.	Uświadamianie o wartości informacji współpracowników i petentów						
15.	Codzienna kontrola operacji wykonywanych wewnątrz organizacji. Szyfrowanie nośników pamięci						
16.	Ograniczenie poziomu uprawnień osobom nieprzestrzegającym procedur w organizacji						
17.	Monitoring nadawania uprawnień						
18.	Urządzenia antypodsłuchowe						
19.	Procedura postępowania przy stanowisku komputerowym						
20.	Ochrona antywirusowa przed nielegalnym oprogramowaniem						
21.	Płatne, certyfikowane oprogramowanie						
22.	Certyfikaty bezpieczeństwa						
23.	Specjalnie wydzielone miejsca do przechowywania dokumentów, archiwa, nośników danych						

7. Proszę wskazać Pani/Pana zdaniem poziom oddziaływania na poszczególne zagrożenie.
Wstaw znak „x" przy wybranej odpowiedzi
Skala 0-5 (gdzie poziom: 0- nie mam zdania, 1-nieważne, 2-mało istotne, 3-umiarkowanie istotne, 4-ważne, 5-bardzo ważne).

Lp.	Zagrożenie	Poziom oddziaływania zagrożenia (skutek)					
		0	1	2	3	4	5
1.	Szpiegostwo gospodarcze						
2.	Nieprzestrzeganie i niezastosowanie się do regulaminu obowiązującego w firmie						
3.	Nieodpowiednie utylizowanie dokumentów papierowych						
4.	Kradzież nośników danych, dokumentów						
5.	Niewłaściwe korzystanie z poczty e-mailowej						
6.	Brak utworzonej PBI						
7.	Brak fizycznej ochrony budynków, drzwi, okien						
8.	Brak szkoleń dla kadry pracowniczej z zakresu bezpieczeństwa informacji						
9.	Brak reakcji na osoby postronne znajdujące się w budynku						
10.	Brak weryfikacji osoby postronnej						
11.	Brak w firmie Inspektora Ochrony Danych Osobowych lub zatrudnianie na tym stanowisku niewykfalifikowanych pracowników						
12.	Nieodpowiednie przygotowanie umowy z personelem, kontrahentami i dostawcami						
13.	Awaria, utrata zasilania						
14.	Brak mechanizmów monitorowania						
15.	Odtworzenie danych z odnalezionych nośników						
16.	Ujawnienie aktywów firmy osobom nieupoważnionym						
17.	Przekroczenie uprawnień poprzez nieuprawniony dostęp do informacji						
18.	Podsłuch komputerowy						
19.	Awaria sprzętu komputerowego						
20.	Nieprawidłowe korzystanie z oprogramowania						
21.	Włamania do systemu komputerowego, możliwość kradzieży danych						
22.	Wykorzystanie przez petenta informacji udostępnionych w firmie w celu stworzenia kontroferty						
23.	Nieuprawniony dostęp do informacji i jej wykorzystywanie						

8. Czy w Państwa firmie udało się zredukować wspomniany w pytaniu 7, niekorzystny wpływ utraty bezpieczeństwa informacji?
(Proszę o postawienie znaku „x" przy wybranej odpowiedzi)

Tak	
Nie	
Nie wiem	

9. Proszę wskazać, do jakiego rodzaju informacji ma Pani/Pan dostęp?
(Proszę o postawienie znaku „x" przy wybranej odpowiedzi)

Ogólnodostępne, jawne,	
Wewnętrzne	
Dane osobowe	
Tajemnica przedsiębiorstwa	
Tajemnice zawodowe	
Tajemnice prawnie chronione	

10. W jakim stopniu Pani/Pana zdaniem, obowiązujące obecnie przepisy prawne, (rozporządzenia, ustawy) są gwarancją odpowiedniej ochrony?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi w zakresie od 0 do 5)

Skala	**Ocena**
0-nie mam zdania	
1-bardzo mało ważne	
2-mało ważne	
3-średnio ważne	
4-ważne	
5-bardzo ważne	

11. Czy w realizowanych projektach, umowach z kontrahentami istnieją zapisy dotyczące zachowania poufności informacji?
(Proszę o wstawienie znaku „x" przy wybranej odpowiedzi)

Tak	
Nie	
Nie wiem	

12. Czy w Państwa firmie stosuje się Politykę Zarządzania Incydentami, związaną z utratą bezpieczeństwa informacji?
(Proszę o wstawienie znaku „x" przy wybranej odpowiedzi)

Tak	
Nie	
Nie wiem	

13. Czy podpisywaliście Państwo oświadczenie o zachowaniu poufności informacji?
(Proszę o zakreślenie znakiem "x" wybranej odpowiedzi)

Tak	
Nie	
Nie wiem	

14. Kto w Państwa firmie prowadzi ewidencję nadawania uprawnień dostępu do danych?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Asystentka Prezesa	
Administrator Danych- Zarządzający przedsiębiorstwem	
Dział Kadr	
Specjalista ds. ochrony informacji np. Inspektor Ochrony Danych	

15. Jak w Państwa firmie odbywa się utylizacja sprzętu używanego w przedsiębiorstwie np.: nośników danych?
(Proszę o wstawienie znaku "x" przy wybranych odpowiedziach)

Przechowujemy w specjalnym miejscu	
Wyrzucamy do śmieci	
Firma zewnętrzna odbiera zużyty sprzęt	
Sami utylizujemy	

16. Czy dopuszczalne jest wg. Pani/Pana udostępnienie swojego służbowego loginu i hasła innemu współpracownikowi lub stażyście?
(Proszę o wstawienie znaku „x" przy wybranej przez Państwa odpowiedzi)

Tak	
Nie	
Nie mam zdania	

17. Które z wymienionych działań Pani/Pana zdaniem istotnie wpływają na usprawnienie systemu zarządzania ryzykiem?
(Proszę o wstawienie znaku „x" przy wybranej odpowiedzi lub więcej)

Działania korygujące	
Identyfikacja zagrożeń i potencjalnych skutków	
Analiza i ocena ryzyka	
Monitorowanie podatności wystąpienia zagrożenia	
Monitorowanie pojawiającego się zagrożenia	
Sporządzenie procedur postępowania w sytuacji wystąpienia zagrożenia	
Szkolenia personelu z zakresu zarządzania ryzykiem	
Żadne z wcześniej wymienionych	

18. Co to jest ryzyko Pani/Pana zdaniem:
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Przedsięwzięcie, którego wynik jest niepewny.	
Niepewność związana z przyszłymi wydarzeniami	
Skutek niepewności w stosunku do ustalonych celów	
Zjawisko niepewne, którego zajście będzie miało negatywny skutek na przedsiębiorstwo	
Kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji	

19. Proszę określić czy w jednostce jest dokonywana identyfikacja oraz analiza ryzyka?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi).

Tak	
Nie	
Nie mam zdania	

20. W przypadku odpowiedzi „Tak” w pytaniu 19 proszę wskazać jak często jest dokonywana identyfikacja i analiza ryzyka.
(Proszę o wstawienie znaku „x” przy wybranej jednej odpowiedzi)

Raz na kwartał	
Raz na ½ roku	
Raz na rok	
W sytuacji wystąpienia incydentu	

21. Proszę wskazać, czy Pani/Pana zdaniem w przypadku wystąpienia ewentualnego incydentu przedsiębiorstwo podejmuje działania celem minimalizacji utraty informacji?
(Wstaw znak ”x” przy wybranej odpowiedzi)

Tak	
Nie	
Nie mam zdania	

22. W jakim stopniu ocenia Pani/Pan skuteczność działań zapobiegających występowaniu potencjalnych zagrożeń bezpieczeństwa informacji?
Proszę o wstawienie znaku „x” przy wybranej jednej odpowiedzi w skali 0- 5 (gdzie: 0-nie mam zdania 1-nieważne, 2-mało istotne, 3-umiarkowanie istotne, 4-ważne, 5-bardzo ważne)

Skala	**Ocena**
0-nie mam zdania	
1-nieważne	
2-mało istotne	
3-umiarkowanie istotne	
4-ważne	
5-bardzo ważne	

23. Kto w ramach struktury organizacyjnej w Państwa firmie jest odpowiedzialny za wprowadzenie zasad doskonalących System Zarządzania Bezpieczeństwem Informacji oraz działań redukujących ryzyko?
(Proszę o wstawienie znaku „x” przy wybranej jednej odpowiedzi)

Zarząd/Kierownictwo	
Inspektor Ochrony Danych	
Kierownik organizacji	

24. Jakie metody stosujecie Państwo w przedsiębiorstwie celem ochrony monitora komputera.
(Proszę o wstawienie znaku „x” przy wybranej(-nych) odpowiedzi(-iach))

Wygaszacz ekranu	
Barierki ochronne	
Prawo wstępu pojedynczej osoby do biura obsługi klienta	

25. Czy w firmie dokumenty przechowywane są w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym?
(Proszę o wstawienie znaku „x” przy wybranej jednej odpowiedzi)

Tak	
Nie	
Nie wiem	

26. Jak zorganizowana jest w Państwa przedsiębiorstwie praca w obszarach z ograniczonym dostępem?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi lub więcej)

Zakaz nagrywania i fotografowania	
Wejście tylko upoważnianych osób	
Kontrola dostępu	
Zakaz używania telefonów komórkowych	

27. Jak często dokonuje się w Pani/Pana firmie aktualizacji oprogramowania antywirusowego?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Raz na rok	
Raz na dwa lata	
Aktualizacja automatyczna	

28. Czy w Państwa przedsiębiorstwie wykorzystywana jest sieć bezprzewodowa?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	
Nie wiem	

29. W jaki sposób zorganizowany jest w przedsiębiorstwie dostęp do budynków i pomieszczeń biurowych?
(Proszę o wstawienie znaku „x" przy wybranej jednej lub więcej odpowiedzi)

Dostęp do budynku swobodny (każdy może wejść)	
Systemy alarmowe, sygnalizacji włamania i napadu, czujniki ruchu	
Usługi zewnętrzne firmy ochroniarskiej	
Kontrola dostępu-udostępniana poszczególnym wyznaczonym przez system osobom	
Monitoring wizyjny	

30. Jakie rodzaje zabezpieczeń preferowane są w państwa firmie?
(Proszę o wstawienie znaku „x" przy wybranej jednej lub więcej odpowiedzi)

Szlaban przy wjeździe na parking	
Drzwi ochronne	
Ogrodzenie terenu przedsiębiorstwa	
Fizyczne zabezpieczenie wejścia/wyjścia	
Nadzór nad punktami dostępu tj.: obszary dostaw, załadunku, przez które nieuprawnione osoby mogą wejść do pomieszczeń	
Bezpieczeństwo okablowania w celu ochrony przed przechwyceniem, zakłóceniem czy uszkodzeniem sygnału	
Konserwacja sprzętu w celu ciągłej dostępności i integralności	
Zasady czystego biurka i czystego ekranu	

31. Proszę o odpowiedź Panią/Pana czy w miejscu gdzie podejmowane są ważne decyzje stosowane są narzędzia ochrony przed podsłuchem?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	
Nie wiem	

32. Czy w godzinach pracy zdarza się Państwu korzystać z innych stron internetowych w celu prywatnych potrzeb (poczta, portale społecznościowe, itp.)
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	

33. Czy w czasie pracy możne korzystać Pani/Pan z prywatnej pamięci flash, pendriva?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	
Nie wiem	

34. Czy zdarzyło się Pani/Panu zgubić firmowy sprzęt komputerowy lub inne nośniki danych?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	
Nie pamiętam	

35. Czy w Państwa przedsiębiorstwie prowadzony jest rejestr osób wchodzących i wychodzących z firmy?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Tak	
Nie	

36. Jak w Państwa firmie wygląda przyjmowanie gości?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Goście, interesanci swobodnie poruszają się po firmie	
Rejestr gości	
Zawsze w obecności kogoś trzeciego z firmy	

37. Jakie konsekwencje grożą pracownikom za nieprzestrzeganie zasad bezpieczeństwa informacji?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Upomnienie	
Nagana	
Brak premii	
Żadne	
Zwolnienie dyscyplinarne	

38. W jakim stopniu Państwa zdaniem w firmie istnieje potrzeba szkolenia z zakresu bezpieczeństwa informacji?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi w zakresie od 0 do 5)

Skala	**Ocena**
0-nie mam zdania	
1-bardzo mało ważne	
2-mało ważne	
3-średnio ważne	
4-ważne	
5-bardzo ważne	

METRYCZKA

1. Proszę o podanie stopnia Pani/Pan wykształcenia?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Zawodowe	
Średnie	
Wyższe-licencjackie	
Wyższe-inżynierskie magisterskie	

2. Proszę o wstawienie stanowiska, jakie Pani/Pan zajmuje?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Kierownicze wyższego szczebla	
Kierownicze niższego szczebla	
Nie kierownicze	

3. Proszę o określenie stażu pracy w firmie?
(Proszę o wstawienie znaku „x" przy wybranej jednej odpowiedzi)

Do roku	
Od 1 do 3 lat	
Od 3 do 5 lat	
Od 5 do 10 lat	
Powyżej 10 lat	

ARKUSZ OBSERWACJI

TEMAT:
„TEORETYCZNO-DOSWIADCZALNA ANALIZA POZIOMU BEZPIECZEŃSTWA INFORMACJI w PRZEDSIEBIORSTWIE WRAZ z SYSTEMEM ZMNIEJSZENIA RYZYKA UTRATY INFORMACJI”
CEL: Aby poprawnie i dokładnie przeprowadzić proces analizy i szacowania ryzyka bezpieczeństwa informacji dla badanego przedsiębiorstwa pomocne będzie zebranie danych co do stanu faktycznego i uzupełnienie wniosków z badań ankietowych
TEREN OBSERWACJI: Przedsiębiorstwo motoryzacyjne
ZAKRES PROBLEMOWY: Zakres problemowy został omówiony w postaci zadanych pytań. Kwestionariusz ankiety ściśle związany jest z podejściem naukowym w analizie bezpieczeństwa informacji w organizacjach
Data rozpoczęcia Badania zostały przeprowadzone w miesiącach od kwietnia do grudnia 2019r. Próba reprezentatywna dotyczyła łącznie 158 pracowników z 9 przedsiębiorstw. Data zakończenia grudzień 2019r.
Forma: Bierna

L.p	PYTANIA DO PRZEDMIOTU OBSERWACJI	WNIOSKI
1	Czy informacje zawarte w dokumentach, są należycie przechowywane tzn. w szafach pod zamknięciem?	
2	Czy w obszarach technologicznych lub też w miejscach gdzie przebywają księgowe, kadrowe oraz inne osoby odpowiedzialne za przetwarzanie informacji, są niszczarki do dokumentów?	
3	Czy w pomieszczeniach, które służą do przechowywania, przetwarzania informacji wyposażony został w system telewizji dozorowej? Czy zauważono odpowiednie oznakowania dotyczące monitoringu?	
4	Czy zauważono w pomieszczeniach system sygnalizacji pożaru?	
5	W jaki sposób ustawiony jest ekran komputera? Czy ustawienie go, uniemożliwia odczytanie informacji?	
6	Czy zauważono barierki przed wejściem do stref bezpieczeństwa?	
7	Czy pracownicy praktykują zabezpieczenie pomieszczeń podczas chwilowej nieobecności?	
8	Czy informacja o wdrożeniu Polityki Bezpieczeństwa Informacji jest na widocznym miejscu w organizacji?	
9	Czy zauważono identyfikatory u pracowników?	
10	Czy zauważono przy komputerach zapisane hasła?	
11	Jak wygląda wejście do budynku? Czy jest szlaban na parkingu oraz recepcja z służbami ochrony?	
12	Czy prosi się gości o wpisanie się do rejestru osób odwiedzających? Czy zauważono księgę wejścia i wyjścia?	
13	Czy zauważono kopiarkę ksero lub drukarkę sieciową na holu lub na korytarzu, między pomieszczeniami gdzie chodzą pracownicy? Kto z pracowników ma do niej dostęp?	
14	Czy zauważono informację w recepcji dotyczącą zakazu fotografowania i nagrywania?	
15	Czy zauważono oznaczenie strategicznych pomieszczeń np.: serwerowni? Czy serwerownia mieści, się w tym samym miejscu, w którym jest siedziba firmy?	
16	Czy w pomieszczeniach administracyjno-biurowych kosze na śmieci były	

	wypełnione dokumentami, które nosiły znamiona zapisanej informacji i powinny być poddane zniszczeniu w niszczarkach?	

KWESTIONARIUSZ WYWIADU

TEMAT:
„TEORETYCZNO-DOSWIADCZALNA ANALIZA POZIOMU BEZPIECZEŃSTWA INFORMACJI w PRZEDSIEBIORSTWIE WRAZ z SYSTEMEM ZMNIEJSZENIA RYZYKA UTRATY INFORMACJI”
CEL: Aby poprawnie i dokładnie przeprowadzić proces szacowania ryzyka bezpieczeństwa informacji dla badanego przedsiębiorstwa pomocne będzie zebranie danych co do stanu faktycznego i uzupełnienie wniosków z badań ankietowych
TEREN: Przedsiębiorstwa motoryzacyjne
ZAKRES PROBLEMOWY: Zakres problemowy został omówiony w postaci zadanych pytań. Kwestionariusz ankiety ściśle związany jest z podejściem naukowym w analizie bezpieczeństwa informacji w organizacjach
Uprzejmie proszę o udzielenie odpowiedzi na zadane pytania
Data rozpoczęcia: Badania zostały przeprowadzone w miesiącach od kwietnia do grudnia 2019r. Próba reprezentatywna dotyczyła łącznie 158 pracowników z 9 przedsiębiorstw. Data zakończenia: grudzień 2019r.

1. Czy doświadczyli Państwo ataku socjotechnicznego?
2. Czy personel był szkolony z zakresu socjotechniki?
3. Czy pracownicy kiedykolwiek zareagowali na obecność w przedsiębiorstwie osób nieznanych, podejrzanie się zachowujących?
4. Czy zdarzyło się komuś z organizacji zgubić telefon firmowy, kartę dostępu lub identyfikator?
5. Czy sprawdza się ile czasu określony pracownik spędza w danym systemie?
6. Czy w firmie istnieje potrzeba dotycząca szkoleń pracowników z bezpieczeństwa informacji?
7. Czy w określonych działach, w których są przetwarzane informacje wszyscy pracownicy mają aktualne upoważnienia o przetwarzaniu informacji?
8. Jakie wprowadzono zmiany po ostatnim audycie bezpieczeństwa informacji?
9. Czy pracownicy znają zasady korzystania w czasie pracy z Internetu?
10. Czy w Państwa organizacji obowiązuje procedura, co do pozbawiania zapisów na dyskach, czy nośnikach danych przeznaczonych do likwidacji lub dalszej odsprzedaży?
11. Proszę o odpowiedź, czy dokonywanie regularnej analizy ryzyka wpłynie na poprawne funkcjonowanie

systemu bezpieczeństwa informacji w organizacji gospodarczej?

12. z ilu znaków składa się Pani/Pana hasło do komputera?

W przedziale 1-5	
W przedziale 6-10	
W przedziale 11-15	

13.Proszę odpowiedzieć z ilu poziomowego uwierzytelnienia odbywa się dostęp do systemu komputerowego?

14. Czy korzysta Pani/Pan automatycznego blokowania dostępu do systemu?

15. Czy korzystacie Państwo z procedury dotyczącej incydentów związanych z naruszeniami bezpieczeństwa informacji?

16. Czy Pani/Pana zdaniem zasoby firmowe typu laptopy czy telefony kluczowych osób w firmie są odpowiednio zabezpieczone?

17. Czy w polityce bezpieczeństwa informacji zawarte są procedury postępowań korygujących i zapobiegających powstawaniu incydentom?

18. Jak zorganizowana jest w Państwa przedsiębiorstwie praca w obszarach z ograniczonym dostępem?

19. Czy zdarza się pracownikom pożyczać karty dostępu lub identyfikatora współpracownikowi?

20. Czy podmioty zewnętrzne, mają nadawane uprawnienia dostępu do informacji?

21. Jak wygląda rozliczenie zwolnionych pracowników z mienia organizacji, środków uwierzytelniających? (czy prowadzi się raport zdanych urządzeń), Kto to nadzoruje?

22. Ile razy w roku system zabezpieczeń komputerowych ulega uszkodzeniu?

23. Przy pomocy, jakich urządzeń Państwo korzystacie tworząc kopie zapasowe?

24. w jaki sposób wybierane są w organizacji zabezpieczenia oraz jak się je wdraża?

25. Czy w szkoleniach uczestniczą osoby pracujące tymczasowo, stażyści, praktykanci, doktoranci? Jakie szkolenia w ostatnim czasie przeszły osoby przetwarzające informacje?

26. Kto w organizacji jest odpowiedzialny za zarządzanie ryzykiem?

27. Czy firmy zewnętrzne, z którymi Państwo współpracujecie zobowiązały się do podpisania klauzuli o zachowaniu poufności?

28. Proszę powiedzieć czy istnieje w organizacji procedura zastępstw?

POLITYKA
BEZPIECZEŃSTWA
INFORMACJI

Spis treści:

1. Cel opracowania Polityki Bezpieczeństwa Informacji

Posiadane zasoby informacyjne przyczyniają się do możliwości konkurowania z innymi organizacjami gospodarczymi. Jest to równoznaczne z podniesieniem prestiżu i wizerunku organizacji oraz odniesieniem sukcesu na rynku zbytu. Tak, więc aktywa powinno się należycie chronić przed zagrożeniami z otoczenia wewnętrznego, jak i zewnętrznego. W tym też celu tworzy się Politykę Bezpieczeństwa Informacji (PBI), która pozwoli zapewnić wysoki poziom bezpieczeństwa przechowywanych, przetwarzanych zbiorów, zgodnie z kanonami szeroko rozumianego bezpieczeństwa. Dokument ten, jest również wymogiem międzynarodowej normy PN-ISO/IEC 27001:2017.

Dlatego Politykę Bezpieczeństwa Informacji, należy traktować, jako zbiór zasad, procedur, instrukcji wewnętrznych dotyczących postępowania pracowników w komórkach organizacyjnych. Ponadto, PBI wskazuje na sposób przechowywania dokumentów, zarówno tych papierowych, jak i elektronicznych.

Wdrożenie niniejszej polityki jest równoznaczne z określeniem:

a) obowiązków pracowników w zakresie bezpieczeństwa przechowywanych i przetwarzanych danych;
b) technik archiwizacji danych;
c) zabezpieczeń dokumentacji papierowej;
d) zasad korzystania z komputerów przenośnych, w których przetwarzane, są informacje także w pracy zdalnej;
e) sposobu użytkowania z służbowych telefonów komórkowych;
f) ograniczenia ryzyka do minimum poprzez wdrożenie zabezpieczeń technicznych i organizacyjnych;
g) działań kontrolnych, monitorujących poziom ryzyka;
h) programu praktycznych szkoleń [1].

Ponadto, w Polityce Bezpieczeństwa Informacji realizowane są następujące cele:

a) ciągłe doskonalenie procesu szkoleń pracowników, gdzie w klarowny sposób opisuje się wymagania dotyczące modelu Planuj – Wykonuj – Sprawdzaj – Działaj, w skrócie (PDCA);
b) wykorzystanie urządzeń z legalnym oprogramowaniem, dobierając adekwatne do potrzeb przedsiębiorstwa zabezpieczenia;
c) nadzór Inspektora Ochrony Danych Osobowych oraz Pełnomocnika ds. bezpieczeństwa informacji;
d) sprawdzenie kwalifikacji, partnerów oraz dostawców;
e) ogół działań SZBI, skierowanych na zabezpieczenie przedsiębiorstwa przed pojawiającym się zagrożeniem;
f) zapewnienie poufności, dostępności, integralności, autentyczności, rozliczalności oraz niezawodności w omawianym przedsiębiorstwie;
g) zagwarantowanie ciągłości działania w momencie wystąpienia zagrożenia;
h) zobowiązanie do prowadzenia rejestru naruszeń [1].

W niniejszym dokumencie można znaleźć definicje związane z ochroną informacji, które są fundamentem Systemu Zarządzania Bezpieczeństwem Informacji tzw. SZBI. System ten wspomaga system kontroli zarządczej, a dla niego SZBI jest systemem nadrzędnym. W ramach tego systemu określa się przyjęte zasady postepowania, które jasno pokazują sposoby ochrony informacji. Z uwagi na to, że PBI ma charakter obowiązkowy, odpowiedzialność za jej przestrzeganie ponoszą:

- ✓ zarząd;
- ✓ dyrektorzy działów/struktury organizacyjnej;
- ✓ kierownicy działów;
- ✓ pełnomocnik ds. bezpieczeństwa;
- ✓ inne osoby wskazane w umowach zawartych przez organizacje.

Kontrola nad przestrzeganiem zasad PBI w organizacji kierowana jest na kierowników organizacji, w ramach nadzoru nad pracownikami.

2. Zakres stosowania Polityki Bezpieczeństwa Informacji

Dokument PBI określa strategię bezpieczeństwa w organizacji. Takie postępowanie dotyczy działów, dla których należy opracować szczegółową strategię zarządzania systemowego, jakości, przyporządkowania odpowiedzialności w tworzeniu bezpieczeństwa, rozwoju polityk bezpieczeństwa dla każdej podklasy informacji, komunikowania się wewnątrz organizacji oraz z otoczeniem zewnętrznym, reakcji personelu na powstanie incydentu.

W dokumencie PBI, przedstawione zasady dedykowane, są całemu procesowi przetwarzania informacji w organizacji. Należy obowiązkowo się z nimi zapoznać. Dotyczy to wszystkich zainteresowanych, czyli pracowników, dostawców oraz klientów, którzy zobowiązani są postępować zgodnie z zasadami wyszczególnionymi w Polityce Bezpieczeństwa Informacji.

Zasady i postanowienia dotyczą:

a) wszystkich nośników danych, np.: papierowych, optycznych, magnetycznych, na których znajdują się lub będą się znajdować jakiekolwiek informacje;
b) informacji dotyczących partnerów handlowych lub klientów, a będące własnością administratora i procesora na podstawie powierzenia;
c) systemów informatycznych oraz dokumentów w formie papierowej, w których znajdują się informacje podlegające ochronie;
d) ogółu budynków i pomieszczeń, w których są lub będą przetwarzane informacje;
e) wszystkich pracowników przetwarzających [85].

3. Deklaracja Zarządu

Zarząd chcąc chronić posiadane zasoby przed nowo powstałymi zagrożeniami, zdaje sobie sprawę z tego, iż informację należy traktować wysoce priorytetowo z uwagi na ogromną jej wartość. W ramach zabezpieczeń wdrożono SZBI (system zarządzania bezpieczeństwem informacji), który skutecznie zapewni oczekiwany poziom bezpieczeństwa oraz pomoże w zastosowaniu efektywnych i skutecznych rozwiązań.

Zarząd, wdrażając omawiany system, deklaruje zaangażowane podejście do działań doskonalących, wynikających z SZBI. Swoje działanie opiera na zdobytej wiedzy, co do znajomości i znaczenia atrybutów BI.

4. Podstawy prawne dotyczące bezpieczeństwa informacji w organizacji

Przepisy regulujące kwestię związaną z przestrzeganiem zasad bezpieczeństwa informacji uregulowane są w różnych aktach prawnych, dlatego też zaleca się podczas prowadzenia działalności gospodarczej poznanie, chociaż niektórych z nich. Ponadto, dokumentacja związana z bezpieczeństwem informacji oraz dokument PBI m.in. wynikają z poniżej wymienionych przepisów:

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r.
- Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych.
- Rozporządzenie Parlamentu Europejskiego i rady UE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)
- Ustawa z dnia 17 stycznia 2019r. o rachunkowości
- Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej
- Ustawa z dnia 21 sierpnia 1997r. prawo o publicznym obrocie papierami wartościowymi
- Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną
- Ustawa z dnia 29 sierpnia 1997 prawo bankowe
- Ustawa z dnia 29 lipca 2005 o obrocie instrumentami finansowymi
- Ustawa z dnia 15 marca 2019 prawo telekomunikacyjne
- Ustawa z dnia 21 sierpnia 1997 o publicznym obrocie papierami wartościowymi

- Ustawa z dnia 29 lipca 2005 o ofercie publicznej i warunkach wprowadzania instrumentów do zorganizowanego systemu obrotu oraz spółek publicznych
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 18 października 2019 r. w sprawie ustawy o ochronie baz danych
- Ustawa o podpisie elektronicznym 18 września 2001
- Ustawa o zmianie ustawy o prawie autorskim i prawach pokrewnych oraz ustawy o ochronie baz danych z dnia 22 listopada 2018
- PN-ISO/IEC 27005: 2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (Information technology – Security techniques – Information security risk management)
- PN-ISO/IEC 27001: 2017-06 Systemy zarządzania bezpieczeństwem informacji-wymagania, wersja angielska zastępująca normę PN-ISO/IEC 27001:2014-12
- PN-ISO 31000: 2018-08 Zarządzanie ryzykiem –Wytyczne
- ISO/IEC TR 13335-1 (PN-I-13335-1:1999)
- ISO/IEC TR 13335-2 (PN-I-13335-2:2003)
- PN-EN ISO/IEC 27002: 2017-06 - wersja polska Technika informatyczna - Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji.

5. Wyjaśnienie podstawowych pojęć

Opis znaczenia następujących definicji:

- Bezpieczeństwo informacji- zachowanie wszystkich własności bezpieczeństwa tzn. poufności, integralności, dostępności, autentyczności, rozliczalności, niezawodności, niezaprzeczalności. Określona informacja nie zostanie ujawniona niepowołanym osobom, lecz tylko upoważnionemu do tego personelowi.
- Ryzyko- prawdopodobieństwo wystąpienia zagrożenia, które w wyniku wystąpienia podatności może doprowadzić do uszkodzenia i zniszczenia informacji, powodując straty i zniszczenie zasobów. Ryzyko określa się zazwyczaj poprzez dwa czynniki: prawdopodobieństwo wystąpienia oraz skutek, który tym zdarzeniem może zostać wykonany.
- Zabezpieczenia- praktyka, czy też procedura lub mechanizm redukujący ryzyko do określonego akceptowalnego poziomu, które nazywamy ryzykiem szczątkowym. Najczęściej stosowane zabezpieczenia: ochrona przed zagrożeniem, minimalizacja podatności, ograniczenie strat, utrzymanie założonego poziomu bezpieczeństwa.
- Ryzyko szczątkowe- ryzyko, które pozostaje po procesie postępowania z ryzykiem, w zasadzie zawsze pozostaje takie ryzyko, którego dalsza minimalizacja jest już nieekonomiczna.
- Szacowanie ryzyka- proces, w którym zawarta jest analiza i ocena ryzyka.
- Postępowanie z ryzykiem- proces, w którym wybiera się oraz wdraża środki modyfikujące.
- Zarządzanie ryzykiem- proces, w którym identyfikuje się kontroluje i minimalizuje ryzyko dotyczące bezpieczeństwa, może dotyczyć systemów informatycznych.
- Incydent bezpieczeństwa- czynności, które w znacznym stopniu naruszają przepisy PBI oraz innych dokumentów z nim związanych, mogące doprowadzić do utraty aktywów informacyjnych.
- Hasło- ciąg znaków literowych, cyfrowych, małe i duże litery oraz znaki specjalne, znany tylko osobie uprawnionej do systemu informatycznego.
- Usuwanie danych- dotyczy niszczenia danych lub też modyfikacji danych.
- System informatyczny- szeroko rozumiane urządzenia, programy, procedury, służące do przetwarzania informacji oraz narzędzia programowe przeznaczone do przetwarzania informacji.
- Przetwarzanie danych- rozumiane, jako wykonywanie różnych operacji, tzn.: zbieranie, utrwalanie, przechowywanie, opracowywanie, dokonywanie zmian, udostępnianie lub ich usuwanie.
- Zbiór danych- rozumiany, jako zestaw danych o charakterze osobowym lub firmowym, dostępny przy pomocy wskazanych kryteriów, niezależnie od rozproszenia czy podziału.
- Administrator danych- tak zwany Administrator Danych Osobowych, który decyduje o celach i środkach przetwarzania informacji.

- Administrator systemu teleinformatycznego- osoba, na której spoczywa odpowiedzialność za wdrożenie technicznych zabezpieczeń systemu informatycznego.
- Pełnomocnik ds. bezpieczeństwa -osoba sprawująca kontrolę i nadzór nad funkcjonowaniem systemu zarządzania bezpieczeństwem informacji w organizacji. Ponadto, otrzymuje odpowiedzialności i uprawnienia w obszarze wdrażania mechanizmów ochronno-zabezpieczających organizację przed zagrożeniem.
- Zasób- wszystko, co przedstawia jakąś wartość dla organizacji (informacja-dokumenty papierowe, informacje elektroniczne, baza danych, oprogramowanie, zasoby ludzkie, dobra materialne, zasoby fizyczne- budynki, sprzęt informatyczny).
- Poufność danych- zapewnienie dostępu do informacji wyłącznie osobom upoważnionym oznacza, że informacja nie jest udostępniania lub wyjawiana innym podmiotom czy procesom.
- Integralność danych- zapewnienie o dokładności i kompletności aktywów. Dane (informacje) nie mogą być zmienione lub zniszczone w sposób nieautoryzowany.
- Dostępność danych- zapewnienie, że osoby upoważnione będą miały dostęp do informacji, gdy jest to uzasadnione.
- Niezawodność danych- definiowane, jako zdolność jednostki funkcjonalnej do wykonania funkcji w danych warunkach i w danym przedziale czasu.
- Rozliczalność danych- działania podmiotu, które mogą być przypisane tylko jednemu podmiotowi.
- Autentyczność danych- właściwość zapewniająca, iż tożsamość podmiotu i zasobu jest taka, jak deklarowana wcześniej.
- Niezaprzeczalność danych -właściwość uniemożliwiająca nadawcy zaprzeczenie, że wysłana wiadomość pochodzi od niego.
- System Zarządzania Bezpieczeństwem Informacji (SZBI) - jest to system oparty na wymogach normy PN-ISO/ISO 27001.
- Dokumentacja bezpieczeństwa informacji- rozumiana, jako Polityka Bezpieczeństwa Informacji oraz współtowarzysząca Instrukcja Zarządzania Systemem Informatycznym oraz polityki wewnętrzne, regulaminy, procedury, instrukcje i formularze wskazujące reguły postępowania z informacją.
- System przetwarzania informacji- przetwarzanie informacji tylko i wyłącznie w systemach do tego przeznaczonych, opisanych w PBI.
- System informatyczny- określny, jako zespół współpracujących ze sobą urządzeń, programów, procedur pomocnych w przetwarzaniu informacji oraz narzędzi programowych potrzebnych do przetwarzania informacji w systemie.
- Uwierzytelnienie- ukierunkowanie na działania weryfikacyjne zadeklarowanej tożsamości podmiotu.
- Identyfikator użytkownika- ciąg znaków literowych lub też cyfrowych, małe i duże litery oraz znaki specjalne, dzięki którym identyfikuje się osobę upoważnioną do przetwarzania informacji w systemie informatycznym.
- Odbiorca danych- może być każdy, komu udostępnia się dane osobowe z wyjątkiem osoby, której te dane dotyczą, osoby upoważnionej do przetwarzania danych, podmiotu, któremu powierzono te dane do przechowywania i przetwarzania oraz organów państwowych, którym niezbędne jest przekazanie danych w celu prowadzonego postępowania.
- Użytkownik- osoby z personelu organizacji posiadający uprawnienia do przetwarzania informacji (w tym wykorzystania jej w systemie informatycznym) powołany przez Administratora.
- Zagrożenie- potencjalna przyczyna niechcianego incydentu, który może być w skutkach szkodliwy dla systemu.
- Atak- próba naruszenia bezpieczeństwa systemu informatycznego.
- Naruszenie- ingerencja, dotycząca naruszenia bezpieczeństwa systemu informatycznego w celu spowodowania modyfikacji, zniszczenia przez nieuprawnione podmioty.
- Dane osobowe- wszelkie informacje służące do zidentyfikowania osoby fizycznej, poprzez określenie jej tożsamości bezpośrednio lub pośrednio, po numerze identyfikacyjnym lub po

specyficznych czynnikach określających cechy fizyczne tej osoby, fizjologiczne, umysłowe, ekonomiczne, kulturowe, czy społeczne.

- Dane wrażliwe- Ustawa o ochronie danych osobowych **z** dnia 10 maja 2018 roku, wskazuje na dane dotyczących pochodzenia rasowego, etnicznego, poglądów politycznych, przekonań religijnych, filozoficznych wyznaniowych, partyjnych, informacji dotyczących stanu zdrowia, kodu genetycznego, życia seksualnego, danych dotyczących skazań sądowych i orzeczeń o ukaraniu i mandatach karnych a także innych orzeczeniach wydanych przez sąd.
- UODO - Urząd Ochrony Danych Osobowych.

6. Ogólne zasady obowiązujące w jednostce

✓ Osoby mające dostęp do poufnych informacji zobowiązane są do zachowania tajemnicy, zarówno podczas trwania stosunku pracy jak i ukończeniu pracy;
✓ Ochrona przetwarzanych informacji obejmuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych, bez względu na zajmowane stanowisko pracy oraz miejsce wykonywania, jak również po ustaniu stosunku pracy;
✓ Dyrekcja oraz Zarząd jednostki organizacyjnej, są odpowiedzialni za opracowanie, wdrażanie, i doskonalenie PBI;
✓ Polecenia osób upoważnionych przez dyrekcję do wdrożenia działań z obszaru bezpieczeństwa informacji, systemu informatycznego powinny być bezwzględnie wykonane przez wszystkich pracowników i użytkowników systemu;
✓ Każdy pracownik winien odbyć szkolenie z zasad ochrony informacji, spełnić kryteria upoważnienia do przetwarzania informacji oraz podpisać oświadczenie o zachowaniu poufności informacji;
✓ Organizacja świadczy tylko, takie usługi, których wymaga od niego kontrahent;
✓ Każdy pracownik posiada ograniczone prawo dostępu do informacji, koniecznych do wykonywania powierzonych zadań;
✓ Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp i związanych z tym powierzonych zadań;
✓ Za bezpieczeństwo w poszczególnych działach odpowiadają określone osoby upoważnione przez zarząd organizacji. Należą do nich kierownicy działów oraz pracownicy tych działów.

7. Zabezpieczenia dostępu do danych informacji

Dostęp do pomieszczeń, w których przetwarzane są dane lub znajdują się serwery baz danych lub też przechowywane są kopie zapasowe mają tylko osoby, które wcześniej uzyskały do tego upoważnienia. Wnioski upoważniające dostęp do informacji składają pisemnie kierownicy działów do Administratora.

Nadzór nad pomieszczeniami przeznaczonymi do przetwarzania informacji wchodzą w skład obowiązków ochrony budynku, na podstawie uprawnień wydanych przez Pełnomocnika ds. bezpieczeństwa.

7.1. Nadawanie uprawnień

Podział obowiązków pracowniczych oraz nadanie odpowiedzialności, dotyczących zabezpieczeń powinny zostać wcześniej określone i przyporządkowane do stanowisk pracy. Upoważnienia, wydaje się na wniosek pisemny kierownika określonego działu. Upoważnienie otrzymuje się w celu zagwarantowania dostępu użytkownikowi do systemu. Upoważnienia są nadawane stosownie do zajmowanego stanowiska. Użytkownik systemu nie może mieć więcej upoważnień, niż jest to niezbędne do wypełnienia służbowych obowiązków.

Nie wolno dopuścić do przetwarzania informacji krytycznych przez wyłącznie pojedynczego pracownika.

W organizacji prowadzi się ewidencję i aktualizację nadanych i utraconych uprawnień dla użytkowników. Zweryfikowanie tożsamości pracownika pozwalają na kontrolę w organizacji osób, z zewnątrz, bez statusu pracownika.

8. Środki organizacyjne i techniczne niezbędne w celu zapewnienia bezpieczeństwa informacji w organizacji

8.1. Środki organizacyjne

Związane są z czynnościami dotyczącymi określenia oraz przyporządkowania struktury wew. organizacji w kierunku ochrony przechowywanych przez nią zasobów. Do działań mających na celu zwiększenie bezpieczeństwa systemu zaliczono:

- ✓ wdrożenie i opracowanie PBI;
- ✓ w rejestrze UODO wskazanie na Inspektora Ochrony Danych Osobowych;
- ✓ przetwarzanie informacji przez osoby wyłącznie posiadające upoważnienia nadane przez Administratora;
- ✓ prowadzona ewidencja osób upoważnionych do przetwarzania informacji w formie imiennych upoważnień;
- ✓ procedura szkoleń dla osób upoważnionych do przetwarzania informacji wraz z zapoznaniem ich z przepisami oraz treścią PBI;
- ✓ osoby otrzymujące upoważnienia do systemu informatycznego, znają przepisy z zakresu zabezpieczenia systemu;
- ✓ osoby upoważnione do przetwarzania informacji zobowiązały się pisemnie do zachowania poufności, w tym do zachowania tajemnicy służbowej;
- ✓ odpowiednio dedykowane szkolenia z zakresu przetwarzania informacji dla osób nowo zatrudnionych. Dopiero, po odbytym szkoleniu nadaje się upoważnienia i pracownik zobowiązuje do zachowania tajemnicy przedsiębiorstwa;
- ✓ przetwarzanie informacji dokonuje się wyłącznie w warunkach chroniących i ograniczających dostęp osób nieuprawnionych;
- ✓ zakazuje się prowadzenia prac prywatnych w organizacji gospodarczej, wykorzystując firmowe materiały lub sprzęt;
- ✓ nie wolno na teren jednostki organizacyjnej wnosić prywatnego sprzętu, bez wcześniejszej zgody przełożonego;
- ✓ nie dopuszcza się przebywania osoby nieuprawnionej w pomieszczeniach, w których przetwarzane są informacje strategiczne dla organizacji.

8.2. Przekazywanie danych na zewnątrz

Udostępnienie powierzonych informacji stosuje się poprzez pisemne powierzenie przetwarzania lub też podczas zawierania umów z klientami. Udostępnienie takich danych wymaga pisemnej zgody Administratora, zgodnie z wymaganymi przepisami. Takie wnioski powinny, być umotywowane pisemnie i odnotowane w systemach informatycznych.

8.3. Postępowanie z dokumentami w formie papierowej

- ✓ Nie dopuszcza się do pozostawienia dokumentów ksero w kserokopiarkach bez nadzoru pracownika;
- ✓ Dokumenty i wydruki nie potrzebne, niszczy się w niszczarkach, od razu po ustaniu celu ich przetwarzania;
- ✓ Do momentu ich fizycznego zniszczenia przechowuje się takie dokumenty w miejscu, do którego nie mają dostępu inne osoby niepowołane;

- ✓ Podejmuje się odpowiednie działania zapobiegające pozostawieniu dokumentów, na widocznym miejscu, podczas przyjmowania kontrahentów czy partnerów organizacji;
- ✓ Zaleca się zastosowanie szczególnych środków ostrożności w celach przenoszenia dokumentów poprzez noszenie ich w ochronnych teczkach lub segregatorach;
- ✓ Nadzorowanie zbioru danych, podczas transportu samochodowego w inne miejsce polega, na przewożeniu w niewidocznym dla wzroku innych miejscu (pod siedzeniem, w teczce lub bagażniku). Skuteczna w tym miejscu będzie blokada drzwi podczas jazdy;
- ✓ W pomieszczeniach zabezpieczonych np.: fizycznie umieszcza się dokumenty i wydruki zawierające dane osobowe przed wglądem osób nieuprawionych;
- ✓ Aby nie udostępnić informacji wszyscy pracownicy zobowiązani są do przestrzegania zasad czystego biurka. Dotyczy to przechowywania dokumentów niepotrzebnych w danej chwili lub po zakończeniu pracy, w sposób zabezpieczający przed kradzieżą np.: w zamkniętych szafach. Zakazuje się swobodnego pozostawienia dokumentów bez zabezpieczeń.

8.4. Dostęp do pomieszczeń przez pracowników

- ✓ Pojawiające się niezgodności w zabezpieczeniach pomieszczeń należy niezwłocznie zgłosić Pełnomocnikowi ds. bezpieczeństwa;
- ✓ Osoba, która wchodzi pierwsza do pomieszczenia winna sprawdzić, czy zostało ono dobrze zabezpieczone i czy przypadkiem nie doszło do jakiegoś incydentu;
- ✓ Osoba, która wychodzi ostatnia z pomieszczenia zobowiązana jest do zamknięcia drzwi, okien, wyłączenia wszystkich świateł, odłączenia sprzętów komputerowych;
- ✓ Osoba wychodząca ostatnia z biura powinna również sprawdzić czy dokumenty nośniki, pendrive, dyski twarde zostały należycie zabezpieczone,. Jeśli nie, to zobowiązana jest do ich zabezpieczenia;
- ✓ Nie wolno zostawiać kluczy w zamkach po zakończeniu pracy;
- ✓ Nie wolno spożywać alkoholu, ani palić tytoniu w pomieszczeniach organizacji;
- ✓ Nie należy spożywać posiłków, ani pić napojów w bliskim sąsiedztwie komputerów;
- ✓ Podczas wyjścia z pomieszczeń, w których przetwarza się informacje nie wolno zostawić otwartego pokoju, bez nadzoru pracownika.

8.5. Zagwarantowanie poufności w dokumentach

- ✓ Każda informacja powinna być zabezpieczona poprzez elementy zabezpieczające, których się nikomu nie ujawnia;
- ✓ Zabrania się wykorzystywania danych informacji o, ile nie są one jawne, w celach innych niż służbowe**.**
- ✓ Nie dopuszczalne jest podawanie jakichkolwiek informacji, podczas rozmów telefonicznych, osobom nieuprawnionym;
- ✓ Dostęp do powierzonych danych związany jest z zachowaniem tajemnicy, do których pracownik ma dostęp w związku z wykonywanymi obowiązkami służbowymi. Jednak, tajemnica obowiązuje, zarówno w okresie zatrudnienia, jak i po ustaniu stosunku zatrudnienia.
- ✓ Wszystkich pracowników obowiązuje całkowity zakaz wykorzystywania informacji powiązanych z obowiązkami służbowymi i pracą zawodową, w celach prywatnych. Dotyczy to np. publikowania zdjęć na portalach społecznościowych itp.

8.6. Postępowanie związane z korzystaniem z telefonów komórkowych

Użytkownik korzystający z telefonu komórkowego zobowiązany jest do przestrzegania poniższych ustaleń:

- ✓ Ustalenia hasła dla karty SIM oraz telefonu komórkowego celem zabezpieczenia dostępu;
- ✓ Noszenia telefonu ze sobą i nie pozostawienie go w miejscach widocznych dla osób trzecich;

- ✓ Całkowitego usunięcia z pamięci telefonu komórkowego danych, a głównie książki telefonicznej z kontaktami, w razie zmiany telefonu.
- ✓ W momencie zgubienia lub też kradzieży telefonu wymaga się natychmiastowego zablokowania karty SIM u operatora sieci komórkowej oraz powiadomienia o tym fakcie kierownika organizacji.
- ✓ Skonfigurowanie blokady telefonu po maksymalnym czasie 3 minut od momentu ostatniego użycia telefonu, wprowadzając kod przed ponownym użyciem telefonu.

8.7. Zabezpieczenia systemu informatycznego

Zabezpieczenia sprzętowo-programowe dotyczą zabezpieczeń infrastruktury informatycznej i teleinformatycznej. Są to czynności oraz metody o następującym charakterze ochraniającym posiadane zasoby w organizacji:

- ✓ Wykorzystywanie licencjonowanego oraz certyfikowanego sprzętu teleinformatycznego, dotyczącego oprogramowania systemowego i użytkowego;
- ✓ Wdrożenie programowych lub sprzętowo-programowych zapór sieciowych tzw. Firewall;
- ✓ Wykorzystanie na bieżąco aktualizowanego oprogramowania systemowego i użytkowego. Dotyczy to również oprogramowania producenta sprzętu tzw. firmware;
- ✓ Korzystanie z narzędzia do tworzenia kopii zapasowych bezpieczeństwa danych tzw. Bickup;
- ✓ Kopie zapasowe powinno się przechowywać w miejscach zabezpieczających przed nieuprawnionym dostępem i przejęciem, modyfikacją, czy też uszkodzeniem i w konsekwencji zniszczeniem;
- ✓ Po ustaniu użyteczności kopii, niezwłocznie się je usuwa;
- ✓ Na urządzeniach komputerowych, przeznaczonych do przetwarzania danych informacji używa się programów z uwzględnieniem praw autorskich;
- ✓ Przeprowadzenie odpowiednio bezpiecznej konfiguracji sprzętu oraz oprogramowania użytkowanego w stacjach roboczych, serwerach i urządzeniach teleinformatycznych;
- ✓ Stosowanie nadmiarowych urządzeń, środków technicznych w celu zapewnienia ciągłości działania procesów przetwarzania, przesyłania, udostępniania danych oraz ich archiwizacji. Dotyczy to zapasowych komputerów, serwerów, macierzy dyskowych RAID, zapasowych łączy teleinformatycznych oraz odpowiednio licencjonowanego oprogramowania.
- ✓ W systemie komputerowym rejestrowany jest dla każdego użytkownika odrębny identyfikator, dzięki któremu użytkownik może zalogować się do systemu;
- ✓ Identyfikator, który utracił uprawnienia do przetwarzania informacji nie jest już przydzielany żadnej innej osobie;
- ✓ Dostęp do danych jest możliwy po wprowadzeniu dwóch czynności zabezpieczających: identyfikacji i dokonaniu jego uwierzytelnienia;
- ✓ Używanie oprogramowania antywirusowego, efektywnego oraz zaktualizowanego;
- ✓ W archiwizacji danych o znaczeniu strategicznym, bardzo ważne jest, stosowanie technik kryptograficznych (siła i jakość wykorzystywania algorytmu szyfrowania oraz używania kluczy prywatnych lub publicznych. Należy chronić klucze przed utratą oraz zabezpieczyć fizycznie miejsca, w których przechowywane są klucze;
- ✓ Używanie aplikacji służących do detekcji i blokowania nieuprawnionych działań intruzów typu IDS/IRS;
- ✓ Przebywanie osób nieuprawnionych w miejscach, w których przetwarzane są informacje jest niedopuszczalne. Jedynym wyjątkiem obecności takich osób jest, uzyskanie zgody od Administratora [2].
- ✓

8.8. Serwisowanie oraz obsługa nośników danych

- ✓ Niszczenie nośników danych musi odbywać się zgodnie z obowiązującymi zasadami i procedurami obowiązującymi w przedsiębiorstwie;

- ✓ Należy dokładnie sprawdzić partnerów, z którymi organizacja kooperuje, upewniając się że posiadają certyfikaty, co do odpowiedniego i bezpiecznego serwisowania urządzeń;
- ✓ Przed transportem urządzeń do serwisu, należy zabezpieczyć połączenie z internetem, poprzez tulnet.

8.9. Środki techniczne

Stosowanie zabezpieczeń technicznych dotyczy informatyki lub też wykorzystywanych technologii informatycznych, które znacznie wpływają na bezpieczeństwo organizacji. Środki techniczne można podzielić na urządzenia techniczne, programowe, kontroli dostępu oraz kryptograficzne. Oto niektóre z nich:

- ✓ Nadzór nad dostępem do pomieszczeń organizacji gospodarczej w czasie pracy, ale i po godzinach pracy. Zastosowanie instalacji alarmowych tj. sygnalizacji głosowej i światła włamania i napadu, pożaru oraz monitoringu tj. telewizji przemysłowej;
- ✓ Odpowiednie wentylowanie pomieszczeń oraz korzystanie z systemu klimatyzacji;
- ✓ Całościowe ekranowanie pomieszczeń, w których przechowuje się dane, poprzez zastosowanie klatki Faradaya, która nie przepuszcza fal elektromagnetycznych z zewnątrz ani też na zewnątrz;
- ✓ Stosowanie w miarę możliwości mediów transmisyjnych. Dotyczy to światłowodów zabezpieczających przed podsłuchem;
- ✓ Zainstalowanie bezpieczników przepięciowych;
- ✓ Zaimplementowanie urządzeń podtrzymujących zasilanie typu UPS (zastosowane centralnie lub jednostkowe stabilizatory napięcia, podtrzymujące ciągłość pracy);
- ✓ Korzystanie z kart magnetycznych i mikroprocesorowych, umożliwiających odczytywanie, zapisywanie oraz weryfikacje podpisów cyfrowych;
- ✓ Stosowanie urządzeń biometrycznych, zajmujących najważniejsze miejsce w ochronie bezpieczeństwa informacji. Dokonując weryfikacji poprzez odcisk palca, głos lub rozpoznanie siatkówki oka rozpoznaje się tożsamość nadawców i odbiorców.
- ✓ Korzystanie z urządzeń blokujących dostęp oraz korzystanie z sieci teleinformatycznych;
- ✓ Korzystanie ze sprzętowej blokady dostępu do klawiatury, czy napędów dysków. Dotyczy to urządzeń nadzorujących pracę i wyłączających się po określonym czasie nieaktywności użytkownika. Takie odblokowanie nastąpi dopiero po ponownym wpisaniu hasła lub przybliżeniu specjalnej karty;
- ✓ Wykorzystywanie urządzeń do tworzenia kopii zapasowych oraz korzystanie z metod, ich przechowywania. Tworzenie kopii zapasowych, na taśmach magnetycznych, dyskach magnetycznych, optycznych, czy chmurach. Podczas awarii np. dysku twardego, kopia zapasowa jest w stanie odzyskać informacje zapisane na dysku;
- ✓ Zastosowanie ukrytych przewodów na posadzce, poprowadzenie mediów transmisyjnych oraz urządzeń teleinformatycznych w specjalnych osłonkach zabezpieczających;
- ✓ Zastosowanie systemów ogrodzeniowych, instalowanych na wewnętrznym ogrodzeniu obwodnicy (kable elektromagnetyczne, ogrodzenia aktywne z wmontowanymi czujnikami mechaniczno-elektrycznymi);
- ✓ Zastosowanie systemów naziemnych, opartych o bariery mikrofalowe czy podczerwień;
- ✓ Zastosowanie systemów ziemnych, dotyczących kabli elektrycznych aktywnych (wytwarzających pole elektryczne) lub magnetycznych pasywnych wytwarzających pole magnetyczne;
- ✓ Systemy ogrodzeniowe, naziemne i ziemne można sprzęgnąć z systemem telewizji dozorowej w kierunku szybkiego wyszukania przyczyny alarmu;
- ✓ Zastosowanie systemów optycznych typu bliska podczerwień, długa podczerwień, wizyjne detektory ruchu [3].

9. Ochrona fizyczna informacji

Niezależnie od sytuacji, powierzenia ochrony organizacji gospodarczej wyspecjalizowanej agencji ochrony lub powołania własnych służb partnerskich, powołuje się osoby, które zapoznane zostały

z problematyką znaczenia i ochrony bezpieczeństwa fizycznego. Do takich osób zaliczamy, np. członka zarządu, który prezentuje najwyższe kierownictwo, posiadający wiedzę na temat finansów przeznaczonych na utrzymanie bezpieczeństwa oraz członka niższego szczebla kierowniczego, który posiada pisemne upoważnienie do działań z zakresu bezpieczeństwa fizycznego w organizacji.
Do ochrony fizycznej informacji zaliczono następująco:

- ✓ Kontrolowanie wejść i wyjść oraz obecności osób obcych na terenie organizacji;
- ✓ Ograniczenie dostępu do pomieszczeń, biur, czy korzystanie z urządzeń typu: zamki, kraty, kłódki, metalowe drzwi, sejfy, szafy pancerne;
- ✓ Prawidłowy wybór pomieszczenia dla serwerów baz danych, czy miejsc, w których przechowuje się nośniki pamięci;
- ✓ Zwrócenie uwagi, z jakich materiałów zbudowany jest budynek, mianowicie ściany (ściany powinny mieć trwałą konstrukcję) okna, szyby, drzwi (szczególnie zewnętrzne powinny być odpowiednio zabezpieczone poprzez zamki, alarmy, mechanizmy kontroli);
- ✓ Utworzenie stref ochronnych w podmiocie gospodarczym, utrudniające i opóźniające wtargnięcie intruza do ochranianych zasobów;
- ✓ Stworzenie barier fizycznych wokół pomieszczeń w instytucji, w której przetwarzane są informacje, typu ściana, bramka wejściowa, otwieranie drzwi za pomocą karty;
- ✓ Każda bariera stanowi obwód zabezpieczający, który pomaga w całkowitym zabezpieczeniu przed wtargnięciem niepowołanej osoby;
- ✓ Bariera fizyczna powinna być rozciągnięta od podłogi do sufitu, dla ochrony przed nieuprawnionym wejściem osób z zewnątrz, zanieczyszczenia dymem po pożarze, czy zalaniem wodą;
- ✓ Obwód zabezpieczający wyraźnie zaznaczony;
- ✓ Obwód miejsca, w którym przetwarzane są informacje wytrzymały pod względem fizycznym, bez przerw w obwodzie, gdzie mogłoby dojść do włamania;
- ✓ Uruchomienie recepcji, obsługiwanej przez recepcjonistkę lub zapewnienie innych środków fizycznej kontroli;
- ✓ Wszystkie drzwi w obwodzie zabezpieczone alarmem i zamkiem samozatrzaskowym;
- ✓ Najważniejsze urządzenia mają zostać tak rozmieszczone, aby uniknąć dostępu osób nieupoważnionych;
- ✓ Fotokopiarki, faks, ksero, zlokalizowane w obszarach bezpiecznych, unikając tym samym dostępu osób nieupoważnionych;
- ✓ Przechowywanie sprzętu zapasowego, czy nośników z kopiami zapasowymi w pomieszczeniach, które znajdują się w bezpiecznej odległości;
- ✓ Materiały niebezpieczne czy też łatwopalne składowane są w odpowiednio bezpiecznej odległości od chronionego obszaru bezpieczeństwa;
- ✓ Wszystkie drzwi zewnętrzne oraz okna wyposażone w systemy wykrywania wtargnięć. Natomiast w obszarach bezobsługowych stosuje się dozorowe systemy alarmowe [3], [4].

10. Zabezpieczenia organizacyjne

Każdy z podmiotów gospodarczych winien zapewnić skuteczne bezpieczeństwo dla przechowywanych, przetwarzanych zasobów, wspierając się działaniami organizacyjnymi. Zaliczono do nich:

- ✓ Wykupienie przez organizację polisy ubezpieczeniowej;
- ✓ Wdrożenie polityki kadrowej, w której będą zawarte informacje dotyczące zatrudniania, zwolnienia pracowników, szkoleń oraz przekazywania uprawnień np. administratorowi systemu, czy też kierownikowi działu IT;
- ✓ Utworzenie stref ochronnych w organizacji gospodarczej;
- ✓ Wdrożenie kompleksowej PBI;
- ✓ Opisanie przeznaczenia poszczególnych pomieszczeń, budynków, lokali w tym określenie ich lokalizacji;

- ✓ Powołanie działu czy komórki, odpowiedzialnej za bezpieczeństwo danych;
- ✓ Ustalenie odpowiedzialności związanej z zakresem obowiązków poszczególnych pracowników;
- ✓ Opracowanie planu postępowania w warunkach sytuacji awaryjnych;
- ✓ Opracowanie regulaminu odpowiedniego postępowania pracowników w warunkach zwyczajnych;
- ✓ Kontrolowanie pracy użytkowników systemu [2].

11. Zabezpieczenia administracyjne

Stanowią zbiór czynności podejmowanych przez użytkowników dla ochrony posiadanych zasobów. W tym celu prowadzi się działania związane z uzyskaniem certyfikacji obiektu, jako pisemnego zapewnienia od poświadczającego podmiotu, że obiekt spełnia określone wymogi certyfikacyjne. Taki certyfikat uzyskuje oprogramowanie, sprzęt, budynek. Ponadto, zabezpieczenia te związane są, z zarządzaniem systemami informatycznymi. Do grupy zabezpieczeń administracyjnych zalicza się:

- ✓ Sterowanie dostępem do poszczególnych stref bezpieczeństwa (pomieszczeń) w danej organizacji gospodarczej;
- ✓ Kontrolowanie poprzez prowadzenie rejestru nadawania i odbierania użytkownikom uprawnień dostępu do zasobów;
- ✓ Wprowadzenie nadzoru nad poprawnym funkcjonowaniem zasobów;
- ✓ Wprowadzenia modernizacji oraz konfigurowanie zasobów;
- ✓ Prowadzenie rejestru pojawiających się nowych naruszeń bezpieczeństwa;
- ✓ Prowadzenie rejestru czasu pracy osoby wykonującej kopie zapasowe;
- ✓ Odpowiednie, zgodne z procedurami niszczenie zbędnych wydruków z danymi lub nośników danych;
- ✓ Korzystanie z kluczy kryptograficznych [5].

12. Archiwizacja –tworzenie kopii zapasowych

Należy korzystać z oprogramowania do tworzenia kopii zapasowych poprzez następujące sposoby tworzenia kopii

- ✓ Archiwizacja pełna- dotyczy każdorazowego zapisu danych przeznaczonych do archiwizacji;
- ✓ Archiwizacja różnicowa- kopia dotyczy tylko danych z ostatniego dnia tygodnia, natomiast w pozostałe dni zapisują się tylko te dane, które uległy modyfikacji od czasu pełnej archiwizacji;
- ✓ Archiwizacja przyrostowa- pełna kopia danych dotyczy tylko danych kopiowanych w ostatnim dniu tygodnia, a w pozostałe dni kopiowane są dane modyfikowalne, od wersji wykonywanej w dniu poprzedniej archiwizacji [2].

13. Profilaktyka antywirusowa

Związana jest z ograniczeniem ryzyka i wywołanymi stratami spowodowanymi ujawnieniem informacji. Dlatego też należy:

- ✓ Korzystać tylko i wyłącznie z oprogramowania antywirusowego;
- ✓ Co tydzień aktualizować sygnatury baz wirusów;
- ✓ Aktualizować i konfigurować oprogramowanie systemowe, użytkowe;
- ✓ Zakazywać otwierania załączników z poczty e-mailowej z nieznanego źródła;
- ✓ Zakazywać odpowiadania na wiadomości spam;
- ✓ Nie uruchamiać plików firmowych na swoich prywatnych komputerach.

14. Szkolenia dla pracowników

Podczas rozwoju przedsiębiorstwa rosną wymagania wobec obsługi systemów informatycznych, teleinformatycznych. Jest to związane z potrzebą zatrudniania wykfalifikowanych pracowników. Zatem, organizacja jest zobowiązana do zapewnienia kompetencji pracownikom, zgodnie z określonymi wcześniej wymaganiami stanowiskowymi. Niezbędne w tym celu będą szkolenia dla wszystkich grup pracowniczych.

W ramach planowania programu szkoleń należy wziąć pod uwagę:

- ✓ Zanim użytkownik systemu zostanie dopuszczony do pracy, w którym przetwarzane są informacje lub przetwarza zbiory danych, powinien niezwłocznie odbyć szkolenie w zakresie zasad ochrony informacji w zbiorach papierowych lub elektronicznych;
- ✓ Odpowiedzialną osobą za przeprowadzenie szkoleń załogi pracowniczej jest Pełnomocnik ds. bezpieczeństwa;
- ✓ Program szkoleń dotyczący bezpieczeństwa powinien obejmować wprowadzenie środków prewencyjnych we wszystkich poziomach organizacji (od zarządu do pracowników produkcyjnych);
- ✓ Na szkoleniu pracownik poznaje metody ochrony informacji, oparte o obowiązujące aktualnie ustawy, akty normatywne, rozporządzenia, cele bezpieczeństwa, strategię ochrony oraz sposoby wdrożenia zabezpieczeń;
- ✓ Program szkoleń powinien uświadomić pracownikom potrzebę oraz konieczność wprowadzania zabezpieczeń do systemów informacyjnych oraz nabierze umiejętności działania zgodnego z procedurami określonymi w PBI;
- ✓ Po przeprowadzonym programie szkoleniowym pracownik powinien w pełni rozumieć wymogi i oczekiwania zarządu przedstawione w PBI oraz wiedzieć, jak przyczynia się ona do realizowanych celów organizacji w obszarze zarządzania systemami informacyjnymi;
- ✓ Szkolenia odbywają się regularnie, i są z góry, są uwzględniane w planie rocznym;
- ✓ Po ukończeniu szkolenia, pracownicy podpisują pisemnie zobowiązanie do przestrzegania zasad ochrony informacji w systemach oraz co najważniejsze o zachowaniu tajemnicy przedsiębiorstwa;
- ✓ Oświadczenie pracownika o dochowaniu tajemnicy przedsiębiorstwa przechowywane jest w aktach pracownika i stanowia podstawę do podjęcia działań w celu nadania mu uprawnień do użytkowania systemu informatycznego;
- ✓ Administrator nadaje uprawnienia dostępu do systemu informatycznego poszczególnym użytkownikom, którzy spełnili określone wymagania z zakresu kompetencji;
- ✓ Wtórne programy szkoleń prowadzony jest w momencie zaistnienia incydentu zagrażającego bezpieczeństwu informacji w organizacji;
- ✓ Pracownicy zajmujący się w swoich obowiązkach analizą ryzyka powinni odbyć odrębne szkolenie specjalistyczne, nabywając zawansowanych umiejętności dotyczących szacowania ryzyka, wdrażania nowych zabezpieczeń dla zasobów przedsiębiorstwa;
- ✓ Wszyscy kierownicy wyższego oraz niższego szczebla zarzadzania powinni przejść specjalistyczne szkolenia dotyczące wymagań zarządu, związane z odpowiednim sposobem klasyfikowania i oznaczenia informacji. Ponadto, powinni umieć instalować nowe mechanizmy zabezpieczające systemy informacyjne.

15. Bezpieczeństwo informacji w zarządzaniu projektami

- ✓ Każdy projekt, szkic, realizowany w organizacji gospodarczej jest oceniony przez Pełnomocnika ds. bezpieczeństwa pod względem ochrony bezpieczeństwa informacji;
- ✓ Prototypowa ochrona obejmuje pojazdy, komponenty i części sklasyfikowane, jako wymagające ochrony, które nie zostały jeszcze publicznie przedstawione [6].

15.1. Bezpieczeństwo fizyczne w zarządzaniu projektami

- ✓ Środki wymagane do ochrony prototypu muszą być stosowane i wdrażane w odniesieniu do obiektów dostawców, partnerów i usługodawców. Koncepcja bezpieczeństwa musi być opracowana przez danego operatora;
- ✓ Nieautoryzowany dostęp do chronionych obiektów musi być uniemożliwiony, poprzez użycie ogrodzeń, ścian, krat, szyb ochronnych, których z kolei nie można usunąć za pomocą zwykłych narzędzi;

- ✓ Zapobiega się nieuprawnionemu dostępowi i kontroli dostępu poprzez ustanowienie koncepcji dostępu dla obszarów, które mają być chronione. Można to osiągnąć za pomocą zarówno mechanicznych i elektronicznych systemów kontroli dostępu;
- ✓ Śledzenie alarmów musi być prowadzone przez certyfikowane służby ochrony, centrum kontroli. Alternatywą dla systemu sygnalizacji włamania i napadu jest całodobowa ochrona przez certyfikowane służby ochrony. Należy opracować i zweryfikować plany reakcji na alarm;
- ✓ Wszyscy odwiedzający przedsiębiorstwo podlegają obowiązkowemu wpisowi w księgę wejść/wyjść oraz zapoznaniu się z regulaminem bezpieczeństwa dla gości. Partnerzy handlowi muszą wyrazić zgodę na udokumentowanie zawarcia umowy o zachowaniu poufności;
- ✓ Należy przestrzegać przepisów dotyczących ochrony danych osobowych RODO;
- ✓ Projekty poszczególnych klientów muszą być fizycznie oddzielone. Oddzielenie to można uzyskać poprzez zastosowanie ruchomych urządzeń (np. ruchomych przegród). Ponadto, należy oddzielić opracowanie różnych projektów [6].

15. Bezpieczeństwo organizacyjne w zarządzaniu projektami

W celu zapewnienia bezpieczeństwa i zapobieganiu ujawnieniu informacji stosuje się wymagania organizacyjne:

- ✓ Należy z klientem, interesariuszem podpisać zobowiązanie, tzn. umowę o zachowanie poufności. Wszyscy pracownicy i osoby zaangażowane w projekt zobowiązane są do podpisania oświadczania o nieujawnianiu informacji;
- ✓ Podwykonawcy również muszą podpisać umowę o zachowaniu poufności oraz dochowaniu tajemnicy handlowej;
- ✓ Osoby zaangażowane w realizację projektu muszą obowiązkowo przechodzić szkolenia dotyczące bezpieczeństwa informacji, w szczególności z zakresu przedmiotu ochrony prototypu. Działania takie muszą być udokumentowane pisemnie;
- ✓ Proces kontroli dostępu do obszarów bezpieczeństwa, cofniecie praw dostępu oraz kodeks postępowania musi być wdrożony i udokumentowany pisemnie;
- ✓ Utworzenie dokumentu dotyczącego spisu urządzeń przenośnych do robienia zdjęć oraz filmowania, które mogą być wnoszone i używane na terenie obiektu;
- ✓ Podczas transportu (dotyczy to transportu lotniczego, morskiego, drogowego) pojazdy, komponenty, części zaklasyfikowane, jako wymagające ochrony muszą być odpowiednio chronione przez nieautoryzowanym dostępem, oglądaniem, filmowaniem, robieniem zdjęć [6].

15.3. Szyfrowanie wiadomości

Szyfrowanie wiadomości dotyczy form zapisu fotograficznego, rozmowy telefonicznej, faksu, identyfikowania użytkowników, baz danych, podpisu elektronicznego dokumentów, nienaruszalności danych przesyłanych itp.

Następujące metody szyfrowania przesyłanych danych:

- ✓ Szyfrowanie kluczem symetrycznym, gdzie nadawca i odbiorca wiadomości używają tego samego klucza do szyfrowania i odszyfrowania tekstu wiadomości. Do algorytmu szyfrowania zalicza się: RC4, DES, 3DES, IDEA
- ✓ Szyfrowanie kluczem asymetrycznym polega na używania dwóch kluczy, które uzupełniają się (klucza publicznego i prywatnego). Jeden z kluczy jest znany, natomiast drugi znany jest tylko użytkownikowi.

  Do algorytmu klucza asymetrycznego zalicza się: RSA, ECC, Diffiego- Hellmana, ElGamal, RSA używane w podpisach cyfrowych.
- ✓ Szyfrowanie transportu między systemami e-mail powinien odbywać się za pomocą TLS .
- ✓ Należy szyfrować wiadomości e-mail w bramie szyfrowania wiadomości e-mail (PGP lub S / MIME). Konfiguracja na serwerach firm partnerskich powinna zostać odpowiednio zmieniona [2].

15.4. Podpis cyfrowy

Celem podpisu cyfrowego jest zastąpienie podpisu tradycyjnego. Identyfikacja osoby, która podpisuje dokument oraz uwiarygodnienie autentyczności dokumentów w formie elektronicznej odbywa się podpisem cyfrowym. Taki podpis posiada funkcję spójności, niezaprzeczalności oraz wiarygodności nabywcy.

Nadawca używając swój klucz prywatny do szyfrowania podpisu, podpisuje dokument, natomiast odbiorca odszyfrowuje go kluczem publicznym.

Ponadto zaleca się uwierzytelnienie użytkowników systemu poprzez protokoły zapewniające bezpieczną komunikację:

- ✓ SSL-między partnerem, a serwerem szyfrując wszystkie informacje;
- ✓ S-http- zapewnia głównie bezpieczeństwo protokołowi;
- ✓ SSH- kanał transmisyjny pomiędzy serwerem a partnerem, blokujący odczytywanie przesyłanych treści;
- ✓ SOCKS- kanał łączności przy pomocy internetu, między siecią wew. organizacji, a zewnętrznymi serwerami;
- ✓ PSec- zapewnia bezpieczeństwo dla usług sieciowych.

15.5. Zapora sieciowa

Należy do systemu składających się z rozwiązań programowych, sprzętowo-programowych. Celem firewalla jest monitorowanie przepływu danych informacji. Jest to główny punkt zarządzania systemem ochrony oparty o zasady bezpieczeństwa. Kontroluje zasady użytkowania podmiotów zewnętrznych z zasobów organizacji. Firewalle, monitorujące pracę sieci decydują też, do których zasobów mogą mieć dostęp zewnętrzni użytkownicy, czy też pracownicy.

Należy firewalle odpowiednio skonfigurować zgodnie z obowiązującą PBI, tak by blokować przenikanie złośliwego oprogramowania [5].

16. Bezpieczeństwo zasobów ludzkich

16.1. Przed zatrudnieniem

Warunkiem zatrudnienia nowej osoby w organizacji będzie podpisanie przez pracownika oświadczenia o zachowaniu poufności.

Należy dokładnie określić stanowisko pracy, zadania pracownika i wynikające z tego zakresy powierzonych obowiązków oraz zdefiniować odpowiedzialność pracownika. Kierownictwo powinno wiedzieć, jaki sprzęt powierza pracownikowi oraz do jakich danych będzie miał on dostęp.

Określając i definiując stanowiska pracy, należy określić ich znaczenie dla systemu informatycznego. W zależności od stanowiska, rekrutuje się pracowników wg. specjalnie wytyczonych zasad. Podczas zatrudnienia nowego pracownika, bezwzględnie należy go przeszkolić z zasad dotyczących bezpieczeństwo informacji.

16.2. Podczas zatrudnienia

Kierownictwo jest odpowiedzialne za stały nadzór nad pracownikami w zakresie realizacji wymagań, wynikających z SZBI.

16.3. Po ustaniu stosunku pracy

Zwalniany pracownik powinien przekazać wszystkie informacje dotyczące przetwarzanych aktywów tzn. dokumentów elektronicznych, struktury katalogów, hasła do logowania, klucze kryptograficzne itp. Natychmiast po ustaniu zatrudnienia pracownika, należy go wylogować z systemu informatycznego, likwidując jego konto systemowe oraz sprawdzić działanie aplikacji i urządzeń, do których miał, dostęp.

17. Zarządzanie aktywami

Własność aktywów fizycznych i programowych należy przypisać osobom dysponującym tymi zasobami (pracownicy oraz podmioty zewnętrzne zapewniają, że aktywa należące do omawianej organizacji, a będące w ich posiadaniu w momencie ustania stosunku pracy, czy zawartej wcześniej umowy, należy niezwłocznie zwrócić).

Wymaga się zidentyfikowania wszystkich aktywów w następujący sposób:

Informacyjne aktywa, do których zalicza się: zbiory danych, pliki, nośniki pamięci, struktury IT, procedury dotyczące bezpieczeństwa informacji, system kopii zapasowych, materiały edukacyjne, plan ciągłości działania;

Oprogramowanie, dzięki któremu przetwarza się dane, systemy operacyjne, biurowe;

Fizyczne aktywa, do których zalicza się: serwery, nośniki magnetyczne oraz mechaniczne, urządzenia peryferyjne (drukarki, skanery), komputery, sprzęt sieciowy, pomieszczenia wraz z wyposażeniem (oświetlenie, ogrzewanie) [7]. Należy wyznaczyć stanowisko dla osoby odpowiedzialnej za wszystkie aktywa oraz urządzenia do przechowywania ich. Do zakresu obowiązków takiej osoby należy: poprawne klasyfikowanie informacji, okresowe przeglądy dostępu.

Należy określić sposoby oraz zasady korzystania z wymienionych aktywów dla partnerów, dostawców, pracowników oraz osób, które, w jaki kolwiek sposób współpracują z organizacją. Może to dotyczyć, np. wytycznych o sposobach użytkowania urządzeń przenośnych typu laptop, telefon, dyski pamięci poza obszarem organizacji. Osoby współpracujące z organizacją są odpowiedzialne za powierzone im aktywa oraz świadome bezpiecznego używana powierzonych akywów.

17.1. Klasyfikacja informacji

Posiadane zbiory informacji należy dokładnie spisać, określając dostęp pracowników do informacji. Należy uszeregować je pod względem znaczenia i podatności na zagrożenie. Takie podejście pomoże ustalić kolejność i ważność ochrony informacji, wskazując na priorytet ochrony dla kluczowych, strategicznych informacji. W organizacji obowiązuje sposób sklasyfikowania informacji, określający jej hierarchiczność. Klasyfikacja informacji oznacza, więc kategoryzacje informacji na różnych poziomach w zależności od wartości dla organizacji. Klasyfikuje się informacje, wg. określonych kryteriów, dotyczących wymogów prawnych, krytyczności, wartości, wrażliwości, poufności, integralności, dostępności, ze wskazaniem na określony sposób jej ochrony.

- ✓ Kierownicy działów zobowiązani są do uzyskania wiedzy od przedstawicieli działów na temat rodzaju i typu informacji przetwarzanych w tych działach pod kątem atrybutów BI.
- ✓ Aby unikać różnic pomiędzy systemami i jego podsystemami należy utworzyć standardowy spójny systemu klasyfikowania informacji dla wszystkich, komórek organizacyjnych współpracujących ze sobą;
- ✓ Wymagane jest opracowanie definicji dla poziomów informacji oraz utworzenie ścisłej instrukcji dla właścicieli informacji tak, by każdy bez problemów mógł sklasyfikować informacje występujące w postaci drukowanej lub elektroniczej;
- ✓ Niewłaściwa klasyfikacja informacji, a później wynikające z niej postępowanie może doprowadzić do powstania zagrożenia, a w konsekwencji ujawnienia informacji. Jeśli wybrany poziom klasyfikacji jest zbyt niski lub zbyt wysoki to zabezpieczenia mogą nie zadziałać [8].

17.2. Zasady klasyfikacji informacji

Przykład zastosowania klasyfikacji informacji:

- ✓ Informacja o strategicznym znaczeniu- ujawnienie, takiej informacji spowoduje utratę prestiżowej pozycji na rynku zbytu i związane z tym straty finansowe.
- ✓ Informacja o ważnym znaczeniu- ujawnienie, takich informacji grozi załamaniu konkurencyjności organizacji, a równoczesnym wzmocnieniu, pozycji konkurencji.
- ✓ Informacja zastrzeżona- podczas ujawnienia organizacja nadwyręża swoją dobrą opinię i naraża na szkodę interes pracowników, bagatelizując bezpieczeństwo personalne (ujawnienie zatrudnionych danych osobowych)
- ✓ Informacje pozostałe- zaliczamy do tej grupy informacje niezbędne do prowadzenia działalności,

- ✓ Informacje jawne- informacje, które nie posiadają dużej wartości i mogą zostać upublicznione, jawne dla ogółu, logo przedsiębiorstwa, reklama, znaki towarowe.

Pierwsze cztery grupy informacji zaliczamy do tajemnicy przedsiębiorstwa [8].

17.3. Etykietowanie informacji- proces oznaczenia informacji

Formą oznaczenia zasobów jest prawidłowe etykietowane informacji konieczne do bezpiecznego obchodzenia się z nią. Etykietowanie dotyczy dokumentów w postaci fizycznej. Ponadto, w formie elektronicznej wymaga się elektronicznego oznakowania, widocznego również i dla innych użytkowników systemu, zgodnego z upoważnieniem wcześniej nadanym na etykiecie.

Dlatego stosuje się oznakowanie, zgodne z przyjętą klasyfikacją.

- ✓ Zarówno odbiorca, jak i podmiot przetwarzający oraz właściciel dokumentu powinien być oznaczony, zgodnie z klauzulą o zachowaniu poufności;
- ✓ Ponadto, oprócz schematu klasyfikacji, stosuje się kodowanie kolorystyczne podczas otwierania informacji cyfrowych, tzn. e-maila, czy pliku prezentacyjnego. Dzięki temu odbiorca ma możliwość wizualne wskazać i ocenić poziom klasyfikacji informacji cyfrowej.

18. Monitorowanie i weryfikacja zabezpieczenia

Podmioty gospodarcze, korzystające w swojej praktyce biznesowej z sieci teleinformatycznych, bezwzględnie są zobowiązane do dokładnego monitorowania skuteczności kontroli bezpieczeństwa informacji. Ponadto zespół IT, jest zobowiązany do cotygodniowego sprawdzania poprawności logowania się użytkowników oraz kontrolowania ilości czasu spędzonego, przez użytkownika w danym systemie [6].

19. Proces dotyczący pracy zdalnej

- ✓ Administrator pracownika pracującego zdalnie, zobowiązany jest do udostępnienia mu służbowego sprzętu komputerowego;
- ✓ Wysyłane wiadomości w sieciach teleinformatycznych muszą być zaszyfrowane szyfrem (kluczem symetrycznym lub asymetrycznym albo podpisem cyfrowym), polegającym na utajnieniu wiadomości, (aby niemożliwym stało się odczytanie przez postronną osobę);
- ✓ Uwierzytelnienie wiadomości od pracowników odbywa się poprzez wybrane protokoły: SSL, http (jeden z najczęściej wybieranych protokołów komunikacji w Internecie. Szyfruje komunikację między klientem a serwerem sieciowym), SSH, SOCKS, PSec;
- ✓ Pracownik, korzystający z urządzenia służbowego nie może korzystać ze stron zewnętrznych, a wyjątkiem wcześniej zgody administratora lub przełożonego.
- ✓ Pracownik na każde wezwanie administratora, zobowiązany jest do oddania urządzenia celem weryfikacji i sprawdzenia;
- ✓ Organizacja gospodarcza stosuje dostęp zdalny za pośrednictwem VPN.

20. Incydenty zagrażające bezpieczeństwu informacji w organizacji

20.1. Zdarzenia, które mogą wywołać zagrożenie lub incydent zagrażający bezpieczeństwu informacji w organizacji

Do zagrożeń systemu BI zaliczono:

- ✓ Nieprzestrzeganie zasad PBI przez pracowników;
- ✓ Niezabezpieczenie lub nieodpowiednie zabezpieczenie sprzętu informatycznego po zakończeniu pracy
- ✓ Niezabezpieczenie lub niewłaściwe zabezpieczenie fizyczne pomieszczeń, w tym urządzeń i dokumentów.

Do incydentów zaliczono:

- ✓ Błędy ludzkie, spowodowane niewłaściwymi procedurami (pozostawienie dokumentów w miejscach widocznych bez nadzoru, kluczy w zamkach, urządzeń przenośnych typu dyski twarde, pendrive, błędy informatyków);
- ✓ Zdarzenia losowe typu pożar obiektu, powódź, utrata zasilania, utrata łączności, uszkodzenie komputerów, dysków pamięci, zaginięcie danych;
- ✓ Awarie oprogramowania i sprzętu komputerowego;
- ✓ Incydenty wywołane celowym ujawnieniem informacji osobom nieuprawnionym, celowe zniszczenie dokumentów, włamanie do systemu informatycznego, zainstalowanie szkodliwego oprogramowania.

20.2. Sposób postępowania w sytuacji stwierdzenia naruszenia bezpieczeństwa informacji

Z uwagi na to, że każdy pracownik, przetwarzający dane jest odpowiedzialny za ich bezpieczeństwo, to w sytuacji stwierdzenia zagrożenia powinno się niezwłocznie poinformować o zaistniałym fakcie bezpośrednio przełożonego. Informację należy przekazać osobiście lub telefonicznie, e -mailowo, podając imię i nazwisko osoby zgłaszającej, dokładny czas wskazujący na naruszenie bezpieczeństwa danych oraz opis zdarzenia i stan techniczny sprzętu, na którym doszło do ujawnienia informacji. Sposób postępowania podczas zidentyfikowania zagrożenia został szczegółowo przedstawiony i opisany w procedurach, zgodnych ze schematem postepowania systemowego.

Sytuacje, które można uznać, jako naruszenie są następujące:

- ✓ Brak możliwości otworzenia i zalogowania się do aplikacji zawierającej określone informacje;
- ✓ Zmniejszona możliwości wykonywania określonych operacji dotychczas dostępnych;
- ✓ Wygląd aplikacji inaczej niż zazwyczaj;
- ✓ Zakres danych zwiększony bardziej niż zazwyczaj;
- ✓ Zakres danych zmniejszony bardziej niż zazwyczaj;
- ✓ Widoczne spowolnienie systemu informatycznego
- ✓ Widoczne niestandardowe komunikaty;
- ✓ Widoczne ślady włamania do systemu komputerowego;
- ✓ Kradzież nośników danych;
- ✓ Kradzież materiału kryptograficznego;
- ✓ Kradzież sprzętu informatycznego;
- ✓ Podejrzenie zniszczenia elementów systemu informatycznego, który przetwarza informacje;
- ✓ Komunikat o zainfekowaniu systemu informatycznego.

Zabezpieczając miejsce zdarzenia, powinno się zabezpieczyć wszystkie dokumenty pomocne w ustaleniu okoliczności naruszenia. Należy je podpisać oraz oznakować datą.

W wyniku pojawienia się zagrożenia należy dowiedzieć się czy osoba nieuprawniona otrzymała dostęp do systemu lub pomieszczeń oraz określić, z jakimi danymi związane jest naruszenie. Natychmiast, eliminując czynnik bezpośredniego zagrożenia należy sporządzić protokół z przeprowadzonych czynności. Jeśli odnotowano wysoki poziom ryzyka naruszenia praw i wolności osób fizycznych to należy poinformować w ciągu 72 h Urząd Ochrony Danych Osobowych.

Wówczas, gdy poziom ryzyka jest wysoki zaleca się powzięcie działań przez Administratora systemu teleinformatycznego, poprzez zmianę hasła dla użytkownika, odłączenie fizyczne urządzeń, które mogłyby umożliwić dostęp do bazy danych oraz wylogowanie podejrzanej osoby o naruszenie. Ma to na celu zabezpieczenie systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia oraz przywrócenie pierwotnego stanu, czyli sprzed zaistnienia incydentu.

Ponadto, zaleca się, aby Administrator systemu teleinformatycznego podjął działania mające za zadanie usunięcie podobnych naruszeń w czasie przyszłym, a przy tym zmniejszenie ryzyka poprzez wyeliminowanie negatywnych jego skutków.

Nie bez znaczenia jest fakt, prowadzenia ewidencji zdarzenia w rejestrze zdarzenia związanego z zaistniałymi okolicznościami. W omawianym rejestrze zdarzenia umieszcza się imię i nazwisko osoby zgłaszającej incydent, kto przyjął zgłoszenie oraz kiedy (dokładna data), jakie działania podjęto, aby

wyjaśnić przyczyny pojawienia się incydentu. Podjęte czynności są niezbędne do przeprowadzenia analizy ryzyka, opracowaniu wyników oraz ustalenia, kierunku działań naprawczych.

21. Monitoring

Należy dołożyć wszelkich starań, aby wykrywać nieuprawnione działania dotyczące przetwarzania informacji, W tym celu system BI powinien być monitorowany, a pojawiające się zagrożenia odnotowane w rejestrze zdarzeń.

- Administrator systemu teleinformatycznego jest zobowiązany do monitorowania możliwości pracy systemów komputerowych z przed zdarzenia, które powoduje utratę pracy systemu, jak i przywrócenia go do stanu normalnego;
- Administrator systemu teleinformatycznego powinien bezzwłocznie dokonać wszelkich starań, aby systemy komputerowe wróciły do stanu z przed zdarzenia;
- Administrator systemu teleinformatycznego jest odpowiedzialny za weryfikację środków przepięć oraz utratę prądu;
- Administrator systemu teleinformatycznego powinien posiadać wiedzę o poprowadzeniu drugiej linii zasilania prądotwórczego i znać czas pracy agregatu prądotwórczego oraz wiedzieć czy agregaty automatycznie się załączą;
- Administrator systemu teleinformatycznego zakupuje dla organizacji agregaty prądotwórcze tylko z atestami;
- Administrator systemu teleinformatycznego odpowiada za zapewnienie ciągłości pracy;
- Osoba odpowiedzialna za nadawanie uprawnień będzie odpowiedzialnie sprawdzać aktualność nadanych uprawnień oraz ich zasięg.

22. Postanowienia końcowe

- ✓ PBI jest dokumentem podstawowym, długoterminowym oraz wewnętrznym, którego inicjatorem utworzenia jest zarząd a odpowiedzialność za prace nad dokumentem spoczywają na pełnomocniku ds. bezpieczeństwa;
- ✓ Pełnomocnik ds. bezpieczeństwa odpowiada za zgodność PBI z rzeczywistymi wymaganiami technicznymi i prawnymi, natomiast to kierownicy poszczególnych działów są odpowiedzialni za kontrolę nad przestrzeganiem jej w swoich działach;
- ✓ Kodeks pracy przewiduje konsekwencje za nieuzasadnione zachowania niedopełnienia obowiązków wynikających z PBI traktując je, jako ciężkie naruszenie. Grozi za to kara dyscyplinarna;
- ✓ Należy wszcząć postępowanie dyscyplinarne wobec osoby, która nie podjęła żadnych działań w przypadku naruszenia bezpieczeństwa informacji. W szczególności dotyczy to osób, które nie powiadomiły o wystąpieniu incydentu przełożonego oraz pełnomocnika ds. bezpieczeństwa;

Literatura

[1]. Łuczak J., Trybulski M.; Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001

[2]. Nowicki A., Turek T.: Technologie informacyjne dla ekonomistów. Narzędzia zastosowania. 2010

[3]. Nowak A., Scheffs W.: Zarządzanie bezpieczeństwem informacyjnym Akademia Obrany Narodowej 2010r.

[4]. Jańczak J., Nowak A.: Bezpieczeństwo informacyjne Wybrane problemy Akademia Obrony Narodowej 2012r.

[5]. Nowicki A.; Komputerowe wspomaganie biznesu Placet 2008

[6]. Pańkowska M.; Zarządzanie zasobami informatycznymi Difin 2001

[7]. Polaczek T.; Audyt bezpieczeństwa informacji w praktyce Helion

[8]. Wojciechowska-Filipek S., Ciekanowski Z.; Bezpieczeństwo funkcjonowania w cyberprzestrzenią Jednostka-Organizacja-Państwa Cedewu 2016

PROCEDURY ZGODNE ZE SCHEMATEM POSTĘPOWANIA SYSTEMOWEGO

<table>
<tr><td colspan="5">Procedura postępowania w przypadku wykrycia zagrożenia</td></tr>
<tr><td>Nazwa dokumentu</td><td>Podpis osoby odpowiedzialnej</td><td>Procedura operacyjna nr.1</td><td>Data opracowania</td><td>Podmiot odpowiedzialny za realizację procedury: kierownicy poszczególnych działów, pełnomocnik ds. bezpieczeństwa, pracownicy działu analizy ryzyka.</td></tr>
<tr><td colspan="5">Cel procedury:
Określenie procesu organizacyjnego dotyczącego postępowania podczas weryfikowania incydentu.
Procedura służy zapewnieniu odpowiedniego sposobu zgłaszania i reagowania na wystąpienie incydentu.
Uczestnicy procedury: Pracownicy wykrywający incydent, kierownicy działów, w których wystąpił incydent.
Kiedy procedura jest uruchamiana: zgłoszenie incydentu
Opis postępowania:
➢ Każda zatrudniona osoba, stwierdzająca pojawienie, się incydentu jest zobowiązana do niezwłocznego zgłoszenia, takiej sytuacji bezpośredniemu przełożonemu.
➢ Weryfikacja zdarzenia przez przełożonego.
➢ Jeżeli zagrożenie nie zostało potwierdzone, to nie podejmujemy żadnych działań.
➢ W przypadku potwierdzenia zdarzenia, należy bezzwłocznie poinformować pełnomocnika ds. bezpieczeństwa o wystąpieniu incydentu (w formie telefonicznej, e-mailowej, osobistej, pisemnej).
➢ Potwierdzenie faktu zaistnienia incydentu przez pełnomocnika ds. bezpieczeństwa (czy jest realne czy też nie) i odnotowanie w rejestrze incydentów.
➢ Określnie przez pełnomocnika czy dany incydent klasyfikuje się jako zagrożenie.
➢ W przypadku uznania danego incydentu, jako zagrożenia należy zweryfikować, czy znajduje się ono w katalogu zagrożeń
➢ Jeżeli zagrożenia znajduje się w katalogu zagrożeń, należy sprawdzić czy przypisane zabezpieczenia będą wystarczająco skuteczne. w przypadku braku wystarczającej skuteczności zabezpieczenia uruchomienie procedury nr2.
➢ Jeżeli zagrożenie nie znajduje się w katalogu zagrożeń, należy opisać nowe zagrożenie oraz dokonać jego analizy ryzyka.
➢ Odnotować wystąpienie nowego zagrożenia w rejestrze zagrożeń, które nie było, dotychczas zdefiniowane
➢ W przypadku zidentyfikowania nowego zagrożenia uruchomienie procedury nr 2.</td></tr>
</table>

Procedura poszukiwania zabezpieczeń				
Nazwa dokumentu	Podpis osoby odpowiedzialnej	Procedura operacyjna nr.2	Data opracowania	Podmiot odpowiedzialny: osoby pracujące w dziale analizy ryzyka, pełnomocnik ds. bezpieczeństwa, kierownicy działów.

Cel procedury:

Znalezienie zabezpieczenia dla zidentyfikowanego zagrożenia

Uczestnicy procedury:

- Osoby pracujące w dziale analizy ryzyka
- Kierownik określonego działu, w którym doszło do powstania zagrożenia

Kiedy procedura jest uruchamiana:

- przez procedurę nr1 wówczas, gdy szukamy środków zabezpieczających dla pojawienia, się zagrożenia
- jeżeli dla danego zagrożenia otrzymany poziom ryzyka, jest nieakceptowalny

Opis postępowania:

- Zweryfikowanie zabezpieczeń, dla nowo zidentyfikowanego zagrożenia.
- W przypadku stwierdzenia posiadania zabezpieczenia dedykowanemu zagrożeniu, sprawdzenie parametrów tego zabezpieczenia.
- W przypadku braku zabezpieczenia opracowanie nowego zabezpieczenia, dla ujawnionego zagrożenia i kolejno uzupełnienie katalogu zagrożeń. Przypisanie nowych zabezpieczeń do ujawnionego zagrożenia (uzupełnienie katalogu zabezpieczeń o dane zabezpieczenie).
- Przeprowadzenie analizy ryzyka, dla określonych zabezpieczeń.
- Jeżeli zabezpieczenia, są wystarczające i występuje akceptowalny poziom ryzyka, wówczas nie poszukujemy nowych zabezpieczeń.
- Jeżeli zabezpieczenia, są niewystarczające i występuje nieakceptowalny poziom ryzyka, poszukiwanie innych zabezpieczeń.
- Określenie celu i skuteczności zastosowania nowego zabezpieczenia.
- W przypadku konieczność wprowadzenia nowych środków zabezpieczających uruchamianie procedury nr 3.

Procedura informowania i decyzji zarządu				
Nazwa dokumentu	Podpis osoby odpowiedzialnej	Procedura operacyjna nr.3	Data opracowania	Podmiot odpowiedzialny: osoby upoważnione przez zarząd do realizacji tego typu działań, dyrektorzy działów.

Cel procedury:

Sposób przekazania do zarządu informacji o propozycji nowych zabezpieczeń dedykowanych zidentyfikowanym powstałym zagrożeniom.

Uczestnicy procedury:

Dyrektorzy pionów, kierownicy działów, członkowie zarządu.

Kiedy procedura jest uruchamiana: wywołana wprowadzeniem procedury nr 2.

Opis postępowania:

- Przekazanie informacji o potrzebie zabezpieczenia (wynika z przeprowadzonej analizy ryzyka).
- Dokonanie oceny ekonomicznej wprowadzenia nowego zabezpieczenia.
- Podjęcie decyzji, przez organ zarządczy o wprowadzeniu proponowanego zabezpieczenia.
- W przypadku braku zgody członków zarządu, na proponowane działania zabezpieczające podjęcie, przez zarząd strategicznej decyzji o zmianie wytycznych poziomu akceptowalności ryzyka. Przejęcie przez członków zarządu poziomu ryzyka wcześniej nieakceptowalnego.
- W przypadku, jakiejkolwiek zmiany specyfikacji lub modyfikacji zabezpieczenia wymaga, się poddania środka zabezpieczającego procesowi ponownej analizy ryzyka.
- Uruchomienie procedury nr 4.

Procedura wdrażania nowych zabezpieczeń				
Nazwa dokumentu	Podpis osoby odpowiedzialnej	Procedura operacyjna nr.4	Data Opracowania	Podmiot odpowiedzialny: pełnomocnik ds. bezpieczeństwa, Inspektor Ochrony Danych Osobowych, kierownicy działów.

Cel procedury:
Wdrożenie nowych zabezpieczeń do organizacji.
Zapobieganie powstawaniu ponownych sytuacji, w których ujawni się tego typu zagrożenie lub podobne temu.
Uczestnicy procedury:
Pracownicy działów, w których będą dokonywane zabezpieczenia, dział analizy ryzyka.
Kiedy procedura jest uruchamiana:

- Wywołana decyzją zarządu. Uruchomienie procedury z pozycji nr 3.

Opis postępowania:

- Przekazanie do realizacji nowego zabezpieczenia.
- W przypadku zmiany, jakichkolwiek planów lub ustaleń lub, też innych parametrów technicznych urządzeń zabezpieczających wymaga, się uruchomienia procedury nr.2.
- Uzupełnienie katalogu zabezpieczeń z pełnym opisem wprowadzanego zabezpieczenia i jego wpływu, na zidentyfikowane zagrożenie.
- Dokumentowanie procedury wdrożenia
- Zabezpieczenie pełnej dokumentacji wdrożenia zabezpieczenia.

Częstochowa 06.12.2021r.

Dissertation abstract

D. thesis of Estera Pietras, M.Sc.

titled. "Information Security Management in

companies of the automotive industry".

Observing the growing interest of businesses in protecting their information assets and the dynamically emerging threats of information loss, one can conclude, that the problem of ensuring information security in companies is a topical issue and requires detailed analysis. Management boards of business organizations, aware of the imperfections of their information protection systems, are looking for effective methods of identifying emerging threats, combined with proper risk management. Thus, in the management of the enterprise, one of the very important factors is to prepare for the appearance of a threat and to create opportunities to skillfully reduce its impact on the information resources held.

Due to the occurring problems of inadequate protection during storage, processing and sharing of information, the dissertation attempts to enhance the knowledge of information security and proposes a system to reduce the risk of information loss.

The study adopted the following hypothesis: *"The intense increase in the number of information security threats in enterprises requires the use of adaptable security management systems in which technical and procedural measures are adapted to the requirements determined by current information loss risk analyses."*

The utilitarian aim of the study was to develop guidelines in the field of information security management, which will take into account important, and so far ignored threats, for a selected group of companies, belonging to the automotive sector.

As a result of literature analysis and empirical research, the dissertation's aim was achieved by identifying new threats and concepts of conduct, in the information security management system. The importance of information in companies was highlighted, the way of its protection was shown taking into account the results of risk analysis. The paper identifies subsystems for information flow and security and develops a system design to reduce the risk of information loss.

Surveys were conducted among senior and lower saber management positions and employees in non-management positions. The use of analysis tools (survey, interview, observation, and experiment) allowed us to identify many deficiencies in information security systems. A taxonomy of hazard sources was performed according to the 5M method. The discussed methods enabled the author of this paper to describe the investigated enterprises, establish facts, motivation of employees and their level of awareness towards the stored information and expectations concerning the applied security in the employing unit. In addition, an experiment involving a simulated attack aimed at obtaining potentially protected information showed that organizations lack resilience to real-world events that could result in extortion, destruction, or modification of information.

The risk estimation process created a new catalog of grouped risks that remains open to dynamically emerging new sources of risk. Threats were assessed through a risk analysis process based on confidentiality, integrity, availability, accountability, authenticity, reliability. The adopted analysis

methodology led to the determination of the risk of loss of information, or some of its attributes, which turned out to be at a high level. Such a condition cannot be acceptable in any enterprise and requires corrective action to be taken to ensure information security.

Taking into account the construction of information security management systems, the paper develops an information security management system design, reducing the risk of information loss, adapted to the specifics of the analyzed enterprises. The system consists of the following subsystems: project development security, information exchange with the external environment, production and technology used, users and database. Although the research was conducted in nine companies in the automotive industry, the design is versatile enough to be used in other organizations of similar structure and size. The paper mapped the systemic patterns in the form of procedures to facilitate threat identification and faster response to emerging information security incidents.

Conducting research and analyzing the obtained results, the analysis of the risk of information security loss in the studied group of enterprises was performed twice. The first analysis considered the identified risks and existing safeguards and found an unacceptable level of risk. Proposing new safeguards dedicated to the identified threats made it possible to reduce the level of risk of losing information or its attributes to an acceptable level. On the other hand, the implementation of an information security management system should significantly improve management processes in terms of identifying new threats and developing dedicated security measures as quickly as possible.