ANALIZA BEZPIECZEŃSTWA FIZYCZNEGO W KONTEKŚCIE DOSTĘPU DO INFORMACJI

PHYSICAL SECURITY ANALYSIS IN THE CONTEXT OF ACCESS TO INFORMATION

Michał PAŁĘGA

palega.michal@interia.pl

Marcin KNAPIŃSKI

knapinski.marcin@wip.pcz.pl

Politechnika Częstochowska

Wydział Inżynierii Produkcji i Technologii Materiałów

Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa

Streszczenie: W niniejszej publikacji przedstawiono wybrane zagadnienia związane z bezpieczeństwem fizycznym w aspekcie szeroko pojmowanej ochrony informacji w przedsiębiorstwie. Zasady bezpieczeństwa fizycznego stanowią jeden z podstawowych elementów kompleksowego programu zarządzania bezpieczeństwem informacji i dotyczą bezpośrednio sposobów zabezpieczenia biur i pomieszczeń przed zagrożeniami zewnętrznymi związanymi z nieuprawnionym dostępem do informacji. Ponadto, w artykule zaprezentowano także charakterystykę oraz analizę wybranych rodzajów zabezpieczeń stosowanych w badanej jednostce organizacyjnej. Wyniki przeprowadzonych badań pozwoliły również wskazać słabe miejsca i niedociągnięcia występujące w omawianym obszarze oraz zaproponować działania korygujące i profilaktyczne.

Abstract: In this publication selected physical security issues in the aspect of enterprise information security were presented. Physical security rules are one of the cornerstones of a comprehensive information security management program and concern how to protect your offices and premises against external threats related to unauthorized access to information. Also, in this article characteristics and analysis of selected types of security used in the study organization were presented. The results of the study also weaknesses in the area and suggested corrective and preventive measures.

Słowa kluczowe: bezpieczeństwo fizyczne, bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji, ochrona informacji

Key words: physical security, information security, information security management system, protection information

WSTĘP

Zapewnienie właściwego poziomu bezpieczeństwa gromadzonych, przetwarzanych i wymienianych informacji wymaga realizacji szerokiego spektrum działań i procesów oraz zaangażowania różnego typu sił i środków (w tym zabezpieczeń fizycznych).

Ochrona fizyczna stanowi najstarszy, a jednocześnie najważniejszy mechanizm zabezpieczania zasobów materialnych i informacyjnych przedsiębiorstwa. Postrzegana jest ona jako pierwsza linia obrony przed wszelkiego rodzaju zagrożeniami. W opinii specjalistów, jeżeli w przedsiębiorstwach bądź instytucjach nie wdrożono podstawowych zabezpieczeń fizycznych wówczas nie można mówić o istnieniu jakiegokolwiek bezpieczeństwa. Należy

także dodać, iż w dobie powszechnej informatyzacji przedsiębiorstwa ograniczają się do rozwiązań teleinformatycznych, pomijając rolę jaką odgrywają elementarne narzędzia ochrony fizycznej. Stąd też podkreślenia wymaga fakt, iż zastosowanie właściwych zabezpieczeń fizycznych może uchronić organizację przed takimi zagrożeniami jak: włamanie, kradzież sprzętu komputerowego lub/i elektronicznych nośników informacji, awaria zasilania czy sieci teleinformatycznej (Nowak, Scheffs 2010). Norma PN-ISO/IEC 27002:2014 podaje natomiast, iż ochrona fizyczna umożliwia „*zapobieganie nieuprawnionemu dostępowi, uszkodzeniom i ingerencji w pomieszczenia instytucji i jej informacje*".

Celem publikacji jest wskazanie podstawowych elementów składających się na bezpieczeństwo fizyczne oraz ich znaczenia dla ochrony zasobów informacyjnych. Ponadto, w artykule dokonano analizy zabezpieczeń fizycznych wdrożonych w wybranym przedsiębiorstwie produkcyjnym. Na podstawie przeprowadzonego wywiadu z wybranymi pracownikami firmy oraz dokonanej obserwacji nieuczestniczącej zidentyfikowano niedociągnięcia i nieprawidłowości w obszarze bezpieczeństwa fizycznego. Na ich podstawie opracowano koncepcję doskonalenia zarządzania bezpieczeństwem fizycznym, która uwzględnia nie tylko zastosowanie środków ochrony, ale także rozwiązania organizacyjne związane z dostępem do informacji.

1. Ochrona fizyczna, a bezpieczeństwo informacji

Bezpieczeństwo fizyczne uznawane jest za najstarszy, a zarazem najbardziej istotny mechanizm ochrony zasobów materialnych i niematerialnych (w tym informacyjnych) organizacji stanowiący pierwszą linię obrony przed różnego rodzaju zagrożeniami. Brak odpowiedniej ochrony przed włamaniem, kradzieżą sprzętu, może powodować uszkodzenie lub niedostępność zasobów, a w konsekwencji prowadzić do zakłócenia ciągłości działania przedsiębiorstwa (Nowak, Scheffs 2010).

Wobec tego, należałoby zgodzić się z normą PN-ISO/IEC 27002:2014 stanowiącą, że celem ochrony fizycznej jest przede wszystkim zapobieganie przed nieuprawnionym dostępem, uszkodzeniem i ingerencją w pomieszczenia instytucji i jej informacje.

Na podstawie dostępnych publikacji (Staniec, Zawiła – Niedźwiecki 2008, Rozbicki, Ryżko, Sławiński 2000) można stwierdzić, że mechanizmy ochronne ukierunkowane są na zabezpieczenie zasobów informacyjnych przed uszkodzeniem, zniszczeniem bądź ujawnieniem oraz mają na celu zapobieganie przed nieuprawnionym dostępem, czy też zakłóceniem usług telekomunikacyjnych. W tym celu niezbędne działania koncentrują się

wokół procedur dotyczących dostępu do pomieszczeń bądź systemów, sprzętu komputerowego oraz innych urządzeń gromadzących informacje.

Wynika więc z tego, że zasadniczym elementem bezpieczeństwa fizycznego są chronione w sposób nieprzerwany wszystkie trwałe wartości determinujące istnienie oraz funkcjonowanie przedsiębiorstwa. Zaliczyć do nich można:

- ludzi (np. personel, gości oraz potencjał intelektualny zatrudnionych);
- rzeczy (np. teren, budynki, kapitał finansowy, mienie trwałe oraz ruchome – własne i powierzone);
- informacje/ dane (np. własne i powierzone);
- elementy infrastruktury zewnętrznej (np. instalacje: energetyczną, wodno – kanalizacyjną, centralnego ogrzewania, sieci teleinformatycznej, klimatyzacyjną).

Aby organizacje mogły osiągnąć dostateczny poziom bezpieczeństwa dla wskazanych powyżej zasobów, zaleca się wprowadzenie odpowiednich barier fizycznych. Przykładem tego mogą być: drzwi, wzmocnione okna, zamki, ogrodzenia, bramy wejściowe, kolczatki ochronne przy wjeździe i wyjeździe z parkingu. Zabezpieczenia te mogą być wspomagane przez systemy ochrony technicznej, takie jak: systemy monitoringu wizyjnego, systemy alarmowe wewnętrzne i zewnętrzne, systemy kontroli dostępu, a także systemy sygnalizacji pożarowej i gaśniczej.

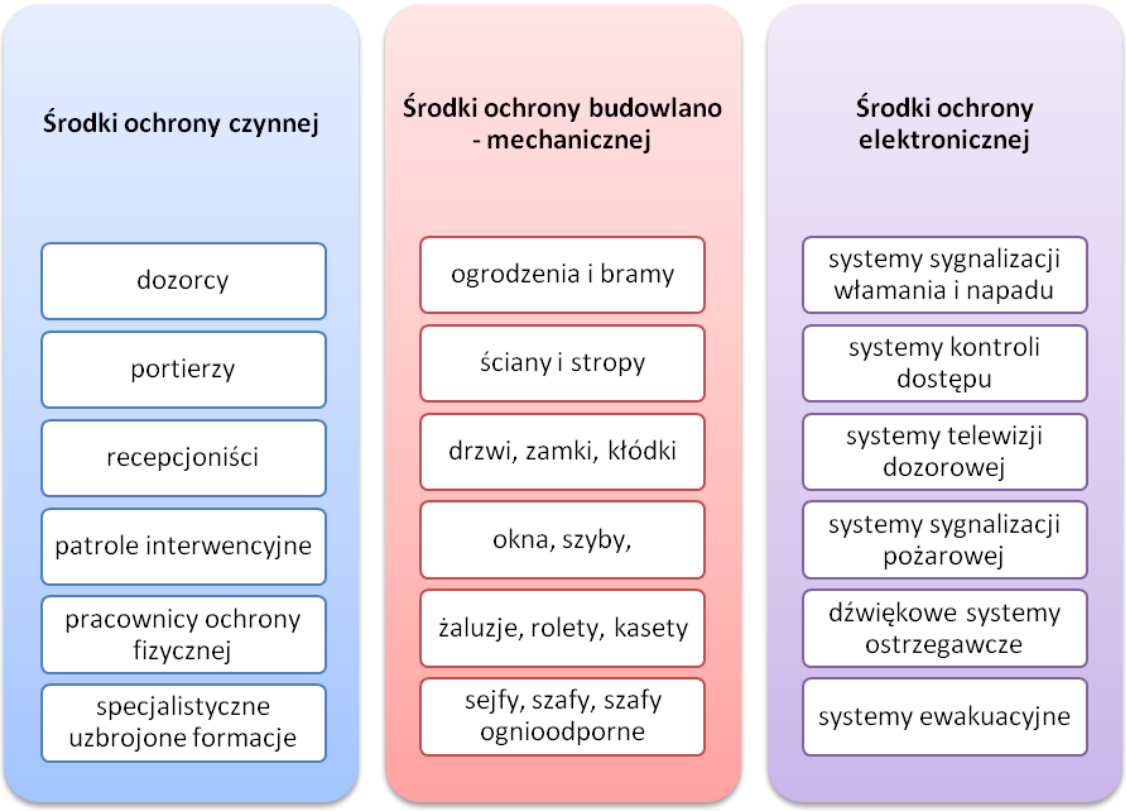
Przyjmuje się, że podstawą skutecznego systemu ochrony fizycznej jest jasny i spójny podział obiektu na strefy zabezpieczające. Ze względu na sposób ich ochrony można podzielić je na strefy: ogólnodostępne, z ograniczonym dostępem, szczególnie chronione oraz zastrzeżone. Dla każdej z wymienionych stref należy przyporządkować oraz zastosować odpowiednie środki ochronne oraz ograniczyć do minimum liczbę osób mających dostęp do kluczowych pomieszczeń obiektu.

Podstawowa funkcjonalność stref ochronnych polega przede wszystkim na (Kifner 1999):

- ograniczeniu liczby niebezpieczeństw (zagrożeń);
- ułatwianiu lokalizacji pojawiania się nowych zagrożeń, na skutek przemian środowiskowych i technologicznych;
- minimalizowaniu możliwości podsłuchu;
- umożliwianiu szybkiej i bezproblemowej rotacji umiejscowienia obiektu chronionego;
- umożliwianiu dobrego, a przy tym nie wyróżniającego się oznakowania strefy ochronnej;

- ograniczaniu możliwości nadużyć za pomocą skutecznego systemu kontrolowania.

Istotnym czynnikiem, w zakresie ochrony fizycznej jest to, aby zastosowane zabezpieczenia były kompleksowe, komplementarne (wzajemnie się uzupełniały), racjonalne (zaakceptowane przez użytkowników) i efektywne (koszt zabezpieczeń nie może być wyższy niż wartość chronionych zasobów). Oprócz tego powinny one obejmować wszystkie rodzaje zabezpieczeń, przedstawione na rysunku 1.



Rys. 1. / Fig. 1. Podział zabezpieczeń fizycznych

Źródło: Opracowanie własne.

Reasumując, w zakresie ochrony fizycznej informacji należy wprowadzić następujące wytyczne i zabezpieczenia: (Staniec, Zawiła – Niedźwiecki 2008)

- strefa ochronna powinna być precyzyjnie wyznaczona;
- strefa budynku lub pomieszczeń, w której mieszczą się urządzenia do przetwarzania danych musi być właściwie zabezpieczona pod względem fizycznym, tak aby nie zawierała przerw, ułatwiających włamanie;
- ściany zewnętrze powinny charakteryzować się wytrzymałą konstrukcją;
- drzwi zewnętrzne należy odpowiednio zabezpieczyć, np. w system kontroli dostępu, czy system włamania i napadu;
- na terenie budynku należy zorganizować recepcję, obsługiwaną przez człowieka;

- zabezpieczenia fizyczne trzeba rozłożyć począwszy od podłogi, a skończywszy na suficie, celem ochrony obiektu przed zagrożeniami środowiskowymi, takimi jak np. powódź czy pożar;
- drzwi przeciwpożarowe muszą być wyposażone w zamek samozatrzaskowy, a także zabezpieczone alarmem.

Poza tym, istotnym elementem w systemie ochrony fizycznej jest wprowadzenie procedur uprawniających do wejścia, przebywania oraz wyjścia z poszczególnych pomieszczeń obiektu (np. przepustki, identyfikatory). Oprócz tego, należy określić zasady przyznawania uprawnień poszczególnym pracownikom organizacji oraz wprowadzić okresową kontrolę przyznawanych uprawnień. Rozwiązania tego typu mogą zapewnić dostęp do pomieszczeń tylko upoważnionym użytkownikom. W ten sposób można ograniczyć nadużycia ze strony nieuczciwego personelu. Należy mieć również na uwadze opracowanie oraz przestrzeganie zasad organizacyjnych, takich jak: eskortowanie gości, zamykanie drzwi i okien w pomieszczeniach na czas nieobecności w nich pracowników, właściwe przechowywanie kluczy do pomieszczeń, nadzór nad personelem pomocniczym – sprzątającym, serwisowym (Polaczek 2006).

2. Analiza zabezpieczeń fizycznych w wybranym przedsiębiorstwie

Kategoryzacji stosowanych na terenie badanego przedsiębiorstwa zabezpieczeń fizycznych dokonano uwzględniając schemat organizacyjny jednostki oraz wyznaczając granice obszarów, które stanowią miejsca przetwarzania różnego rodzaju informacji i wymagają zapewnienia właściwego poziomu bezpieczeństwa.

Przeprowadzana analiza pozwoliła na wskazanie następujących obszarów:

- 1 – teren wokół przedsiębiorstwa;
- 2 – wejście z portiernią i recepcją;
- 3 – sekretariat i biura zarządu;
- 4 – sala konferencyjna;
- 5 – serwerownia;
- 6 – pozostałe pomieszczenia biur (działów: kosztorysowania, ofertowania, logistyki, księgowo – finansowego, kontrolingu, kadrowo - płacowego);
- 7 – pomieszczenia laboratorium;
- 8 – archiwum dokumentacji papierowej;
- 9 – pomieszczenia socjalne dla pracowników.

Szczegółową charakterystykę wskazanych granic przedstawiono w tabelach 1 – 9.

Tabela 1/ Table 1. Obszar 1 – teren wokół przedsiębiorstwa

Szczegóły miejsca	
Pomieszczenie:	Teren wokół przedsiębiorstwa
Zakres:	Miejsce czasowego przetwarzania
Zastosowane zabezpieczenia:	- Teren przedsiębiorstwa otoczony wysokim płotem. - Oświetlenie chronionego obiektu. - Monitoring terenu za pomocą systemu telewizji przemysłowej (8 kamer z systemem rejestracji). - Brama wjazdowa oraz parking nadzorowane przez pracowników służby ochrony fizycznej (w tym wyodrębniona budka wartownicza). - Budynki wyposażone w drzwi antywłamaniowe.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Na podstawie danych zamieszczonych w tabeli można stwierdzić, iż przyjęte przez przedsiębiorstwo zabezpieczenia są wystarczające i chronią one teren firmy przed nagłym wtargnięciem przez osoby niepożądane.

Tabela 2/ Table 2. Obszar 2 - wejście z portiernią i recepcją

Szczegóły miejsca	
Pomieszczenie:	Wejście z portiernią i recepcją
Zakres:	Miejsce przechowywania
Zastosowane zabezpieczenia:	- Wejście nadzorowane przez pracownika służby ochrony fizycznej. - Portiernia wyposażona w szybę antywłamaniową. - Prowadzony rejestr wydawania i zdawania kluczy. - Wydzielone stanowisko obsługi monitoringu wizyjnego. - Pomieszczenie zabezpieczone zwykłymi drzwiami.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Dane zawarte w tabeli 2 wskazują, że obszar wejścia z portiernią i recepcją jest należycie zabezpieczony. W tym przypadku ochrona fizyczna realizowana jest zarówno poprzez zaangażowanie służb ochrony fizycznej, jak również system monitoringu wizyjnego. Jednak zasadniczym mankamentem jest brak rozwiązań technicznych typu wzmocnione drzwi z zamkiem szyfrowanym.

Tabela 3/ Table 3. Obszar 3 - sekretariat i biura zarządu

Szczegóły miejsca	
Pomieszczenie:	Sekretariat i biura zarządu
Zakres:	Miejsce przechowywania

Zastosowane zabezpieczenia:	- Pomieszczenia zabezpieczone zwykłymi drzwiami (niewzmocnionymi, nie przeciwpożarowymi). - Okna w pomieszczeniach zabezpieczone kratami i roletami. - Dokumenty przechowywane są w metalowych i niemetalowych szafach zamykanych na klucz. - Kopie zapasowe przechowywane są w metalowych szafach zamykanych na klucz. - Pomieszczenie sekretariatu wyposażone w gaśnice wolnostojącą. - Pomieszczenia wyposażone w niszczarkę dokumentów i płyt CD.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Analiza danych zamieszczonych w tabeli 3 pozwala stwierdzić, że pomieszczenia sekretariatu oraz biura członków zarządu są zabezpieczone w sposób niewystarczający. Wskazać należy na brak barier fizycznych uniemożliwiających dostęp do pomieszczeń osobom nieuprawnionym. Z kolei uwzględniając elementy wyposażenia wskazanych pomieszczeń można przyjąć, że gwarantują one bezpieczne przechowywanie oraz utylizację dokumentów zawierających wrażliwe informacje.

Tabela 4/ Table 4. Obszar 4 - sala konferencyjna

Szczegóły miejsca	
Pomieszczenie:	Sala konferencyjna
Zakres:	Miejsce czasowego przetwarzania
Zastosowane zabezpieczenia:	- Pomieszczenie usytuowane w ustronnym miejscu, w wydzielonym obszarze, nieoznaczone (aby nie przyciągało niczyjej uwagi). - Pomieszczenie zabezpieczone zwykłymi drzwiami (niewzmocnionymi, nie przeciwpożarowymi). - Okna w pomieszczeniu zabezpieczone roletami.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Na podstawie danych zawartych w tabeli 4 można stwardzić, że przyjęte zabezpieczenia sali konferencyjnej są wystarczające, głównie z uwagi na fakt, że jest ono usytuowane w ustronnym miejscu przedsiębiorstwa. Zaleca się jednak doposażenie wskazanego pomieszczenia w urządzania zabezpieczające przed podsłuchem.

Tabela 5/ Table 5. Obszar 5 - serwerownia

Szczegóły miejsca	
Pomieszczenie:	Serwerownia
Zakres:	Miejsce przechowywania
Zastosowane zabezpieczenia:	- Pomieszczenie usytuowane w ustronnym miejscu, w wydzielonym obszarze, nieoznaczone (aby nie przyciągało niczyjej uwagi). - Pomieszczenie zabezpieczone drzwiami o podwyższonej ognioodporności.

	- Pomieszczenie wyposażone w systemy: przeciwwłamaniowy, kontroli dostępu, monitoringu, przeciwpożarowy oraz wentylacji i klimatyzacji precyzyjnej. - Pomieszczenie zabezpieczone przed skutkami przerw w dostawie prądu za pomocą systemu podtrzymania zasilania oraz agregat prądotwórczy. - Okna pomieszczenia zabezpieczone za pomocą krat i rolet. - Pomieszczenie wyposażone w szafy przemysłowe zamykane na klucz. - Kopie zapasowe przechowywane w sejfie.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Zabezpieczenia serwerowni przedstawione w tabeli 5 pozwalają stwierdzić, iż gwarantują one akceptowalny poziom bezpieczeństwa gromadzonych danych. Pomieszczenie to jest usytuowane w ustronnym miejscu na terenie przedsiębiorstwa i wyposażone w niezbędne zabezpieczenia fizyczne oraz systemy elektroniczne, chroniące przed nieuprawnionym dostępem, czy zdarzeniami losowymi (jak np. pożar).

Tabela 6/ Table 6. Obszar 6 - pozostałe pomieszczenia biur

Szczegóły miejsca	
Pomieszczenie:	Pozostałe pomieszczenia biur
Zakres:	Miejsce przechowywania
Zastosowane zabezpieczenia:	- Pomieszczenia zabezpieczone zwykłymi drzwiami (niewzmocnionymi, nie przeciwpożarowymi). - Okna w pomieszczeniach zabezpieczone kratami i roletami. - Dokumenty przechowywane są w metalowych i niemetalowych szafach zamykanych na klucz. - Pomieszczenia biur wyposażone w gaśnice wolnostojącą. - Stanowiska pracy wyposażone w niszczarkę dokumentów i płyt CD.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Analiza danych zamieszczonych w tabeli 6 pozwala wysnuć wniosek, że podobnie jak w przypadku pomieszczeń sekretariatu i biur członków zarządu przyjęte zabezpieczenia nie gwarantują dostatecznej ochrony, w szczególności przed dostępem osób nieuprawnionych. Takie podejście do kwestii zabezpieczeń naraża firmowe dane na ich utratę, ujawnienie, niekontrolowaną modyfikację, a także kradzież sprzętu komputerowego oraz nośników danych.

Tabela 7/ Table 7. Obszar 7 - pomieszczenia laboratorium

Szczegóły miejsca	
Pomieszczenie:	Pomieszczenia laboratorium
Zakres:	Miejsce czasowego przetwarzania
Zastosowane zabezpieczenia:	- Pomieszczenia usytuowane w ustronnym miejscu, w wydzielonym obszarze, nieoznaczone (aby nie przyciągały niczyjej uwagi).

	- Pomieszczenia wyposażone w systemy: przeciwwłamaniowy, kontroli dostępu, monitoringu, przeciwpożarowy, wentylacji i klimatyzacji precyzyjnej. - Okna pomieszczeń zabezpieczone za pomocą krat i rolet.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Z danych przedstawionych w tabeli 7 wynika, że wdrożone zabezpieczenia fizyczne pomieszczeń laboratorium gwarantują ochronę przed dostępem nieuprawnionych osób, włamaniem czy zdarzeniami losowymi. Istotną jednak kwestią jest ich wspomaganie przez wewnątrzzakładowe rozwiązania organizacyjne.

Tabela 8/ Table 8. Obszar 8 - archiwum dokumentacji papierowej

Szczegóły miejsca	
Pomieszczenie:	Archiwum dokumentacji papierowej
Zakres:	Miejsce przechowywania
Zastosowane zabezpieczenia:	- Pomieszczenie usytuowane w ustronnym miejscu, w wydzielonym obszarze, na piętrze, nieoznaczone (aby nie przyciągało niczyjej uwagi). - Pomieszczenie zabezpieczone drzwiami antywłamaniowymi. - Pomieszczenie wyposażone w systemy: przeciwwłamaniowy, kontroli dostępu, monitoringu, przeciwpożarowy. - Pomieszczenie wyposażone w urządzania kontrolujące temperaturę i wilgotność powietrza. - Okna pomieszczenia zabezpieczone za pomocą krat i rolet. - Dokumenty przechowywane są zamykanych szafach. - Wyposażenie niezbędne do wykonywania zadań.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Dane zawarte w tabeli 8 wskazują, że zabezpieczenia lokalu archiwum gwarantują należytą ochronę przed pożarem oraz włamaniem osób niepożądanych. Dodatkowo, przedsiębiorstwo opracowało plan gotowości i reagowania na wypadek wystąpienia zagrożeń nadzwyczajnych oraz przeszkoliło personel w zakresie właściwego reagowania w sytuacjach krytycznych.

Tabela 9/ Table 9. Obszar 9 - pomieszczenia socjalne dla pracowników

Szczegóły miejsca	
Pomieszczenie:	Pomieszczenia socjalne dla pracowników
Zakres:	-
Zastosowane zabezpieczenia:	- Pomieszczenia zabezpieczone zwykłymi drzwiami (niewzmocnionymi, nie przeciwpożarowymi). - Okna w pomieszczeniach zabezpieczone roletami.

Źródło: opracowanie własne na podstawie danych z przedsiębiorstwa

Zabezpieczenia fizyczne pomieszczenia socjalnego dla pracowników przedsiębiorstwa przedstawione w tabeli 8 można uznać za wystarczające. Wymagają one jednak uzupełnienia o rozwiązania organizacyjne polegające na przestrzeganiu pracowników znajdujących we wskazanej strefie przed rozmowami związanymi ze sprawami służbowymi.

3. Zagrożenia w systemie bezpieczeństwa fizycznego oraz sposoby ich eliminacji

3.1. Nieprawidłowości w obszarze bezpieczeństwa

W wyniku przeprowadzonego wywiadu z wybranymi pracownikami badanej jednostki organizacyjnej oraz obserwacji zidentyfikowano następujące nieprawidłowości w sferze bezpieczeństwa fizycznego:

1. Dokumenty przechowywane są w ogólnodostępnych miejscach, szafach bez wyposażenia w odpowiedniego typu zamknięcia, czy też na półkach, regałach itp.
2. W pomieszczeniach, w których gromadzone są dokumenty papierowe bądź mobilne nośniki danych brak jest instalacji elektronicznych systemów zabezpieczeń, takich jak: system alarmowy, system kontroli dostępu, system monitoringu kamer, system przeciwpożarowy.
3. Do niszczenia nieprzydatnych już dokumentów zawierających wrażliwe dane nie zawsze wykorzystywane są niszczarki dokumentów.
4. Pomieszczenia, w których przetwarza się informacje nie są odpowiednio zabezpieczane przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych do ich przetwarzania.
5. Niewłaściwe zabezpieczenie fizyczne nośników z kopiami zapasowymi lub archiwalnymi. Przechowywane są one w tych samych pomieszczeniach, w których zlokalizowana jest serwerownia.
6. Odnotowano incydenty związane z nieuwagą i nieostrożnością pracowników pionu ochrony, co pozwoliło na przedostanie się osoby postronnej na teren przedsiębiorstwa, bez uprzedniego zweryfikowania jej tożsamości.

Z powyższego wynika, że w sferze zarządzania ochroną fizyczną występujące nieprawidłowości dotyczą przede wszystkim braku barier fizycznych zapewniających dostęp do pomieszczeń wyłącznie osobom upoważnionym. Ponadto, wskazać należy na niewłaściwe rozwiązania organizacyjne w zakresie szybkiej identyfikacji pracowników, reagowania na osoby postronne i podejrzanie się zachowujące oraz bezpiecznej obsługi gości (takie jak: brak ewidencjonowania i eskortowania gości, wydawania przepustek).

3.2. Koncepcja doskonalenia bezpieczeństwem fizycznym

Zarządzanie ochroną fizyczną powinno zapewnić bezpieczeństwo osobom przebywającym w obszarach przedsiębiorstwa oraz jego materialnym i niematerialnym zasobom.

Zarządzanie bezpieczeństwem fizycznym ma na celu:

- zapobiegać nieuprawnionemu fizycznemu dostępowi do pomieszczeń i zasobów przedsiębiorstwa;
- ograniczać dostęp pracownikom do pomieszczeń i zasobów organizacji, zgodnie z zakresem ich uprawnień;
- uniemożliwiać lub opóźniać wtargnięcia przy użyciu siły do pomieszczeń, w których przechowywane i przetwarzane są informacje;
- zapobiegać utracie, uszkodzeniu, kradzieży sprzętu i innych zasobów jednostki gospodarczej;
- zapewniać ochronę przed bezpośrednim działaniem czynników fizycznych i zdarzeń losowych (takich jak np. pożar, powódź, wandalizm, terroryzm, itp.);
- zapobiegać zakłóceniom w działaniu przedsiębiorstwa.

Przy tak zdefiniowanych celach zarządzanie bezpieczeństwem fizycznym powinno obejmować:

- wyznaczenie stref bezpieczeństwa, w tym:
  - przetwarzania informacji krytycznych oraz stosowania krytycznych środków przetwarzania informacji;
  - recepcji i obsługi gości, łącznie z ustanowieniem procedur w zakresie ewidencjonowania i eskortowania gości, wydawania przepustek;
  - przyjmowania korespondencji, łącznie z opracowaniem procedury bezpiecznej jej dystrybucji;
  - dostaw i załadunku;
  - dostaw posiłków dla personelu;
- wdrożenie barier fizycznych zapewniających dostęp do pomieszczeń wyłącznie osobom uprawnionym (takich jak np.: systemy kontroli dostępu, czy rejestratory czasu pracy);
- zabezpieczenie biur, pomieszczeń i obiektów za pomocą rozwiązań mechanicznych (np. drzwi i zamki antywłamaniowe) oraz rozwiązań organizacyjnych (takich jak np. zapewnienie, że drzwi i okna pozostawione bez nadzoru są zamykane);
- opracowanie rozwiązań organizacyjnych, w zakresie :

- szybkiej identyfikacji pracowników (np. odzież, identyfikatory);
- ewidencji dostępu do pomieszczeń, wraz z procedurą zarządzania kluczami (obejmującą ich wydawanie, przechowywanie oraz zdawanie kluczy);
- dostępu do pomieszczeń w sytuacjach szczególnych (takich jak: pożar, zalanie, powódź lub inne awarie);
- dostępu do pomieszczeń osobom trzecim (np. serwis sprzątający, ochrona itp.);
- przebywania uprawnionych pracowników poza ustanowionym czasem pracy (tzn. nadgodziny, dni wolne od pracy);
- właściwego reagowania na osoby postronne i podejrzanie zachowujące się;
- pracy w obszarach bezpiecznych (np. poprzez ustanowienie zakazu: fotografowania, filmowania, wnoszenia i wynoszenia urządzeń elektronicznych, cz też kserowania dokumentów bez uzyskania wcześniejszego zezwolenia).

Wobec powyższych założeń, przyjęto, że wskazane powyżej zabezpieczenia fizyczne w połączeniu z rozwiązaniami organizacyjnymi mogą ograniczyć zidentyfikowane w toku przeprowadzonych badań podatności związane ze zbyt łatwym dostępem do pomieszczeń oraz nieuwagą i nieostrożnością pracowników pionu ochrony. Oprócz tego, umożliwią one zniwelować również zagrożenia dotyczące lekceważenia obecności na terenie organizacji osób postronnych i podejrzanie zachowujących się, a także pozostawiania ich w pomieszczeniach przedsiębiorstwa bez odpowiedniego nadzoru i opieki.

4. PODSUMOWANIE

Bezpieczeństwo fizyczne stanowi niezwykle ważną infrastrukturę każdego obiektu gospodarczego. Pozwala ono na ochronę podstawowych wartości, do których możemy zaliczyć dobra materialne, zasoby informacyjne, a także życie i zdrowie personelu oraz innych osób przebywających na terenie organizacji. Stąd też przedsiębiorstwa zobligowane są do systematycznego przeglądu swoich środków fizycznych oraz weryfikacji ich skuteczności w stosunku do potencjalnych zagrożeń.

W obszarze bezpieczeństwa informacji ochrana fizyczna zaliczana jest do podstawowych elementów ograniczających nieupoważniony dostęp do pomieszczeń i systemów informatycznych, w których te informacje są przechowywane i przetwarzane. Swoim zakresem obejmuje ono środki ochrony czynnej, budowlano – mechanicznej oraz elektronicznej.

Ponadto, zbudowanie odpornego na zagrożenia systemu ochrony fizycznej wymaga uwzględniania także odpowiednich procedur dostępu do informacji, organizacji pracy, a także

zarządzania zasobami przedsiębiorstwa. Pominięcie tego, jakże istotnego aspektu zarządzania ochroną fizyczną może spowodować kompromitację całego systemu bezpieczeństwa. Reasumując należy dodać, iż poziom bezpieczeństwa informacji determinowany jest przez jego najsłabsze ogniowo, a jak pokazują liczne przypadki elementem tym nadal pozostaje czynnik ludzki. Stąd zaprezentowana w pracy koncepcja doskonalenia systemu bezpieczeństwa fizycznego zwraca uwagę na rozwiązania organizacyjne, umożliwiające sprawowanie kontroli nad nieuprawionym dostępem do zasobów przedsiębiorstwa i jego zbioru danych i informacji.

LITERATURA

1. Kifner, T. (1999). *Polityka bezpieczeństwa informacji*. Gliwice: Helion
2. Staniec, I. Zawiła – Niedźwiecki J. (2008). *Zarządzanie ryzykiem operacyjnym. W: M.* Blik (red.), *Bezpieczeństwo fizyczne. Ochrona obiektu i wartośc*i. Warszawa: C.H. Beck.
3. Nowak, A. Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*. Warszawa: AON.
4. Pałęga M. (2016). Rola czynnika ludzkiego w systemie bezpieczeństwa informacji. Praca doktorska napisana pod kierunkiem dr hab. inż. M. Knapińskiego, prof. PCz., Częstochowa: WIPiTM.
5. PN-ISO/IEC 27002:2014
6. Polaczek, T. (2006). *Audyt bezpieczeństwa informacji w praktyce*. Gliwice: Helion.
7. Rozbicki, L. Ryżko, J. Sławiński, J. (2000). Systemy kontroli dostępu. Informatyka (1).