JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 11 (2019) 163-166
Wysłane: 2019-02-14
Przyjęte: 2019-02-28

Analiza i ocena realizacji polityki bezpieczeństwa informacji w wybranych polskich i ukraińskich przedsiębiorstwach branży IT

Andriy Andriychuk*

Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. W artykule przedstawiono rezultaty po przeprowadzeniu ankiet w wybranych przedsiebiorstwach Ukrainy i Polski, a takze opisano porównanie polityk bezpieczeństwa informacji w tych przedsiębiorstwach oraz oceniono, które przedsiębiorstwa lepiej chronią informacje, biorąc pod uwagę wspomniane firmy obu krajów jako przedmiot badań.

Słowa kluczowe: bezpieczeństwo informacji; polityka bezpieczeństwa informacji.

*Autor do korespondencji.

Adres e-mail: werewolfaaa@gmail.com

Analysis and evaluation of the implementation of information security policy in selected Polish and Ukrainian IT companies

Andriy Andriychuk*

Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. The article presents the results after conducting surveys in selected enterprises of Ukraine and Poland, as well as described the comparison of information security policies in enterprises and verbal, which enterprises better protect information, taking into account the companies of both countries as a research subject.The professional literature of the given issue, as well as Internet sources, were used.

Keywords: information policy; security information policy.

*Corresponding author.

E-mail address: werewolfaaa@gmail.com

1. Wstęp

Rozwój i rozpowszechnienie: elektroniki, internetu, urządzeń dostępowych oraz pojawienie się sieci społecznościowych, a także wykorzystywanie sieci publicznych do przekazywania informacji, przyczynia się nie tylko do tworzenia informacji jako kluczowego elementu określającego wiedzę, ale także decydującego czynnika bezpieczeństwa osób fizycznych i prawnych poszczególnych państw.

Bezpieczeństwo informacji od dawna uważane jest za jeden z głównych priorytetów prawie wszystkich organizacji, a w tym przedsiębiorstw branży IT.

Zwiększona uwaga poświęcana temu zagadnieniu wynika z szybko rosnącej ilości informacji, potrzeby jej przetwarzania, przesyłania i przechowywania. Konwersja znacznej części informacji na formę elektroniczną oraz wykorzystywanie lokalnych i globalnych sieci stwarza jakościowo nowe zagrożenia dla niejawnych informacji [1, 2].

Globalna informatyzacja doprowadziła do tego, że informacje korporacyjne i systemy telekomunikacyjne zyskały główne znaczenie w obecnym świecie. Systemy informacji korporacyjnej i telekomunikacyjnej są tworzone w celu uzyskania określonych usług informacyjnych. Jeżeli nie można uzyskać dostępu do informacji o usługach, szkodzi to wszystkim osobom powiązanym z informacjami, zarówno przedsiębiorcom jak i klientom. Dlatego najważniejszym elementem bezpieczeństwa informacji jest dostępność usług systemów informatycznych [3].

2. Założenia badań

Celem badań jest porównanie polityki bezpieczeństwa informacji w polskich i ukraińskich przedsiębiorstwach, a także ustalenie, które organizacje lepiej chronią informacje, podejmując wspomniane wcześniej podmioty obu krajów jako przedmiot badań.

W planie badań uwzględniono zadania:

1. Analiza literatury z zakresu informatyki, która odzwierciedla problem badania.
2. Badanie i identyfikacja współczesnych i najbardziej popularnych sposobów ochrony informacji.
3. Ocena aktualnego poziomu bezpieczeństwa informacji przedsiębiorstw.
4. Propozycja sposobów usprawnienia ochrony informacji w celu osiągnięcia akceptowalnego poziomu bezpieczeństwa zasobów informacyjnych przedsiębiorstwa.

W badaniach sformułowano hipotezę badawczą:

Polityka bezpieczeństwa informacji prywatnych przedsiębiorstw w Polsce jest na wyższym poziomie niż podobnych organizacji na Ukrainie.

Jako teoretyczną podstawę badania wykorzystano publikacje oraz artykuły dotyczące polityki i narzędzi bezpieczeństwa informacji.

Aby osiągnąć cel badań, wybrano klasyczne metody badawcze: sondaż diagnostyczny (przeprowadzenie ankiety wśród przedsiębiorstw Polski i Ukrainy) oraz analizę porównawczą jako metodę weryfikacji wyników ankietowania.

Ankieta została opracowana dla firm komercyjnych na Ukrainie i w Polsce. Pytania ankiety dotyczyły metod ochrony informacji i osób odpowiedzialnych za bezpieczeństwo informacji przedsiębiorstwa.

Autor pracy stosował się do następującego planu działania:

1. Przygotowanie ankiety.
2. Badanie przedsiębiorstw na Ukrainie i w Polsce.
3. Analiza porównawcza.

3. Realizacja i wyniki badań

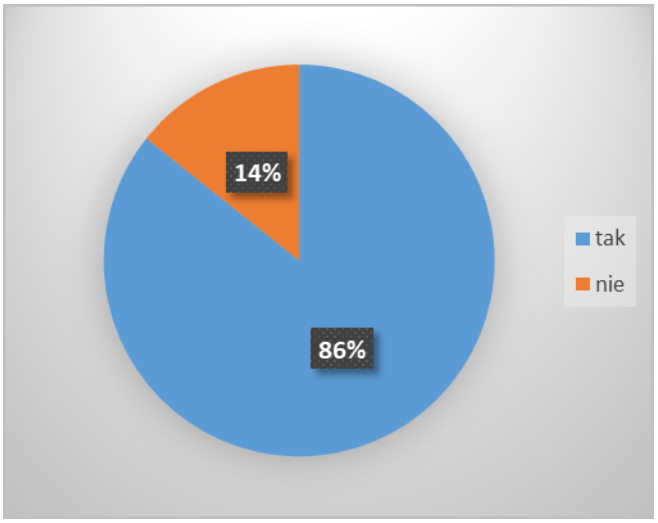
Ankieta została przygotowana pod kątem identyfikacji metod ochrony informacji w przedsiębiorstwach. Przy jej pomocy uzyskano dane o normach i przepisach stosowanych w przedsiębiorstwach dla zapewnienia bezpieczeństwa informacji. Główne zagadnienia objęte ankietą to organizacyjne i sprzętowe środki ochrony informacji, na przykład tworzenie kopii zapasowych i szyfrowanie danych, praca z personelem i dostępem użytkownika.[4, 5]

Od 2 do 30 listopada 2017 r. przeprowadzono ankiety w 74 przedsiębiorstwach. Ankietami objęto: 53 przedsiębiorstwa ukraińskie i 21 polskie. Formularze dla przedsiębiorstw zostały przesłane e-mailem. Wszystkie przedsiębiorstwa są związane z branżą IT i zajmują się tworzeniem oprogramowania lub zasobów internetowych. Różnice w nich wynikały ze specyfiki pracy, liczby personelu i bazy klientów. Pytania ankiety dla polskich firm przedstawiono w tabeli 1.

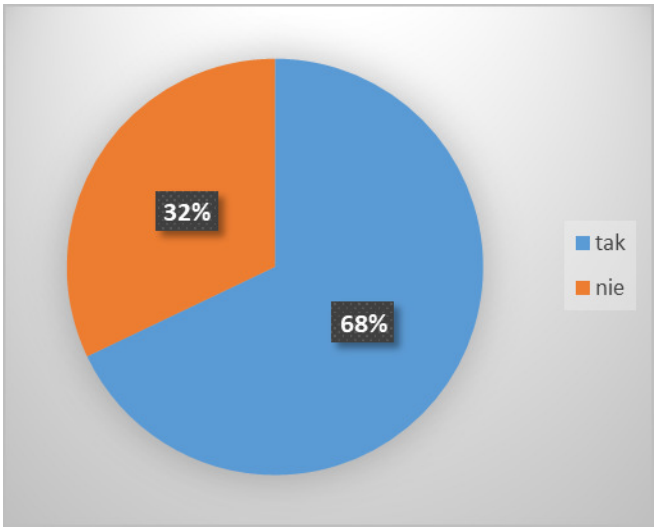
Rezultaty wyników odpowiedzi na wybrane pytania ankiety dla przedsiębiorstw polskich przedstawiono na rys.1, 3, 5, 7, a dla przedsiębiorstw ukraińskich na rys. 2, 4, 6, 8.

Tabela 1. Zestawienie pytań zadanych ankietowanym w sprawie bezpieczeństwa informacji

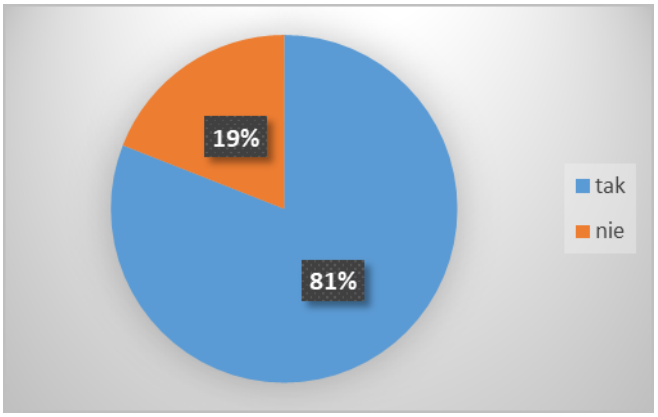
№	Pytanie
1	Czy znają Państwo pojęcie polityki bezpieczeństwa informacji?
2	Czy korzystają Państwo wyłącznie z certyfikowanych narzędzi ochrony danych z nieautoryzowanego dostępu?
3	Czy istnieje u Państwa pełny zestaw dokumentacji dla każdego z narzędzi ochrony danych z nieautoryzowanego dostępu?
4	Czy jest zapewniona u Państwa ochrona hasłem wszystkich komputerów i LANów wykorzystywanych w procesach technologicznych?
5	Czy są u Państwa udokumentowane wymagania dotyczące haseł dostępu?
6	Czy ustalone u Państwa wymagania dotyczace haseł, są przestrzegane?
7	Czy istnieje u Państwa w organizacji osoba odpowiedzialna za zapewnienie bezpieczeństwa informacji?
8	Czy u Państwa monitorowane są następujące procesy: generowanie, rozprzestrzenianie, zmiana, usuwanie haseł, opracowywanie niezbędnych instrukcji, kontrola nad działaniami personelu przy pracy z hasłami?
9	Czy funkcjonuje u Państwa elektroniczny dziennik działań podejmowanych przez personel i użytkowników?
10	Czy istnieje u Państwa podział komputerów na segmenty: księgowość, dział sprzedaży, deweloperzy itp.?
11	Czy istnieje u Państwa priorytet komputerów w sieci? (Kategoryzowanie poziomu ważności poszczególnych chronionych komputerów i ustalanie priorytetów incydentów w systemie)
12	Czy stosują się Państwo do kontroli drukowania (Przydzielanie tylko autoryzowanych drukarek w celu drukowania poufnych informacji w celu wyeliminowania możliwych kanałów wycieku informacji.)
13	Czy stosuje się u Państwa szyfrowanie danych poufnych?
14	Czy stosują się Państwo do ograniczenia praw użytkowników (na przykład ograniczenia dotyczące uruchamiania aplikacji)
15	Czy regularnie wykonują Państwo kopię zapasową danych?
16	Czy korzystają Państwo z serwerów zdalnych do przechowywania informacji?
17	Czy korzystają Państwo z bezpiecznych nośników pamięci?



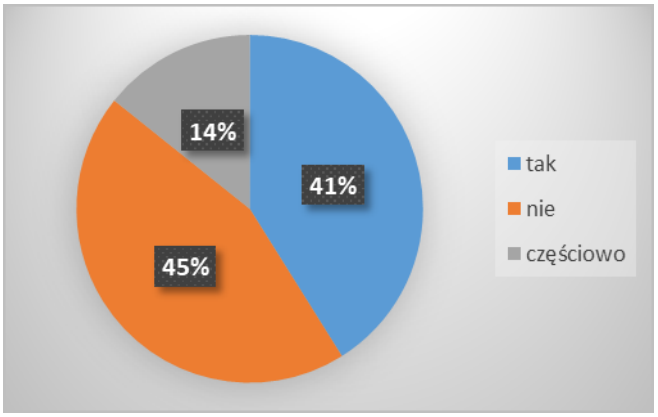
Rys. 1. Wynik odpowiedzi na pytanie: „Czy stosuje się u Państwa szyfrowanie danych poufnych?" w przedsiębiorstwach polskich



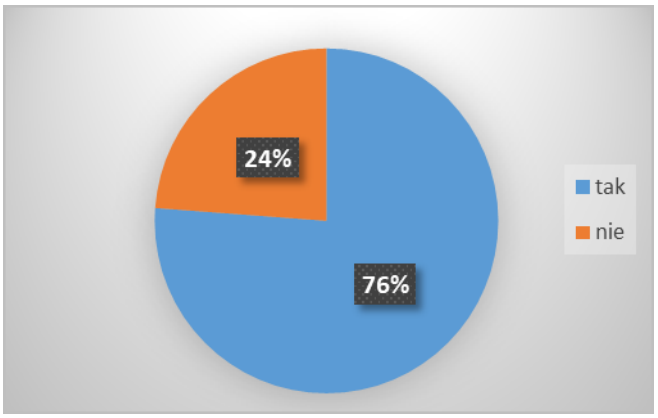
Rys. 2. Wynik odpowiedzi na pytanie: „Czy stosuje się u Państwa szyfrowanie danych poufnych?" w przedsiębiorstwach ukraińskich



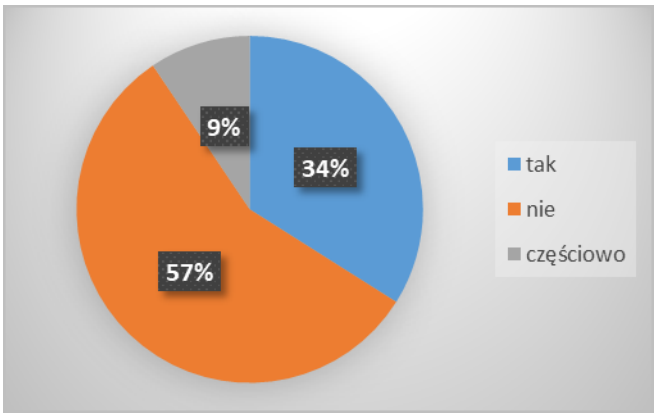
Rys. 3. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa podział komputerów na segmenty: księgowość, dział sprzedaży, deweloperzy itp.?" w przedsiębiorstwach polskich



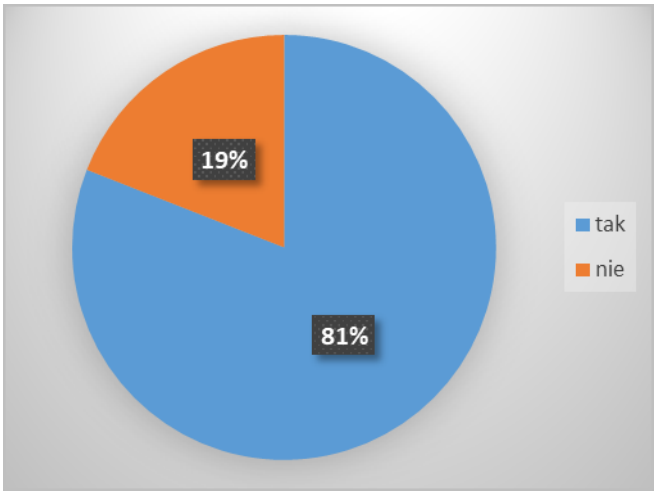
Rys. 4. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa podział komputerów na segmenty: księgowość, dział sprzedaży, deweloperzy itp.?" w przedsiębiorstwach ukraińskich



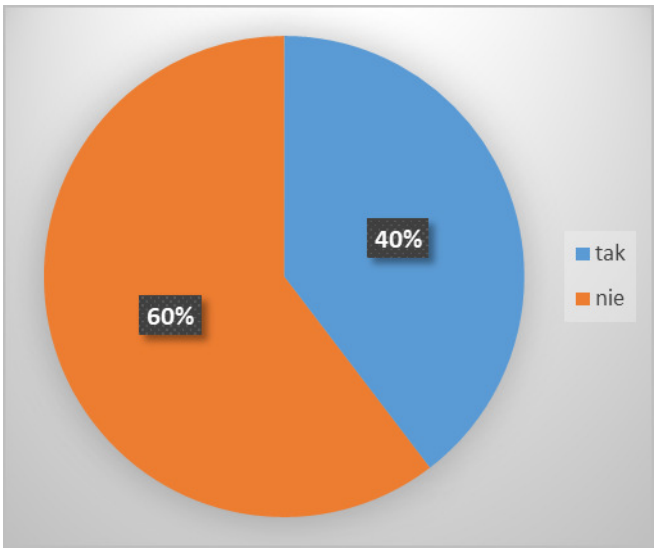
Rys. 5. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa elektroniczny dziennik działań podejmowanych przez personel i użytkowników?" w przedsiębiorstwach polskich



Rys. 6. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa elektroniczny dziennik działań podejmowanych przez personel i użytkowników?" w przedsiębiorstwach ukraińskich



Rys. 7. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa priorytet komputerów w sieci? w przedsiębiorstwach polskich .



Rys. 8. Wynik odpowiedzi na pytanie: „Czy istnieje u Państwa priorytet komputerów w sieci? (w przedsiębiorstwach ukraińskich.)

Zgodnie z wynikami ankiety przeprowadzonej w firmach z branży IT na Ukrainie i w Polsce, można stwierdzić, że polskie firmy używają znacznie więcej certyfikowanych narzędzi bezpieczeństwa niż ukraińskie i monitorują dostępność dokumentacji na ich temat. Jeśli chodzi o prostsze i bardziej niezawodne narzędzia bezpieczeństwa, takie jak ochrona hasłem komputerów i sieci, szyfrowanie i tworzenie kopii zapasowych danych, ograniczenie praw użytkowników, podział komputerów na segmenty i ich priorytetyzacja w sieci, wykazano, że takie działania są obecne w wielu firmach IT w obu krajach. Większość firm zatrudnia pracowników odpowiedzialnych za bezpieczeństwo informacji (ponad 60% respondentów). 76% ankietowanych polskich firm prowadzi elektroniczny dziennik działań podejmowanych przez pracowników oraz użytkowników, a tylko 34% utrzymuje go na Ukrainie lub częściowo utrzymuje (9% respondentów). Również 81% polskich przedsiębiorstw segmentuje swoje komputery, podczas gdy na Ukrainie robi to tylko 41% i 14% częściowo. Również 81% polskich przedsiębiorstw priorytetowo traktuje komputery w sieci, na Ukrainie zrobiono to tylko w 40% przypadków, co wskazuje, że wśród polskich przedsiębiorstw wynik jest prawie dwukrotnie wyższy. Wskaźnik szyfrowania danych jest o 18% wyższy w Polsce niż na Ukrainie.

4. Wnioski

Podsumowując wyniki badań, autor pracy zauważył, że postindustrialny etap rozwoju społeczeństwa wnosi wiele korzyści dla naszego życia.Jednak wraz z pozytywnymi korzyściami przynosi to również ludziom negatywne konsekwencje - nowe zagrożenia dla ich żywotnych interesów. Wśród takich zagrożeń są zagrożenia w sferze informacyjnej [6-8]. Do ich szybkiej lokalizacji i eliminacji konieczna jest polityka informacyjna państwa adekwatna do skali zagrożeń informatycznych. Polityka ta powinna uwzględniać obiektywne procesy globalizacji, rosnącą otwartość społeczeństw i opierać się na priorytecie narodowych interesów Ukrainy i Polski. Potwierdziła się także hipoteza, że polityka bezpieczeństwa informatycznego prywatnych przedsiębiorstw w Polsce jest lepsza niż polityka bezpieczeństwa informatycznego prywatnych przedsiębiorstw na Ukrainie.

Literatura

[1] Харченко Л.С., *Информационная безопасность Украины* : Глоссарий / Л. С. Харченко, В. А. Липкан, А. В. Логинов, Текст, Киев 2004, 136.

[2] https://uchebnikionline.com/politologia/informatsiyna_bezpeka_-_ostrouhov_vv/normativno-pravove_regulyuvannya_informatsiynoyi_bezpeki_ukrayini.htm [20.04.2018]

[3] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, 11-12.

[4] Батюк А.Є., *Інформаційні системи в менеджменті*, Інтелект-Захід, Львів 2004, 343–384.

[5] В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект*, ДУТ, Киев 2015.

[6] Б.Р. Бабаян, *Защита информационных систем*

[7] https://businessinsider.com.pl/firmy/przepisy/rodo-gdpr-regulacje-o-ochronie-danych-osobowych-zmiany-w-firmach/21p6svs.

[8] http://cyclowiki.org/wiki/Средства_защиты_информации