UNIWERSYTET EKONOMICZNY W KATOWICACH
WYDZIAŁ INFORMATYKI I KOMUNIKACJI

INFORMATYKA I EKONOMETRIA

OLENA STUKANOVA

BEZPIECZEŃSTWO TECHNOLOGICZNE I PRAWNE HANDLU ELEKTRONICZNEGO NA PRZYKŁADZIE POLSKI I UKRAINY.

TECHNOLOGY AND LEGAL SECURITY OF INTERNET TRADE ON THE EXAMPLE OF POLAND AND UKRAINE.

Praca magisterska
napisana w Katedrze Informatyki
pod kierunkiem dr Artura Strzeleckiego

Oświadczam, że niniejsza praca została przygotowana pod moim kierunkiem
i stwierdzam, że spełnia wymogi stawiane pracom dyplomowym.

…….. ……
(data) *(podpis promotora pracy dyplomowej)*

KATOWICE 2015

Katowice, dnia .....
Olena Stukanova
Wydział Informatyki i Komunikacji
Informatyka i Ekonometria

OŚWIADCZENIE

Świadoma odpowiedzialności prawnej oświadczam, że złożona praca magisterska pt.: „Bezpieczeństwo technologiczne i prawne handlu elektronicznego na przykładzie Polski i Ukrainy" została napisana przeze mnie samodzielnie.

Równocześnie oświadczam, że praca ta nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. 1994, nr 24, poz. 83) oraz dóbr osobistych chronionych prawem.

Ponadto praca nie zawiera informacji i danych uzyskanych w sposób nielegalny i nie była wcześniej przedmiotem innych procedur związanych z uzyskaniem dyplomów lub tytułów zawodowych uczelni wyższej.

Wyrażam zgodę na przetwarzanie moich danych osobowych oraz nieodpłatne udostępnienie mojej pracy w celu oceny samodzielności jej przygotowania przez system elektronicznego porównywania tekstów oraz przechowywania jej w bazie danych tego systemu.

Oświadczam także, że wersja pracy znajdująca się na przedłożonej przeze mnie płycie CD jest zgodna z wydrukiem komputerowym pracy.

.....

Spis treści

Wstęp 5
Rozdział 1 Istota handlu elektronicznego 7
1.1. Pojęcie handlu elektronicznego 7
1.2. Globalna historia handlu elektronicznego 11
1.3. Typologia handlu elektronicznego 13
1.4. Cele handlu elektronicznego i odmienność od handlu tradycyjnego 15
1.5. Modele biznesowe w handlu elektronicznym 17
1.6. Zalety i wady prowadzenia handlu elektronicznego. 22
1.7. Potrzeby realizacji handlu elektronicznego 25
1.8. Perspektywy i bariery rozwoju handlu elektronicznego 27
Rozdział 2 Bezpieczeństwo technologiczne handlu elektronicznego 31
2.1. Sytuacja aktualna i pojęcie bezpieczeństwa 31
2.2. Obszary zagrożenia w handlu elektronicznym 35
2.3. Cele i strategie bezpieczeństwa technologicznego 40
2.4. Zarządzanie bezpieczeństwem w handlu elektronicznym 42
2.5. Tradycyjne metody bezpieczeństwa danych w sieci Internet 45
2.5.1. Szyfrowanie 46
2.5.2. Podpis cyfrowy 50
2.6. Metody bezpieczeństwa w systemie handlu elektronicznego 52
2.6.1. Zabezpieczona informacja o systemie 52
2.6.2. Zapasowe kopie danych 52
2.6.3. Bezpieczny hosting 54
2.6.4. Ochrona domeny internetowej 54
2.6.5. Bezpieczeństwo serwera WWW 55
2.6.6. Bezpieczeństwo baz danych 57
2.6.7. Bezpieczna transmisja danych 58
2.6.8. Bezpieczne sesje 59
Rozdział 3 Bezpieczeństwo prawne handlu elektronicznego 61
3.1. Generalne inicjatywy międzynarodowe, dotyczące handlu elektronicznego 61
3.1.1. Regulacje Unii Europejskiej 61
3.1.2. Deklaracja OECD 63
3.1.3. Modelowe prawo o handlu elektronicznym ONZ 64

3.2. Wybrane międzynarodowe prawne rozwiązania, dotyczące handlu elektronicznego 64
3.2.1. Rozwiązania prawne, dotyczące opodatkowania i cła....64
3.2.2. Rozwiązania dotyczące podpisów elektronicznych....65
3.2.3. Ochrona konsumenta....65
3.2.4. Ochrona prywatności....66
3.2.5. Ochrona prawa własności intelektualnej....66
3.3. Prawo wobec handlu elektronicznego....67
3.3.1. Regulamin serwisu....68
3.3.2. Przetwarzanie danych osobowych....70
3.3.3. Zawarcie umów przez Internet....71
Rozdział 4 Analiza bezpieczeństwa handlu elektronicznego w Polsce i Ukrainie....72
4.1. Ocena obecnego stanu handlu elektronicznego....72
4.1.1. Obecny stan handlu elektronicznego w Polsce....72
4.1.2. Obecny stan handlu elektronicznego w Ukrainie....78
4.2. Bezpieczeństwo technologiczne....84
4.2.1. Metodologia badania....84
4.2.2. Ocena bezpieczeństwa technologicznego handlu elektronicznego w Polsce....88
4.2.3. Ocena bezpieczeństwa technologicznego handlu elektronicznego w Ukrainie....96
4.3. Ocena bezpieczeństwa prawnego handlu elektronicznego....105
4.3.1. Metodologia badania.....105
4.3.2. Ocena bezpieczeństwa prawngo handlu elektronicznego w Polsce....106
4.3.3. Ocena bezpieczeństwa prawnego handlu elektronicznego w Ukrainie....112
Podsumowanie....119
Bibliografia....122
Indeks rysunków....125
Indeks tabeli....127

Wstęp

We współczesnych czasach handel elektroniczny jest dynamicznie rozwijającym się sektorem gospodarki światowej. Szybki rozwój Internetu i rosnąca konkurencja na rynku przywiodły do poszukiwania przez przedsiębiorstwa nowych metod rozwoju handlu. Prowadzenie działalności gospodarczej w Internecie jest optymalnym rozwiązaniem dla rozwoju jak już istniejącego biznesu tak i powstania nowego. Korzyści są również i dla konsumentów, bo zakupy w Internecie pozwalają na redukcję czasu zakupów, niższą cenę i większą możliwość wyboru. Handel elektroniczny to nie nowe pojęcie, ponieważ istnieje prawie 20 lat, ale rozwój handlu nie jest identyczny w różnych krajach. W takich krajach jak Stany Zjednoczone i państwa Europy Zachodnia rozwój e-handlu przebiega dużo szybszej niż w krajach Europy Środkowo-Wschodniej.

Ze względu na większą popularność handlu elektronicznego kwestia bezpieczeństwa w Internecie staje bardziej aktualna. Sieć Internet rozwija się, codziennie powstają nowe strony, aplikacje, urządzenia, rośnie liczba użytkowników sieci. Ale równocześnie z pozytywnymi aspektami rozwoju Internetu, w tej samej chwili rośnie liczba negatywnych działań, między innym szeroka działalność hakerska. Autorzy licznych badań alarmują o zwiększającym się rozwoju niebezpieczeństwa. Według raportu bezpieczeństwa od CISCO tylko w 2014 roku skradziono dane osobowe 908 mln. ludzi, 68% użytkowników globalnego Internetu stały się ofiarami hakerów, 4.5 bln. zagrożeń jest codziennie blokowanych przez programy antywirusowe. Oczywiście, nowoczesne narzędzia bezpieczeństwa skutecznie blokują zagrożenia, ale bezpieczeństwo najpierw zależy od ludzi, ich działań i świadomości.

Celem tej pracy magisterskiej jest określenie teoretycznych zasad handlu elektronicznego, typowych metod zabezpieczenia handlu w Internecie w sposób technologiczny i prawny, prowadzenie analizy i oceny poziomu bezpieczeństwa polskich i ukraińskich sklepów internetowych. Wyniki analizy posłużą do określenia planu dalszych działań dla zapewniania bezpiecznego handlu elektronicznego w poszczególnych krajach.

Do badania były wybrane Polska i Ukraina, ponieważ to kraję sąsiadujące, ale znajdują się na różnym poziomie rozwoju ekonomicznego i technologicznego. Porównanie sytuacji w tych krajach pomoże w określeniu negatywnych i pozytywnych praktyk, perspektyw dalszego rozwoju gospodarczego.

Praca składa się z czterech rozdziałów. Rozdział pierwszy niniejszej pracy przedstawia ogólną charakterystykę handlu elektronicznego. Omówiono różne podejścia do definicji pojęcia handlu elektronicznego, krótko przedstawiono globalną historię rozwoju handlu elektronicznego. Określono różnicę pomiędzy handlem tradycyjnym i elektronicznym, wady i zalety handlu w Internecie według przedsiębiorstw i użytkowników. Krótko opisano modele biznesowe, istniejące w handlu elektronicznym, potrzeby jego realizacji i bieżące perspektywy i istniejące bariery.

W rozdziale drugim przedstawiono pojęcie bezpieczeństwa technologicznego handlu w Internecie, przeanalizowano aktualną sytuację bezpieczeństwa zakupów w Internecie. Określono najgłówniejsze zagrożenia, powstające przed przedsiębiorstwami i konsumentami przy prowadzeniu działalności gospodarczej lub zakupach w sieci. Główną uwagę poświęcono opisaniu tak klasycznym sposobom bezpieczeństwa w Internecie (szyfrowanie i podpis elektroniczny), jak i wyspecjalizowanym technologiom bezpieczeństwa w e-commerce.

Rozdział trzeci przedstawia pojęcie bezpieczeństwa prawnego w e-commerce, określone są międzynarodowe akty prawne, regulujące działalność handlową w Internecie. Dokładniej przedstawiono podstawowe zagadnienia prawne o ochronie konsumentów, ochronie danych osobowych, problemie opodatkowania. Określono dokumenty prawne, które regulują działalność sklepu internetowego (regulamin sklepu, polityka prywatności, umowy elektroniczne).

W ostatnim – czwartym rozdziale – skupiono się na badaniu bezpieczeństwa technologicznego i prawnego polskich i ukraińskich sklepów internetowych. Do badania wybrano po 50 największych e-sklepów Polski i Ukrainy w pięciu kategoriach. Przeanalizowano sytuację obecną na rynku, sprawdzono i oceniono certyfikaty bezpieczeństwa, posiadane przez sklepy, brak czy posiadanie przekierowania automatycznego w tryb bezpieczny na stronach wprowadzenia informacji poufnych. Z kwestii prawnej przeanalizowano posiadanie przez sklep polityki prywatności i regulaminu sklepu, oceniono jego jakość i zgodność z krajowymi normami prawnymi. Zrobiono podsumowanie, określające działania dla likwidacji problemów, stworzono koncepcję dalszego rozwoju.

Rozdział 1
Istota handlu elektronicznego

1.1. Pojęcie handlu elektronicznego

W ostatnich latach w zakresie Internetu były obserwowane bardzo istotne zmiany, szczególnie wywołane przez innowacje techniczne i technologiczne. Te zmiany wywarły poważny wpływ na procesy ekonomiczne, doprowadziły do zmian w gospodarce, popularyzując wykorzystanie nowych technologii w sektorze komercyjnym. Mobilna komunikacja, Internet i inne technologie online legły u podstaw wykształcenia się pojęcia Nowej Ekonomii dla określenia procesów gospodarczych związanych z handlem elektronicznym.

Główna cecha Nowej Ekonomii wynika z faktu, że Internet stworzył innowacyjne modele biznesowe, które zmieniają funkcjonowanie tradycyjnej ekonomii (tzw. Old Economy) na korzyść Nowej Ekonomii. Ostatecznie, Nowa Ekonomia - to indywidualizacja stosunków prawnych, umożliwiająca zapewnienie precyzji oraz wyjątkowości, indywidualizacji oferty w sposób dotychczas niespotkany, dzięki technicznym możliwościom analizy zachowania użytkowników sieci.

Opisane wyżej cechy stały się elementem, w oparciu, o który wykształciło się pojęcie handlu elektronicznego. Pojęcie to nie posiada jednak ogólnej definicji normatywnej, różne źródła traktują go po swojemu. Na przykład, zdaniem niektórych autorów, handel elektroniczny to suma wszystkich transakcji, które są wykonywane drogą elektroniczną. Ale przy takiej definicji w ogóle wykracza poza tradycyjne pojęcie „handel". Inni pod pojęciem handlu elektronicznego rozumieją działalność reklamową, sprzedaż i dystrybucję produktów za pośrednictwem Internetu[1].

Najpełniejszym pojęciem e-handlu jest następne: handel elektroniczny to szczególny rodzaj przedsięwzięć w zakresie e-biznesu skupiający się wokół pojedynczych transakcji wykorzystujących sieć Internet, jako medium wymiany, obejmujący relacje pomiędzy przedsiębiorstwami (business-to-business, B2B), jak również pomiędzy przedsiębiorstwem

[1] D.Lubasz, *Handel elektroniczny. Bariery prawne.* Lexis Nexis, Warszawa 2013, s.24.

i konsumentem (business-to-consumer, B2C). Inne popularne definicje handlu elektronicznego według znanych firm lub naukowców są przedstawione w tabeli 1.1.

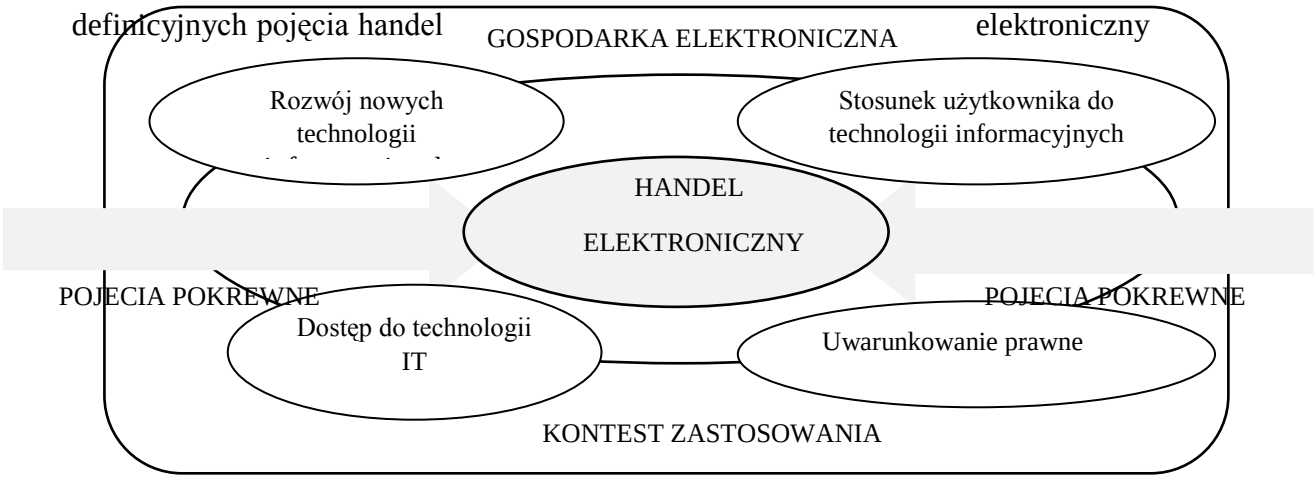
Tabela 1.1. Różne definicje pojęcia „handel elektroniczny"

Źródło	Definicja
CISCO	Sprzedaż w sieci WWW.
GUS	Handel elektroniczny to transakcje przeprowadzone przez sieci oparte na protokole IP oraz przez inne sieci komputerowe, z zastosowaniem standardu elektronicznej wymiany danych EDI.
A.Szewczyk	Prowadzenie działań firmowych (między innym kupno i sprzedaż produktów lub usług oraz różne działania marketingowe) przez sieć Internet.
B. Gregor, M.Stawiszyński	W ujęciu węższym – sposób sprzedaży i kupna towarów i usług, a więc zawierania transakcji z wykorzystaniem środków elektronicznych za pośrednictwem Internetu.
	W ujęciu szerszym – prowadzenie różnorodnych transakcji handlowych przy pomocy sieci teleinformatycznych, bez konieczności bezpośredniego kontaktu między stronami.

Źródło: M.Lewicki, *Instrumenty dla tworzenia wartości dla klienta w handlu elektronicznym.* Rozprawa doktorska. Poznań 2012, s.10.

Przyczyny powstania takiej wielkiej liczby definicji handlu elektronicznego są przedstawione na rysunku 1.1[2].

Rysunek 1.1. Główne źródła trudności definicyjnych pojęcia handel elektroniczny



Źródło: W.Chmielarz, *Systemy biznesu elektronicznego.* Wydawnictwo Difin, Warszawa 2007, s.15.

[2] M.Lewicki, *Instrumenty dla tworzenia wartości dla klienta w handlu elektronicznym.* Rozprawa doktorska. Poznań 2012, s.10.

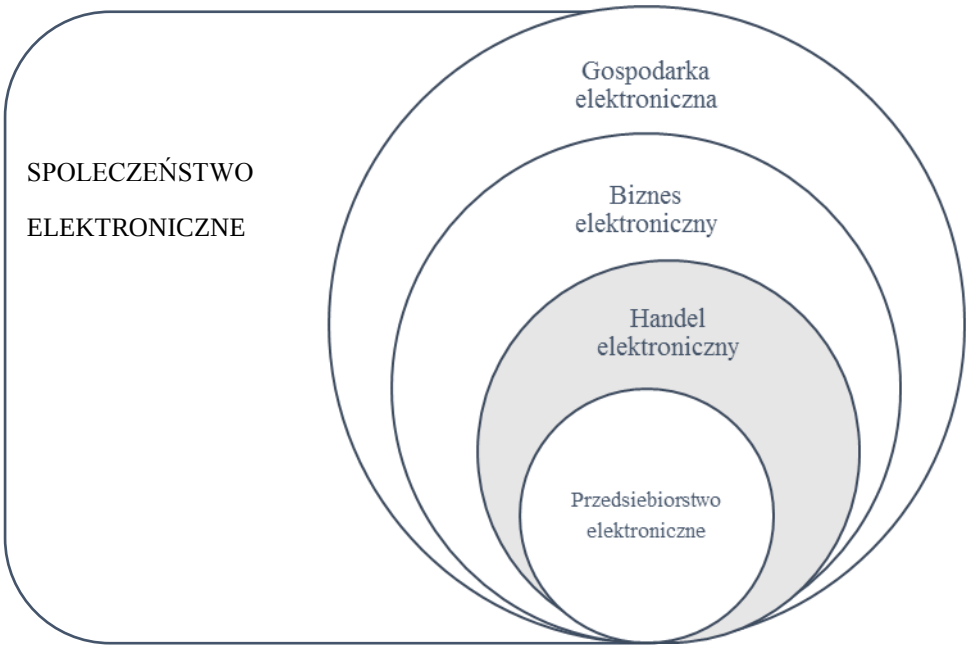
Towary i usługi są zamawiane w sposób elektroniczny, ale płatności można dokonywać nie tylko elektroniczne, a na przykład przy dostawie kartą lub gotówką, możliwe jest płacenie punktami PAYBACK lub za pomocą bankowość elektroniczną. Trzeba zwrócić szczególną uwagę, że zamówienia otrzymane przez telefon, faks, napisane ręczne przez e-mail lub generowane nieautomatyczne nie są traktowane, jako handel elektroniczny.

Handel elektroniczny znajduje najczęstsze zastosowanie w bardzo szybko rozwijających dziedzinach, takich jak finanse, podatki, transport i wszędzie, gdzie następuje wymiana informacji między przedsiębiorstwami. Papierowy obieg dokumentów już prawie został wycofany w zeszłym wieku, zostaje zastąpiony szybszym, pewniejszym, tańszym i bardziej wydajnym obiegiem w postaci elektronicznej[3].

W powyższych definicjach często były podane pojęcia e-biznes, e-handel, e-społeczeństwo. Zastanówmy teraz, jakie miejsce posiada handel elektroniczny w systemie społeczeństwa elektronicznego i określimy różnice pomiędzy pojęciem e-handel i e-commerce.

Na rysunku 1.2. przedstawiony jest schemat struktury społeczeństwa elektronicznego, części jakiego jest i handel elektroniczny.

Rysunek 1.2. Miejsce handlu elektronicznego wśród pojęć pokrewnych



Źródło: W.Chmielarz. *Systemy biznesu elektronicznego.* Wydawnictwo Difin, Warszawa 2007, s.29.

[3] W.Chmielarz. *Systemy biznesu elektronicznego.* Wydawnictwo Difin, Warszawa 2007, s.27.

Dla lepszego zrozumienia schematu, określimy definicję elementów społeczeństwa elektronicznego.

Również jak i pojęcie handlu elektronicznego, tak i pojęcie biznesu elektronicznego posiada wielu definicji. E-biznes (e-business) to jakiekolwiek przedsięwzięcie internetowe - taktyczne lub strategiczne - które przekształca zależności biznesowe, czy będą to relacje business-to-consumer, business-to-business, powiązania w zakresie przedsiębiorstw (intra-business), czy pomiędzy konsumentami (consumer-to-consumer)[4]. Według opinii prof. Wojciecha Cellary, elektroniczny biznes stanowi uogólnienie elektronicznego handlu[5]. Dla firmy International Data Corporation termin e-biznes oznacza„ elektronizację podstawowych transakcji handlowych"[6].

E-gospodarka (e-economy) przedstawia sobą wirtualną arenę, na której prowadzona jest działalność, przeprowadzane są transakcje, dochodzi do tworzenia i wymiany wartości i gdzie dojrzewają bezpośrednie kontakty pomiędzy jego uczestnikami. Procesy w e-gospodarce mogą być powiązane z podobnymi procesami na tradycyjnym rynku, ale są od nich niezależne.

Definicja społeczeństwa informacyjnego (e-society) jest powiązana z definicją e-government. E-government (czyli e-administracja) przedstawia sobą model działania instytucji rządowych i samorządowych bazujący na wykorzystaniu sieci Internet, nowoczesnych technologii i nowych modeli komunikacji pomiędzy obywatelami i rządem. Model ten jest realizowany poprzez związki zewnętrzne (urząd-obywatel, urząd-firma, urząd-dostawca) oraz związki wewnętrzne (urząd-urząd, urząd-pracownicy)". Społeczeństwo informacyjne (Information society) przedstawia sobą nowy system społeczeństwa, który rozwija się w krajach o wysokim stopniu rozwoju technologicznego i ekonomicznego, gdzie zarządzanie informacją, jej jakość i szybkość przepływu są zasadniczymi warunkami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga nowych sposobów gromadzenia, przetwarzania, przekazywania i użytkowania informacji[7].

E-przedsiębiorstwo to jednostka gospodarcza, wyodrębniona w sposób organizacyjny, ekonomiczny i prawny, która specjalizuje się w prowadzeniu działalności gospodarczej (przeważnie kupno i sprzedaż towarów i usług) za pośrednictwem sieci Internet. W różnych

[4] N. Kirov, A. Kuśmierz, R. Rządca, *Jak się kręci e-biznes*. PC Kurier 2003, nr 8, s. 36-39.
[5] D.Nojszewski, *Biznes elektroniczny – czyli jaki?* E-mentor №1(3), 2004.
[6] J. Samołyk, *E-business - globalna rewolucja*. Infoman 1999, nr 7/8, s. 15-17.
[7] J.Winiarski, *Technologie internetowe –wprowadzenie.* http://www.slideshare.net/piniol/gospodarka-elektroniczna-1 [dostęp: 10.04.2014]

źródłach informacji definicja handlu elektronicznego jest często powiązana z pojęciami e-commerce, sprzedaż B2C i e-biznes. Ale trzeba zwracać uwagę, ponieważ te pojęcia mają różne definicje. Różnice poszczególnych pojęć przedstawione w tabeli 1.2[8].

Tabela 1.2. Nieścisłości w zakresie definiowania pojęcia e-handel

e-handel ≠ e-commerce	E-handel jest częścią rynku e-commerce i dlatego nie jest mu całościowo równy. W e-commerce są dodatkowo usługi finansowo-ubezpieczeniowe, turystyczne i inne świadczenia sprzedawane pośrednictwem sieci Internet.
e-handel ≠ wartość sprzedaży w sklepach internetowych +wartość sprzedaży na platformach aukcyjnych	Większość transakcji, które są realizowane na portalach aukcyjnych, są prowadzane bez licytacji ze stałą ceną. Często sprzedawcami są przedsiębiorcy, posiadające również sklepy internetowe i handlujący wyłącznie nowymi artykułami. Wyniki sprzedaży w takim wypadku mają w sobie skumulowaną cząstkową wartość, która była wygenerowana za pośrednictwem platform aukcyjnych.
e-handel ≠ handel B2C	Osoby kupujące w sklepach internetowych nie są wyłącznie konsumentami (B2C), pewna ilość kupujących to przedsiębiorcy (B2B) i instytucje publiczne. Z tego wynika, że wielkość obrotów, podawana przez sprzedawców nie może być równa wielkościom zakupów deklarowanych przez konsumentów.

Źródło: M.Lewicki, *Instrumenty dla tworzenia wartości dla klienta w handlu elektronicznym.* Rozprawa doktorska. Poznań 2012, s.12.

Podsumowując, handel elektroniczny ma wiele definicji, ale sens większości definicji polega na tym, że to proces kupna sprzedaży towarów i usług przez Internet. Trzeba wziąć pod uwagę, że nie każda czynność sprzedażowa w Internecie odnosi się do handlu elektronicznego. W literaturze często używa się pojęcie handlu elektronicznego wymiennie z pojęciem
e-commerce, ale te słowa mają różne definicje.

1.2. Globalna historia handlu elektronicznego

Internet był stworzony w 1967 roku, na początku wyłącznie do celów naukowych. World Wide Web tak bardzo znany dzisiaj był stworzony w 1989 roku. W połowie lat 90-tych rozpoczęło się wykorzystywanie Internetu dla celów komercyjnych i wtedy pojawiło się

[8] Raport serwisu Sklepy24.pl, *E-handel Polska 2009*. http://dotcomriver.pl/files/raport-ehandel-polska-2012.pdf [dostęp: 12.04.2014]

pojęcie handlu elektronicznego. Kolejne etapy rozwoju Internetu w celach komercyjnych były następujące:

1. W 1991 roku zniesiono komercyjne restrykcje nałożone przez NSFNET (National Science Foundation NET) na korzystanie z sieci Internet.
2. Przy współudziale takich firm jak IBM, MCI Communication Corp. oraz Merit Network Inc była stworzona ANS (Advanced Network and Services). ANS to infrastruktura, która umożliwiła komercyjne wykorzystanie Internetu.
3. W 1993 roku została stworzona jedna z pierwszych przeglądarek internetowych – Mosaic. Przeglądarka była pierwszym krokiem do początku używania Internetu przez przeciętnego użytkownika.
4. W 1995 roku ANS sprzedała firmie America Online infrastrukturę. W ramach tej umowy sprzedaży cała infrastruktura sieciowa przeszła z sektora finansowanego ze środków publicznych do sektora prywatnego.

To wszystko doprowadziło do tego, że Internet stał się najszybciej rozwijającą technologią w historii gospodarki[9].

W 1995 roku była rozpoczęta pierwsza działalność handlową w Internecie. Jednymi z pierwszych były Amazon (największy na świecie sklep internetowy z książkami), eBay (pierwsza internetowa aukcja) i Dell (producent sprzętu komputerowego, sprzedający swoje produkty bezpośrednio do użytkownika końcowego). W 1997 roku w USA Prezydent Bill Clinton wystąpił z propozycją stworzenia w Internecie strefy wolnego handlu. Od tego czasu przy współpracy rządu, organizacji międzynarodowych, wielkich korporacji nastąpił szybki progres handlu elektronicznego. Od 2000 roku większość amerykańskich i europejskich przedsiębiorstw oferuje swoje usługi w Internecie. Za danymi agencji Marketer[10] średni roczny wzrost w latach poczatkujących dla handlu elektronicznego (2000-2005 r.) dla segmentu B2C osiągnął 143%, dla segmentu B2B – 245%.

Szybkie początki globalnego rynku elektronicznego potwierdzają dane o penetracji e-biznesu w firmach amerykańskich. W każdej kategorii firm przekracza ona 50%. Jeżeli chodzi o prognozowany w Europie wzrost stopnia obrotów rynku elektronicznego, to w stosunku do Stanów Zjednoczonych Unia Europejska jest znacznie opóźniona[11].

[9] M.Ambrozik, A.Wojciechowski, *E-Commerce - koncepcja biznesu.* Warszawa, 2007, s.2.
[10] *Worldwide B2C Ecommerce: 2012 Complete Forecast.* http://www.emarketer.com/report/1259 [dostęp 12.04.2014]
[11] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warzawa, 2004, s.91.

1.3. Typologia handlu elektronicznego

Jak i w zwykłym handlu są różne rodzaje, tak i handel elektroniczny ma swoją własną typologię. W zależności od działalności handlowej, która jest prowadzona w Internecie handel elektroniczny ma podział na bezpośredni, pośredni i hybrydowy.

Bezpośredni handel elektroniczny (ang. direct e-commerce) to handel, gdzie cała transakcja handlowa od momentu złożenia zamówienia do realizacji płatności i dostawy towaru odbywa się wyłącznie przez sieć. Towary i usługi przesyłane są tylko w formie elektronicznej. Okazanie usługi stworzenia strony internetowej lub nabycie kluczu aktywacyjnego
do programu, to doskonałe przykłady takiego handlu.

W pośrednim (ang. indirect e-commerce) handlu elektronicznym w formie elektronicznej są prowadzone następujące procesy: poszukiwanie towarów, usług, nowych kontrahentów, przesyłanie dokumentów, dokonanie płatności. Dostawa zamówionego towaru lub usługi odbywa się bezpośrednio, w sposób tradycyjny (na przykład, pocztą kurierską, firmą spedycyjną lub przez kontakt bezpośredni w magazynie, biurze dostawcy). Przykładami takiego handlu są wymiany plików muzycznych, e-booków, prenumerat czasopism i gazet, rezerwacja biletów, video na żądanie itp.

Handel hybrydowy charakteryzuje się stosowaniem wielu form przejściowych, wynikiem czego jest zahamowanie rozwoju sieci[12].

Ze względu na stosunki prawne wyróżniają następujące typy handlu elektronicznego:

1. B2B (business-to-business) – typ stosunków obustronnie profesjonalnych, które dominują przeważnie w Internecie. Przykładem realizacji takich stosunków są systemy aukcyjne zamówień lub dystrybucji (reverse auction), systemy brokerskie i platformy transakcyjne;
2. B2C (business-to-consumer) – to stosunki między przedsiębiorcą i konsumentem. Za konsumenta jest uznawana osoba fizyczna działająca w celach, które nie mieszczą się w ramach jej działalności handlowej, gospodarczej lub zawodowej. Do tego typu handlu odnoszą się między innym sklepy internetowe i portale aukcyjne, gdy sprzedawcą jest profesjonalista;

[12] *E-handel (handel elektroniczny),* http://stat.gov.pl/metainformacje/slownik-pojec/definicje-pojec/1778,pojecie.html [dostęp: 12.04.2014]

3. B2A (business-to-administration) – stosunki przedsiębiorca – administracja, przedsiębiorca - rząd (B2G (business-to-government). Te pojęcia są używane dla określenia całości kontaktów przedsiębiorcy z przedstawicielami władzy publicznej;

4. B2E (business-to-employee) – typ stosunków pracodawca – pracownik, wykonywane w oparciu o platformy elektroniczne. Na przykład, okazanie usług outsourcingowych, wykonanych elektronicznie;

5. C2C (consumer-to-consumer) – obustronnie stosunki konsumenckie. Szczególnymi platformami realizacji tych stosunków są systemy aukcyjne (np. e-Bay.com, allegro.pl, autro.ua);

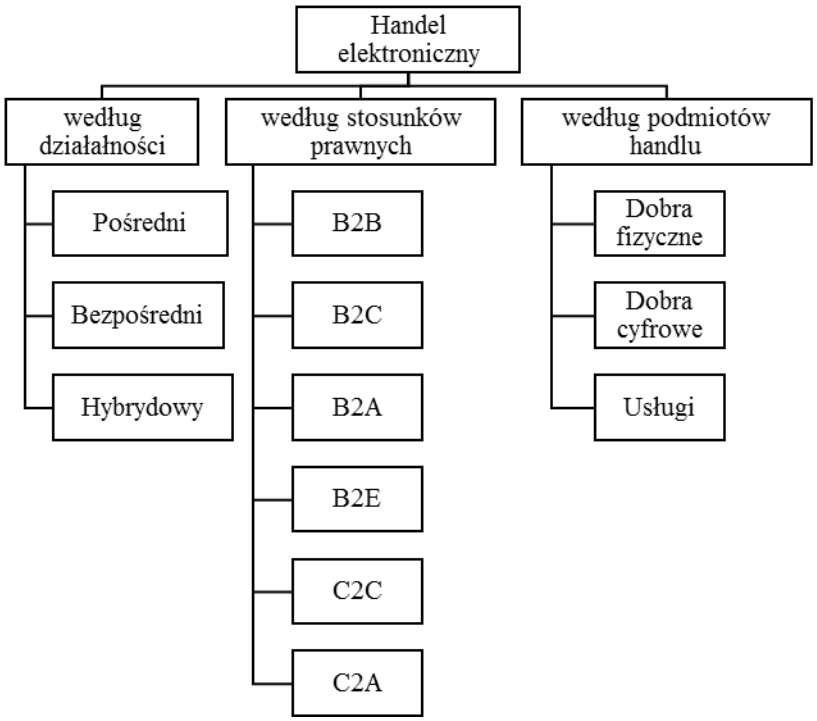
6. C2A (consumer-to-administration) – stosunki konsument – administracja, jaki określają całość kontaktów obywateli z przedstawicielami władzy publicznej;

7. A2B/C/A – (administration-to-business/consumer/administration) – stosunki określane, jako e-governmnt polegające na transformacji administracji „papierowej" na „wirtualną"[13].

Ze względu na przedmioty handlu rozróżniamy handel elektroniczny, głównymi towarami którego są: dobra fizyczne, dobra cyfrowe i usługi.

Na rysunku 1.3. przedstawiono ogólną topologię handlu elektronicznego według poniższej klasyfikacji.

Rysunek 1.3. Topologia handlu elektronicznego



Źródło: opracowanie własne

[13] D.Lubasz, *Handel elektroniczny. Bariery prawne.* Lexis Nexis, Warszawa 2013, s.28.

1.4. Cele handlu elektronicznego i odmienność od handlu tradycyjnego

Handel elektroniczny i tradycyjny mają jeden główny cel: wymiana towarów i usług. Ale inne cele handlu elektronicznego są stworzone w oparciu na nowe metody sprzedaży przez Internet. Rozróżniamy następujące wyróżnienia handlu elektronicznego:

1. Wykorzystanie nowoczesnych technologii w procesach handlowych;
2. Pozyskanie nowych klientów;
3. Reklamowanie i oferowanie klientom nowych produktów i usług;
4. Usprawnienie obsługi klientów;
5. Budowanie lojalności klientów;
6. Wzrost jakości kapitału ludzkiego;
7. Osiągniecie przez przedsiębiorstwa przewagi konkurencyjnej i przywództwa.

Oczywiście, że Internet nie jest oderwany od rzeczywistości wirtualną siecią i musi funkcjonować na tle realnego rynku. W handlu elektronicznym zmieniły się sposoby dokonywania transakcji (czas, miejsce, płatność), które są wykonywane przez technologie informatyczne, co odróżnia je od handlu tradycyjnego. Tym samym zmieniły się metody nawiązywania kontaktów, poszukiwania partnerów, wymiany informacji i przesyłania dokumentacji handlowej, obsługi klientów, zarządzania produkcją, logistyką, finansami, promocją i reklamą, transferu środków płatniczych, działania dystrybucji.

Wszelkie różnice pomiędzy handlem tradycyjnym a handlem elektronicznym są przedstawione w tabeli 1.3.

Transakcje realizowane w handlu elektronicznym mają swoją specyfikę. Proces transakcyjny dzieli się na 3 etapy:

1. Etap przed sprzedażą. Na tym etapie klient zapozna się z oferowanymi towarami i usługami przez firmę. Sprzedawca w tym celu wykorzystuje możliwości multimedialne stron WWW.
2. Etap sprzedaży. Na tym etapie zaczyna się proces negocjacji między sprzedawcą i klientem. Cel negocjacji - ustalenie, jakie produkty i usługi zakupi klient, oraz uzgodnienie formy płatności i transferu zakupionych produktów. W handlu elektronicznym faza sprzedaży jest procesem interaktywnym, w którym obydwie strony poszukują najkorzystniejszych warunków zakupu.

3. Etap po sprzedaży. Polega na przedstawieniu wysokiej jakości serwisu dla klienta po zakupie towaru lub usługi. Ten proces wymuszony jest rosnącą konkurencją[14].

4. Etap przed sprzedażą. Na tym etapie klient zapozna się z oferowanymi towarami i usługami przez firmę. Sprzedawca w tym celu wykorzystuje możliwości multimedialne stron WWW.

5. Etap sprzedaży. Na tym etapie zaczyna się proces negocjacji między sprzedawcą i klientem. Cel negocjacji - ustalenie, jakie produkty i usługi zakupi klient, oraz uzgodnienie formy płatności i transferu zakupionych produktów. W handlu elektronicznym faza sprzedaży jest procesem interaktywnym, w którym obydwie strony poszukują najkorzystniejszych warunków zakupu.

6. Etap po sprzedaży. Polega na przedstawieniu wysokiej jakości serwisu dla klienta po zakupie towaru lub usługi. Ten proces wymuszony jest rosnącą konkurencją[15].

Tabela 1.3. Różnice pomiędzy handlem elektronicznym a tradycyjnym

Handel tradycyjny	Handel elektroniczny
Media	
Komunikacja bezpośrednia twarzą w twarz, używając pomocy pośredników, bądź przy pomocy dokumentów przesyłanych przez pocztę, telefon stacjonarny, faks.	Komunikacja jest prowadzona przeważnie przez Internet (poczta elektroniczna, wyszukiwarki, odnośniki stron, portale), częściowo wspomagana przez media tradycyjne.
Elastyczność działalności	
Niska elastyczność. Skomplikowany proces spowodowany ograniczeniami administracyjnymi.	Wysoka elastyczność. Wynika z roli pośrednika na rynku. Trudności spowodowane są technicznymi posunięciami na rynku.
Logistyka działalności	
Konieczność utrzymywania wielu punktów wytwarzania i dystrybucji.	Oderwanie od procesu wytwórczego, możliwość przesyłania bezpośrednio do klienta.
Formy płatności	
Tradycyjne: gotówka, karta płatnicza, czek; anonimowość kupna i sprzedaży, problemy z wymianą niektórych walut uznanych za obowiązujące na określonym terytorium.	Dominują formy płatności elektronicznej, przekaz pieniędzy elektronicznych, mikropłatności. Dla transakcji konieczne jest przedstawienie danych osobowych.

Źródło: D.Czelstowski, A.Szewczyk, *Problemy rozwoju handlu elektronicznego w Polsce.* Zeszyty naukowe Uniwersytetu Szczecińskiego, № 733, 2012, s. 21-23.

[14] A.Kwasek, *E-commerce i e-business jako nowe koncepcje organizacji procesów biznesowych.* http://www.wsz-pou.edu.pl/magazyn/?strona=mag_kwasek87 [dostęp: 16.04.2014]
[15] Ibidem.

Handel elektroniczny umożliwia bezpośrednie dotarcie do klienta, szybsze reagowanie na jego potrzeby, personalizacje zamówienia według preferencji konsumenta.

Handel elektroniczny, również jak i handel tradycyjny wymaga działalności marketingowej. Internet umożliwia szersze możliwości prowadzenia marketingu. Ale trzeba pamiętać, że sprawna reklama stanowi jeden z podstawowych elementów przewagi konkurencyjnej na rynku i zwykle decyduje dobrana strategia i precyzyjny dobór docelowej grupy klientów, do której jest skierowana.

Podsumowując, konsumenci nadal będą używali tradycyjnych metod robienia, wtedy handel elektroniczny będzie ważnym uzupełnieniem klasycznych metod prowadzenia handlu tradycyjnego.

1.5. Modele biznesowe w handlu elektronicznym

Z szybkim rozwojem technologii informatycznych i handlu elektronicznego rozwiązania, które były zastosowane rok, dwa lata temu, już dziś są nieaktualne. Dlatego, żeby zrozumieć czy nowe modele biznesowe handlu elektronicznego mają szansę powodzenia, należy wprowadzić je w życie i odczekać z ocenami pewien czas. Bez tego tworzenie nowego modelu biznesowego może być jedynie teoretycznym rozważaniem, niemającym zastosowania w praktyce.

Model biznesowy to zestaw zaplanowanych działań, nakierowanych na generowanie zysku w danej firmie. W obszarze handlu elektronicznego model biznesowy ma na celu tworzenie przewagi konkurencyjnej w Internecie[16].

Istnieje szeroka klasyfikacja modeli biznesowych, która została wyróżniona przez kilku autorów, którzy opierali się na modelach handlu elektronicznego rozwiniętych krajów światu, takich jak Stany Zjednoczone, Niemcy, Kanada.

Klasyfikacja składa się z następujących części:

1. Elektroniczna witryna i sklep internetowy (e-shop). Najprostszy z prezentowanych modeli biznesowych, który służy do tworzenie firmy, promocji jej towarów lub usług. Często witryna jest połączona ze sklepem internetowym, w którym bezpośrednio są sprzedawane towary i usługi danej firmy.

[16] P.Timmers, *Business models for electronic markets.* "Electronic Markets", 1998, Vol.8, no. 2.

2. Elektroniczne zaopatrzenie (e-procurement). To pojęcie oznacza elektroniczne składanie ofert i zaopatrywanie w towary i usługi. Usługi mogą być wytworzone w formie elektronicznej, jeżeli chodzi o towar to transport odbywa się w formie tradycyjnej.

3. Elektroniczne centrum handlowe (e-mall). To elektroniczne sklepy (prowadzone przez niezależne podmioty), w których odbywa się sprzedaż towarów i usług. Współpraca między sklepami może być rozszerzona o wspólne metody płatności, dostawy towarów itp.

4. Aukcja elektroniczna (e-auction). Aukcje elektroniczne są najczęściej odpowiednikami aukcji prowadzonych w sposób tradycyjny i również bardzo popularnym jest prowadzenie licytacji.

5. Wirtualna społeczność (virtual community). To bardziej zjawisko internetowe niż model biznesowy. Jest to grupa osób skupionych wokół określonego tematu, którzy komunikują się za pośrednictwem forów internetowych, sieci społecznościowej.

6. Platforma współpracy (collaboration platform). Platforma, która dostarcza narzędzia i środowisko informatyczne, umożliwiające współpracę między firmami;

7. Integrator i dostawca usług łańcucha wartości (value-chain integrator). Model biznesowy, który koncentruje się na integracji całego łańcucha wartości w pierwszym wypadku oraz dostarczaniu specyficznych usług z łańcucha wartości w przypadku drugim;

8. Pośrednictwo informacji (information brokerage). Oferta usług wyszukiwania i kreowania bazy czy profili klientów przez firmy specjalne, którzy mają dostęp do takiej informacji.

9. Usługi zaufania (trust services). Podobny do poprzedniego model biznesowy, w którym firma, która dostarcza specyficzne informacje i gwarantuje zaufanie w procesach biznesowych pomiędzy stronami sieci[17].

Jeżeli chodzi o podział na sektory, to główne modele biznesowe w sektorze B2C przedstawione w tabeli 1.4. W tabeli przedstawiono nazwę modelu, możliwe warianty i dokładny opis z przykładami.

[17] D.Nojszewski, *Biznes elektroniczny – czyli jaki?* E-mentor №1(3), 2004.

Tabela 1.4. Główne modele biznesowe w sektorze B2C

Model	Warianty	Opis
Serwisy informacyjne i portale internetowe	-horyzontalne -wertykalne (Vortale)	-oferują zintegrowane zestawy usług (yahoo.com). -oferują produkty i usługi na branżowych rynkach (iboots.com)
Detaliczna sprzedaż	-wirtualne sklepy; -pasaże handlowe; -katalogi elektroniczne on-line; -bezpośredni wytwórcy.	-detaliczne sklepy on-line (amazon.com) -grupa sklepów, połączonych przez wspólny adres WWW, -zakup produktów przez email, -sprzedaż produktów przez producentów (dell.com)
Dostawcy zawartości (content providers)		Dostarczanie czasopism, poradników, nowości, muzyki (cnn.com)
Brokerzy transakcji (transaction brokers)		Maklerzy giełdowi, agencje turystyczne (e-trade.com, monster.com)
Kreatorzy rynku (Market creators)	Aukcje i inne formy dynamicznego ustalenia cen	Organizacja ogólnodostępnego rynku dla sprzedających i kupujących (ebay.com)
Dostawcy usług (Service providers)		Sprzedaż usług (xdrive.com)
Dostawcy społeczności		Organizowanie miejsc spotkań, wymiany opinii, zainteresowań (about.com)

Źródło: *Systemy e-commerce. Technologie internetowe w biznesie.* Praca zbiorowa pod redakcją Celiny M. Olszak. Katowice, 2004, s.75.

W sektorze B2B podział modeli biznesowych przedstawiony w tabeli 1.5.

Tabela 1.5. Główne modele biznesowe w sektorze B2B

Model	Warianty	Przykłady
Rynki elektroniczne i giełdy	-wertykalne i horyzontalne	-directag.com -e-steel.com
E-dystrrybucja		Grainger.com
Dostawcy usług	-tradycyjne usługi -Apllication Service Provider	-emloyeematters.com -salesforce.com
Doradztwo biznesowe		Iship.com
Pośrednictwo		Autobytel.com

Źródło: *Systemy e-commerce. Technologie internetowe w biznesie.* Praca zbiorowa pod redakcją Celiny M. Olszak. Katowice, 2004, s.75.

W czasopiśmie PC Kurier była podana trochę inna klasyfikacja modeli biznesowych w e-biznesie, która składa się z 8 modeli, częściowo tylko pokrywających się z poprzednimi:

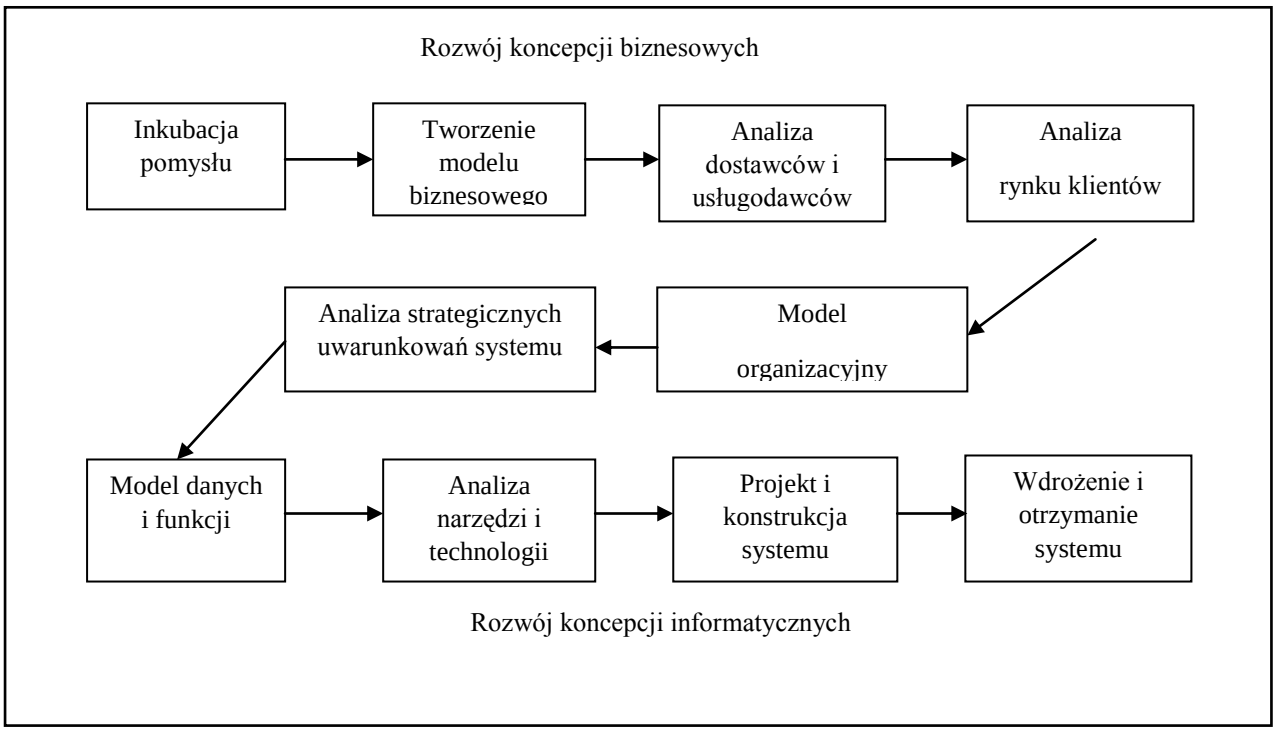
1. Model „prosto do klienta”. Firma dostarcza produkty i usługi bezpośrednio do klienta, pomijając tradycyjne kanały dystrybucji;
2. Model „dostawca z pełnym zakresem usług”. Producent buduje portal tematyczny, za pomocą którego oferuje swoje produkty i również pokrewne produkty innych firm. Jako przykład, firma sprzedająca laptopy, będzie oferować karty SD, etui, oprogramowanie od innych producentów;
3. Model „wirtualna społeczność” - opisana wcześniej;
4. Model „dostawca treści”. Firma zostaje dostawcą treści dla większych portali, które płacą jej za produkty i informacje;
5. Model „wspólna infrastruktura”. Model, w którym firmy tworzą wspólne platformy dla kontaktu z klientami;
6. Model „przedsiębiorstwo”. – Firma, która ma wiele jednostek biznesowych, gdzie każda ma swój własny produkt, tworzy jeden "punkt kontaktu" dla wszystkich produktów firmy;
7. Model „integrator sieci wartości”. Integrator działa wyłącznie w wirtualnym łańcuchu wartości, jego atutem są posiadane dane;
8. Model „pośrednik”. Głównym celem pośrednika jest udostępnienie pojedynczego punktu kontaktu pomiędzy sprzedającymi a kupującymi oraz koncentracja informacji[18].

Niektóre przedsiębiorstwa wykorzystują dwa lub więcej modeli biznesowych w handlu elektronicznym, co pozwała powiększyć swoje wyniki w biznesie i stworzyć nowe kontakty z klientami i firmami.

Zgodnie z wyżej zaznaczonymi modelami biznesowymi można stworzyć ogólny scenariusz wprowadzenia e-handlu, który jest przedstawiony na rysunku 1.4. Ogólny schemat łączy między innym rozwój koncepcji biznesowych i również informatycznych, ponieważ aspekt informatyczny jest bardzo ważny w handlu elektronicznym.

[18] D.Nojszewski, *Biznes elektroniczny – czyli jaki?* E-mentor №1(3), 2004.

Rysunek 1.4. Scenariusz wprowadzenia handlu elektronicznego



Źródło: Opracowanie własne za materiałami wykładu „*IT w biznesie. Prowadzenie do handlu elektronicznego*", PJWSTK, 2012.

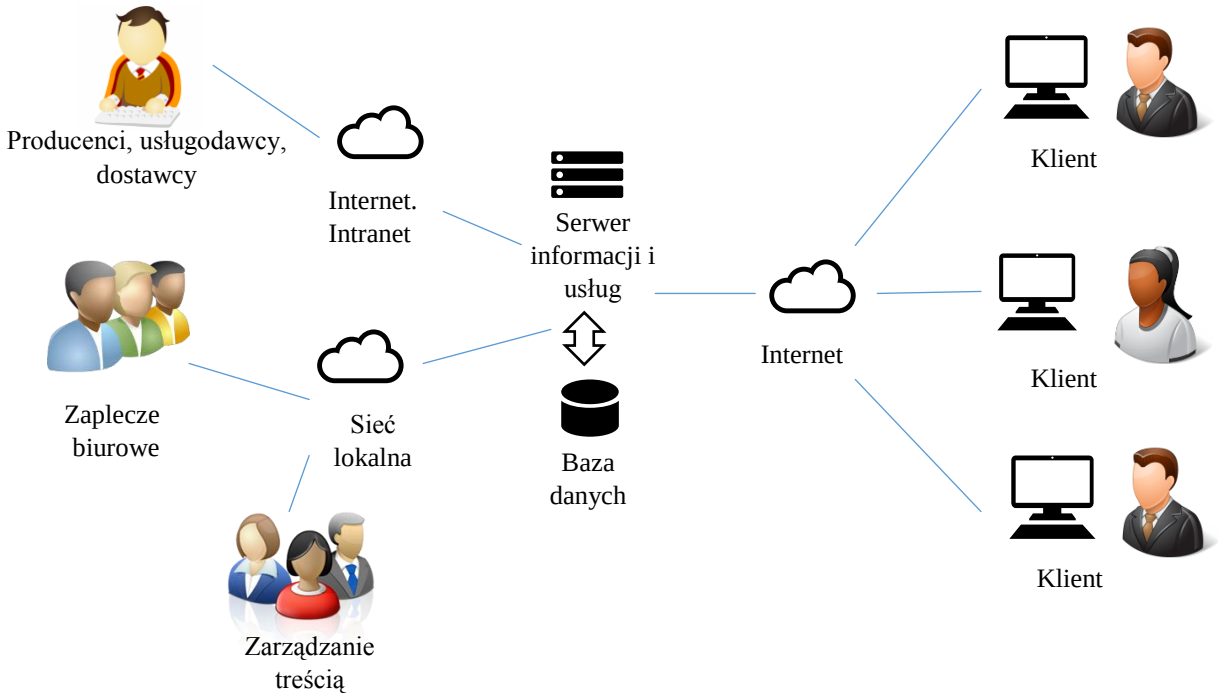
Przy realizacji projektu systemu dla handlu elektronicznego są wykorzystywane różne technologie informatyczne, z których najważniejsze to:

1. techniki związane z Internetem: sieci i serwery, HTML, Java, XML, PHP, WAP;
2. bazy danych: relacyjne, obiektowe, tekstowe, i inne;
3. języki programowania: Java, Perl, C++, C#, PHP i inne;
4. dedykowane systemy: finansowo-księgowe, zarządzanie treścią;
5. mechanizmy ochrony danych oraz dostępu do danych i usług;
6. inżynieria oprogramowania: profesjonalne prowadzenie projektów poprzez wszystkie fazy życia oprogramowania[19].

Najważniejszym zadaniem systemu informatycznego dla e-handlu jest zabezpieczenie pomostu między klientami, "back-office" i łańcuchem dostaw. Przykładowa architektura systemu handlu elektronicznego przedstawiana na rysunku 1.5.

[19] *IT w biznesie. Prowadzenie do handlu elektronicznego*, PJWSTK, Warszawa 2012.

Rysunek 1.5. Architektura systemu informatycznego dla e-handlu



Zródło: Opracowanie własne

Oczywiście dla każdej branży handlu elektronicznego może być inna architektura, ale główne i niezbędne elementy dla każdego systemu to – serwer informacyjny, baza danych, sieć lokalna i Internet.

1.6. Zalety i wady prowadzenia handlu elektronicznego.

Jak i handel tradycyjny tak i handel elektroniczny na swoje wady i zalety. Ogólnymi zaletami handlu elektronicznego są:

1. Łatwy i szybki dostęp do informacji.
2. Możliwość porównywania konkurencyjnych ofert.
3. Możliwość lepszego zapoznania się z ofertą.
4. Dostęp do szerszego asortymentu towarów.
5. Dostęp do oferty sklepów na całym świecie.
6. Bardziej szczegółowe opisy towarów.
7. Niższe ceny.
8. Możliwość przeglądania oferty oraz obsługa klienta 24/7.
9. Możliwość wyszukiwania towarów według dowolnego zadanego kryterium.

10. Możliwości testowania towaru przed kupnem.

Zalety handlu on-line dla sprzedawców:

1. Niski koszt.
2. Możliwość ciągłej i natychmiastowej aktualizacji oferty.
3. Bardziej szczegółowe opisy towarów +możliwość testowania przez klientów.
4. Uatrakcyjnienie oferty poprzez organizowanie licytacji.
5. Dostęp do nowych klientów.
6. Przyspieszenie procesów biznesowych.
7. Uzyskanie przewagi konkurencyjnej.
8. Dostęp do rynku światowego.
9. Skrócenie czasu dostępu do rynku towarów i usług.
10. Eliminacja negatywnego zjawiska sezonowości na rynku lokalnym.
11. Możliwości multimedialne, interaktywność.
12. Efektywność.
13. Żadnych zezwoleń na otwarcie sklepu w Internecie.
14. Wzrost wartości firmy, wzmocnienie jej pozycji.
15. Lepsze wykorzystanie możliwości produkcyjnych[20].

Zalety handlu on-line dla klientów:

1. Szybki i łatwy dostęp do informacji.
2. Dostęp do ofert z całego świata.
3. Możliwość przeczytania opinii o firmie/towarze/usłudze.
4. Możliwość przeglądania ofert przez 24 godziny na dobę/7 dni w tygodniu.
5. Zmniejszenie kosztów połączeń telekomunikacyjnych.
6. Niższe ceny towarów i usług, sprzedawanych przez Internet[21].

Do istotnych wad handlu elektronicznego z punktu widzenia klientów wyróżniamy następujące czynniki:

1. Brak pewności o bezpieczeństwie płatności przez sieć.
2. Niepewność dotycząca rzetelności sprzedawcy.

[20] *Ochrona prywatności konsumentów e-commerce*. http://www.een.org.pl/index.php/internet-i-handel-elektroniczny---spis/page/4/articles/ochrona-prywatnosci-konsumentow-e-commerce.html [dostęp 18.04.2015]
[21] *Zagadnienia handlu elektronicznego*, PJWSTK, Warszawa 2012.

3. Brak możliwości wypróbowania, czy oględzin zakupywanego towaru.

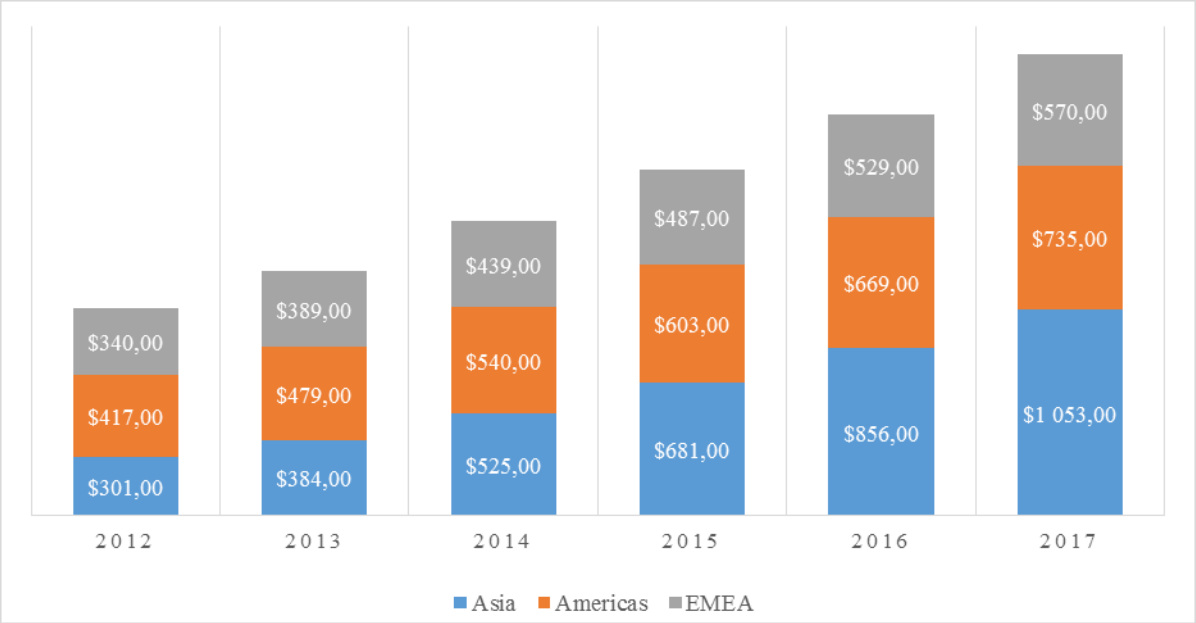
Ze strony firm istnieją następujące wady prowadzenia handlu elektronicznego:

1. Wysokie koszty dostarczenia towaru do klienta.
2. Brak efektywnego i rozbudowanego systemu spedycyjnego i dostawczego.
3. Brak efektywnej obsługi płatności kartami kredytowymi i nietypowymi płatnościami elektronicznymi.
4. Brak bezpieczeństwa danych.

Ale pomimo tych wad, które ma handel elektroniczny, dane statystyczne pokazują, że ten typ sprzedaży bardzo szybko rozwija się i technologie są doskonalsze.

Zgodnie z raportem Website of Marketer, sprzedaż przez Internet nadal rośnie w poszczególnych rejonach świata. Na rysunku 1.6. przedstawiono prognozy sprzedaży e-commerce do 2017r.[22].

Rysunek 1.6. Prognoza sprzedaży e-commerce w świecie



Źródło. Opracowanie własne na podstawie raportu z Marketer.com *Global B2C e-commerce sales to hit $1.3 trillion this year driving by growth in emerging markets.*

Liderem sprzedaż e-commerce jest Azja, na drugim miejscu Stany Zjednoczone, trzecie miejsce zajmują kraje Europy i Afryki.

[22] *Global B2C e-commerce sales to hit $1.3 trillion this year driving by growth in emerging markets*, http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649 [dostęp 04.05.2014]

1.7. Potrzeby realizacji handlu elektronicznego

Jak już wspomniano, handel elektroniczny ma dużo zalet dla przedsiębiorstw ze względu na otwarcie nowego biznesu, kontakt ze stałym klientami i poszukiwanie nowych. Coraz więcej przedsiębiorstw decyduje się na rozpoczniecie działalności handlowej w Internecie i głównymi czynnikami podjęcia takiej decyzji są:

1. Wydajność i oszczędności. Ten czynnik jest związany z wykorzystaniem procedur elektronicznych podczas nabywania produktów i usług, obsługi złożonych ofert, porównywania ofert konkurencji oraz tworzenia wydajnych kanałów dostaw i płatności. Są miedzy innym takie zalety: większa precyzja składanych zamówień, skrócenie cyklu realizacji, zmniejszenie kosztów analizy rynku i zoptymalizowane płatności.
2. Nowy kanał dystrybucji. Oznacza dla niektórych produktów rozpoczęcie sprzedaży drogą elektroniczną, jest dodatkowym kanałem dla tradycyjnych metod sprzedaży detalicznej, sieci sklepów czy ośrodków obsługi telefonicznej.
3. Zarządzanie kontaktami z klientem. W handlu elektronicznym zarządzanie relacjami z klientami staje znacznie łatwiejsze. Aby sprostać konkurencji i odnieść sukces, nie wystarczy tylko utrzymywanie strony WWW, należy zadbać o takie elementy jak wydajne zarządzanie transakcjami (od zamówienia do realizacji).
4. Usprawnienie obsługi klienta. Wykorzystanie Internetu pozwala zwiększyć zadowolenie klientów i jednocześnie zaoszczędzić na kosztach.
5. Koncentracja na kliencie.
6. Pozyskanie nowych klientów.
7. Przywiązywanie klienta do firmy.

Na dzień dzisiejszy dla prowadzenia handlu elektronicznego już nie wystarcza tylko przetwarzanie transakcji. Konieczne stało się rozwijanie kontaktów z klientami, dlatego należy skupić się na działaniach zmierzających do utworzenia atrakcyjnych interaktywnych ośrodków obsługi. Również jest bardzo ważne utrzymanie dotychczasowych klientów i pozyskanie nowych.

Rozwój handlu elektronicznego wiąże się z ogromnym zagrożeniem dotychczasowej stabilnej pozycji dla firm tradycyjnych. W Internecie pojawiają się nowe możliwości pozyskania nowych klientów, rozszerzenia oferty produktów i usług, utworzenia nowych kanałów komunikacji oraz zwiększenia zadowolenia i przywiązania klientów. Właśnie,

dlatego tradycyjne firmy powinny obawiać się jak najbardziej konkurentów, działających w handlu elektronicznych.

W tabeli 1.6 są zaprezentowane rozważania z uwzględnieniem potrzeb współczesnej firmy i korzyści z rozwoju handlu elektronicznego.

Tabela 1.6. Potrzeby i korzyści wynikające z zastosowania handlu elektronicznego

Potrzeby	Korzyści
Obecność na nowych rynkach	- globalny zasięg. - doskonalenie sprzedaży – koncentracja na działaniach strategicznych i generowaniu przychodów kosztem taktycznego zarządzania zamówieniami i szczegółami procesów. - dążenie do eliminowania pośredników. - pozyskanie nowych partnerów drogą elektroniczną. - przyspieszenie wprowadzania produktów na rynek.
Usprawnienia	- niskie koszty transakcji, obsługi klientów i wsparcia technicznego. - oszczędności na marketingu, dystrybucji i niesprzedanych produktach. - mniejsza przestrzeń magazynowa – integracja i prezentacja oferty w stronie WWW. - strategiczne planowanie zaopatrzenia.
Utrzymanie klientów	- lepsze kontakty z klientami osiągnięte dzięki samoobsługowemu składaniu zamówień, obsłudze klienta oraz pomocy technicznej i przywiązaniu klienta do firmy. - dynamiczny wielokierunkowy przepływ informacji w czasie rzeczywistym w relacjach sprzedawca-klient, klient-sprzedawca i klient-klient. - otrzymanie szczegółowego profilu klienta i możliwość analizy jego przyzwyczajeń i zastosowanie marketingu zidealizowanego.

Źródło: A.Kwasek, E-commerce i e-business jako nowe koncepcje organizacji procesów biznesowych. http://www.wsz-pou.edu.pl/magazyn/?strona=mag_kwasek87 [dostęp: 16.04.2014]

Model handlu elektronicznego szybko wkroczył w wiele obszarów biznesu i przywiódł zmiany, jakie obserwujemy dziś w metodach prowadzenia handlu i marketingu. Wykorzystując Internet w działalności handlowej, firmy otrzymują narzędzie o nadzwyczajnych możliwościach, które pozwala prowadzić walkę o przewagę konkurencyjną na rynku globalnym. Internet wymaga rezygnacji dotychczasowych systemów

organizacyjnych
i dostosowania firmy do nowych warunków. W innym przypadku firmie będzie bardzo trudno utrzymać swoją pozycję na rynku globalnym.

Trzeba wziąć pod uwagę, że samo posiadanie strony internetowej nie jest jeszcze handlem elektronicznym. Wiele firm wykorzystuje Internet, jako narzędzie promocji i nabycia informacji, sposób na zdobycie nowych klientów i kontaktów. Ale nie duża liczba firm decyduje się na uruchomienie sprzedaży przez Internet. W ostatnich latach bardzo szeroką popularność zdobywają urządzenia mobilne, codziennie ilość użytkowników smatfonów tylko wzrasta. Odpowiednio z tym idzie dynamiczny rozwój mobilnych kanałów handlowych
i serwisów społecznościowych[23].

1.8. Perspektywy i bariery rozwoju handlu elektronicznego

Od wielu lat rynek handlu elektronicznego jest oceniany, jako szczególnie perspektywiczny. Oprócz zalet handlu elektronicznego są bariery, utrudniające rozpoczęcie działalności w Internecie. Wśród barier niewynikających z intencji subiektów międzynarodowego obrotu towarowego należy wymienić: infrastrukturalne, ludzkie, proceduralne orz związane z technologiami informatycznymi.

Bariery w technologiach informatycznych przestają mieć istotne znaczenie ze względu na dynamiczny postęp w tej branży. Problem polega na tym, że posiadanie ostatnich technologii nie oznacza szybkiej, łatwej i bezpiecznej realizacji transakcji handlowych. Należy skoncentrować się na barierach, które znacznie utrudniają międzynarodowe obroty handlu elektronicznego (bariery infrastrukturalne, ludzkie i proceduralne).

Do bariery infrastrukturalnej odnosimy stabilność systemu walutowego, dostępność usług, dostępność informacji i ogólny poziom bezpieczeństwa obrotu handlowego w Internecie. Do likwidacji tej bariery są podejmowane działania dla stabilizacji światowej sytuacji ekonomicznej, ale nie jest to łatwo ze względu na różny poziom rozwoju poszczególnych krajów.

Mówiąc o barierze ludzkiej należy zwrócić uwagę na dwie grupy zagadnień:

[23] A.Kwasek, E-commerce i e-business jako nowe koncepcje organizacji procesów biznesowych. http://www.wsz-pou.edu.pl/magazyn/?strona=mag_kwasek87 [dostęp: 16.04.2014]

1. Na kompetencje komputerowe (niestety nadal aktualnym problemem zostaje brak dobrej znajomości technologii internetowych) i znajomość języków obcych (dla wstępu na globalny rynek handlu to jest niezbędne).
2. Na etykę osób realizujących i uczestniczących w handlu elektronicznym (chodzi tu o skłonności do działań korupcyjnych, skłonności do oszustwa).

Do działań likwidujących tę barierę można odnieść popularyzację edukacji komputerowej, podwyższenie poziomu znajomości języków obcych, łatwy dostęp do edukacji, wzmocnienie norm prawa.

Bariera proceduralna wiąże się z obsługą dokumentową elektronicznego obrotu handlowego. W każdym kraju są różne reguły prawne co do prowadzenia działalności handlowej w Internecie, co czyni skomplikowanym proces transakcyjny, realizowany pomiędzy partnerami biznesowymi z różnych krajów, lub konsumentami a sklepami internetowymi z różną lokalizacją[24].

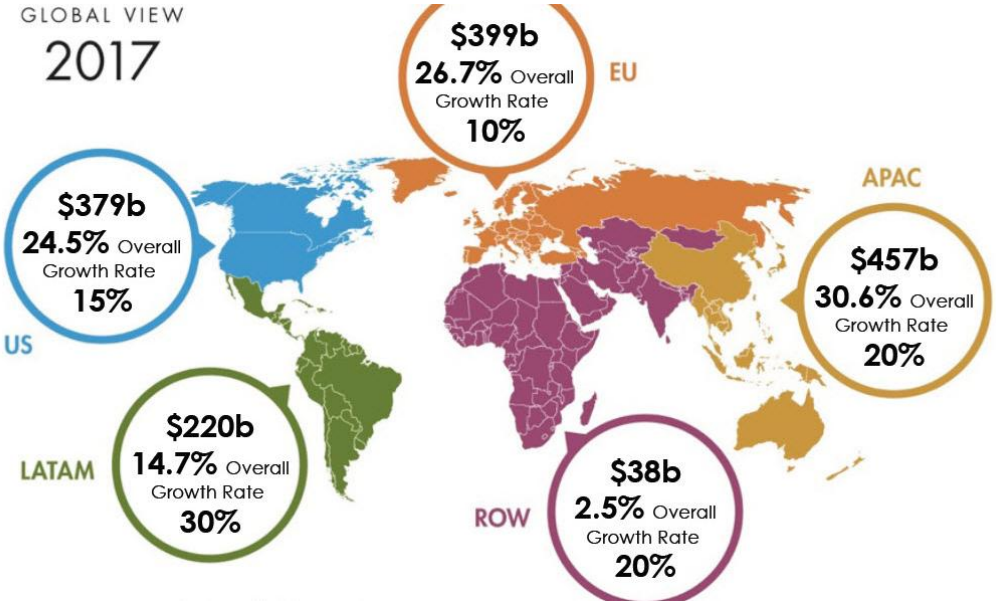
W celu zlikwidowania bariery proceduralnej podejmowane są globalnie i w poszczególnych krajach różnorodne działania zaradcze i standaryzacyjne. Jednym z przykładów jest powstanie w 1960 r. grupy roboczej ds. Upraszczania Procedur Handlowych (UN/ECE/WP.4), obecnie CEFACT (ang.Centre for trade Facilitation and Electronic Commerce), celem której jest podejmowanie działań, jakie sprawią prowadzenie handlu na poziomie globalnym takim łatwym jak i na poziomie lokalnym.

Jak można zobaczyć na rysunku 1.7 najszybciej rozwijającymi rynkami w handlu elektronicznym na świecie za prognozami raportu Forrester[25], są kraje Ameryki Północnej, Afryki i Azji. W innych częściach świata perspektywa rozwoju handlu elektronicznego jest oceniana na więcej niż 10%[26].

Mimo wszystko handel elektroniczny w Europie rozwija się dynamiczne. Za danymi raportu B2C E-commerce[27] za 2014 rok przychody ze sprzedanych towarów i usług za pośrednictwem Internetu wzrosły do 16,3%, i cały przychód z handlu elektronicznego stanowił 2,2% europejskiego PKB.

[24] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warzawa, 2004, s.97-99.
[25] *Global Selling Report 2013,* http://www.channeladvisor.com/platform/global-selling/ [dostęp 08.05.2014]
[26] *Forrester Research Online Retail Forecast 2017,* https://www.forrester.com/Forrester+Research+Online+Retail+Forecast+2013+To+2018+Western+Europe+Q4+2014+Update/fulltext/-/E-res120541 [dostęp 08.05.2014]
[27] Raport rozwoju e-commerce za 2014 rok, opublikowanego przez E-commerce Europe (https://www.ecommerce-europe.eu/)

Rysunek 1.7. Prognozy rozwoju handlu elektronicznego w świecie na 2017 rok.



Źródło: *Forrester Research Online Retail Forecast 2017*

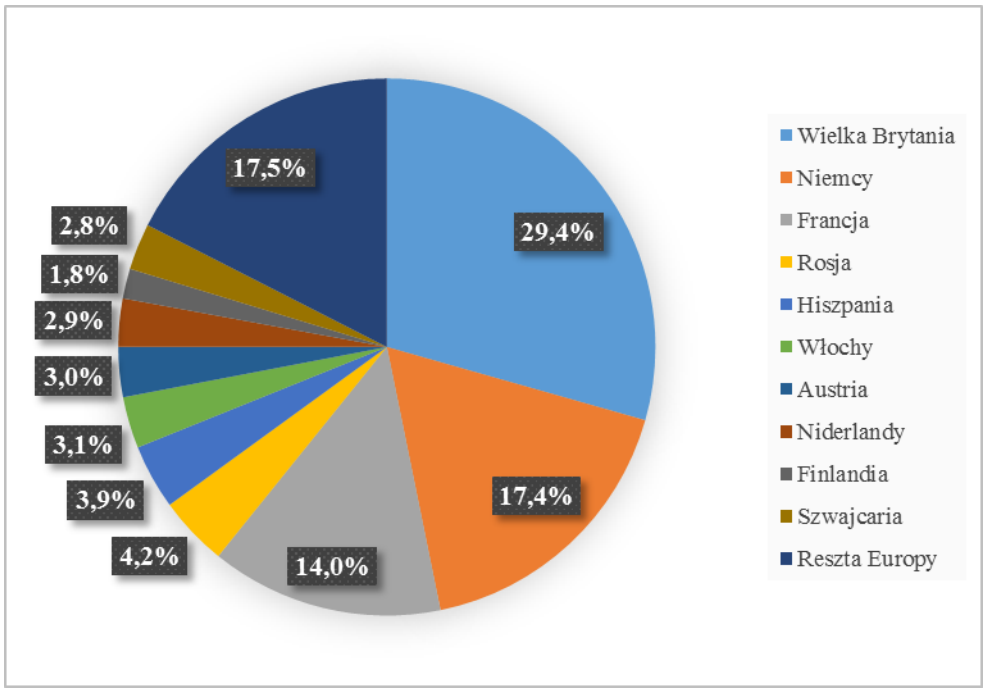
Istnieją jednak jeszcze duże różnice w rozwoju pomiędzy dojrzałymi rynkami w północno-zachodniej Europie, a krajami rozwijającymi się w Europie środkowo-wschodniej. Wielka Brytania, Niemcy i Francja są liderami w sprzedaży przez Internet i razem

produkują 60% od wszystkich sprzedaży e-commerce w Europie. Do krajów najbardziej się rozwijających się w Europie należą Rosja (€ 15500), Hiszpania (€ 14418), Włochy (€ 11268) i Polska (€ 5225). Dokładniej sytuację na rynku e-commerce w Europie można zobaczyć na rysunku 1.8.

Handel elektroniczny postrzegany jest jako główna siła Internetu i ważny katalizator osiągania celów strategii UE 2020 w obszarze rynku wewnętrznego.

Doceniając znaczenie rozwoju handlu elektronicznego, Parlament Europejski (PE) postanowił, żeby od 2013 roku był zapewniony szerokopasmowy dostęp do Internetu w całej Unii Europejskiej. Ma to zasadnicze znaczenie dla rozwoju handlu elektronicznego, bowiem brak dostępu do Internetu postrzegany jest jako jedna z najważniejszych przeszkód w korzystaniu z handlu elektronicznego.

Rysunek 1.8. TOP 10 krajów na europejskim rynku e-handlu



Źródło: Opracowanie własne na podstawie raportu Ecommerce Europe, 2014.

Głównymi trendami rozwoju e-commerce za prognozami ExactTarget[28] są następne: w 2017 roku przychód od sprzedaż e-commerce będzie $ 370 bln, 47% transakcji online będą z darmową wysyłka, powstaną nowe przepisy prawne, które pozwala na zwrot towaru, kupionego przez Internet i otrzymanie faktury VAT. 44% klientów będzie korzystało z możliwości odbioru towaru w sklepie, a 83% klientów będzie zadowolone z kupna towarów i usług w Internecie, z nich 62% klientów będzie robiło zakupy przez urządzenia mobilne.

Podsumowując, handel elektroniczny to szerokie pojęcie, które obejmuje procesy kupna i sprzedaży pośrednictwem Internetu. Powstał handel elektroniczny 20 lat temu, ale jego rozwój nie jest taki samy w różnych krajach świata. Popularność e-handlu wynika z wielu zalet jak i dla firm, tak i dla konsumentów. Istnieją różne modele biznesowe handlu elektronicznego, dlatego firmy mają wybór, w jaki sposób prowadzić biznes w Internecie. Chociaż handel elektroniczny i rozwija się bardzo szybko, są różne bariery dla jego dalszego rozwoju, to między innym niska kompetencja komputerowa użytkowników, brak lub niedoskonałość norm prawnych, regulujących działalność w Internecie. Ale za wynikami licznych badań globalny rynek e-commerce będzie i dalej dynamicznie się rozwijał.

[28] *State of marketing. Retail and e-commerce*, https://www.exacttarget.com/system/files_force/etmc-2014som_retail1.pdf [dostęp 08.05.2014]

Rozdział 2
Bezpieczeństwo technologiczne handlu elektronicznego

Uprawianie działalności gospodarczej z wykorzystaniem Internetu staje się coraz powszechniejsze, chociaż na drodze do elektronicznego biznesu nie brakuje istotnych przeszkód. Specyfika handlu elektronicznego, jego zmienna nowość i związany z tym brak wiedzy o zagrożeniach, zasadach i technikach zabezpieczenia powodują, że jest on bardzo narażony na ataki. Wymaganie pewnej i bezpiecznej wymiany informacji gospodarczych jest warunkiem koniecznym w przypadku każdej działalności handlowej. O bezpieczeństwo systemu handlu internetowego warto dbać, ponieważ zaniedbania w tym obszarze wpływają silnie na całą firmę, na jej reputację, na jej wyniki finansowe i na zdolność konkurowania z innymi firmami na rynku internetowym.

Rozróżnia się bezpieczeństwo technologiczne i bezpieczeństwo prawne. W tym rozdziale omówione zostaną zagadnienia bezpieczeństwa technologicznego.

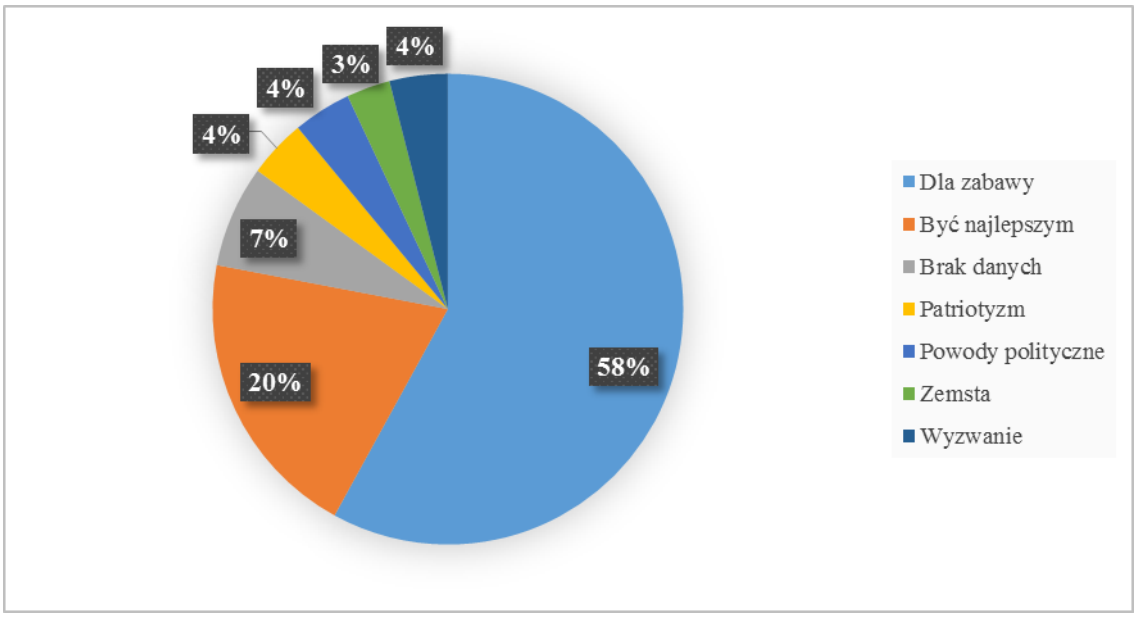
2.1. Sytuacja aktualna i pojęcie bezpieczeństwa

Jak mówi ogólna definicja, bezpieczeństwo to stan, który daje poczucie pewności istnienia i gwarancje jego zachowania oraz szanse na doskonalenie. Bezpieczeństwo jest ważne dla wszystkich dziedzin działalności ludzkiej.

Jeżeli chodzi o dziedzinę IT, tutaj bezpieczeństwo staje się coraz bardziej krytyczne, ze względu na to, że środowisko IT nie jest tylko narzędziem wymiany informacji, ale również miejscem działań biznesowych. Co minutę w Internecie przepływają dane poufne i dlatego organizacje stały się celami działań cyberprzestępczych, które mają wpływ na wydajność i rentowność firmy. Dlatego też firmy muszą chronić swoje aktywa i krytyczne usługi biznesowe poprzez efektywne mechanizmy zabezpieczeń technologicznych. Również bezpieczeństwo danych stanowi największą przeszkodę w szerszej popularyzacji elektronicznego handlu poprzez Internet. Za danymi statystycznymi motywy hakowania serwisów e-commerce są różne (rysunek 2.1). Motywami są: rozrywka, zabawa, nauka, ćwiczenie swoich nawyków, podjęcie wyzwania, zmierzanie do uzyskania korzyści (pieniądze), skrzywdzenie firmie przez złośliwy atak i tzw. haktywizm- forma protestu lub wyrażania poglądów politycznych[29].

[29] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.21.

Rysunek 2.1. Motywy hakowania serwisów e-commerce według serwisu Zone-H[30]



Źródło: L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.22.

W wykresie nie ma kategorii włamań dla pieniędzy, ale w ostatni czas coraz więcej włamań do stron internetowych, baz danych, serwisów stanowi swego rodu źródło dochodu hakerów.

Badania ankietowe przeprowadzone przez Datacom[31] w 2013 r. podają takie statystyki:

1. 90% badanych przyznało, że w ciągu poprzedniego roku stało się obiektem elektronicznego ataku.
2. 74% poniosło wydatki finansowe będące skutkiem włamania.
3. 71% znalazło nieautoryzowany dostęp do danych ze strony pracowników.
4. 70% wykryło inne niż wirusy zagrożenia dla systemu, kradzież informacji, sabotaż[32].

Powyższe statystyki pokazują, że realność zagrożeń jest na tyle duża, że potrzebuje szczególnej uwagi właścicieli biznesu w Internecie, administratorów serwerów i przeciętnych użytkowników.

Ogólny problem polega na tym, że hakerem niestety może stać się prawie każdy. Wystarczy dostęp do Internetu, wyszukiwarka, możliwość uruchamiania programów i podstawy wiedzy informatycznej. Ale osoby działające w taki sposób o bezpieczeństwie

[30] Ibidem, s.23
[31] Ibidem, s.24
[32] M.Niedźwiedziński, *Globalny handel elektroniczny*. Warzawa, 2004, s.91.

i oprogramowaniu wiedzą zazwyczaj niewiele, ale w ich rękach niektóre narzędzia mogą stać się naprawdę niebezpiecznie, a wygenerowane problemy niełatwe do likwidacji.

Dla lepszej wizji jak zapobiegać zagrożeniom, należy najpierw określić pojęcie bezpieczeństwa technologicznego.

Bezpieczeństwo technologiczne to zbiór zagadnień z dziedziny informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych w Internecie, rozpatrywany z perspektywy poufności, integralności i dostępności[33].

Jeżeli chodzi szczególnie o dziedzinie handlu elektronicznego, jaki opiera się na informacjach, najczęściej w formie elektronicznej, to w takim przypadku należy używać pojęcia bezpieczeństwa informacji.

Zgodnie z normą PN-ISO/IEC: 27001:2007[34] bezpieczeństwo informacji – to zachowanie poufności, integralności i dostępności informacji. Dodatkowo mogą być brane pod uwagę inne właściwości: autentyczność, rozłączalność, niezaprzeczalność i niezawodność.

Zabezpieczenie poufności polega na tym, że możliwość przeglądania informacji, mają tylko uprawione do tego osoby. Przykładem zniszczenia poufności może być wyciek informacji o klientach banku, ich danych osobowych, numerów kont, kwot na rachunkach itd.

Integralność oznacza właściwość, przy której dane nie zostaną uszkodzone, zmienione albo zniszczone przez osoby nieuprawnione. Jako przykład utraty integralności, możemy przedstawić zmianę danych: nazwy strony, zmianę nr konta bankowego docelowego, ogólną kwotę przelewu.

Pod terminem dostępności rozumiemy, że system będzie działał, kiedy oczekujemy, że będzie działał. Na przykład, brak dostępu do systemu sklepu internetowego na określony czas[35].

Ogólnie bezpieczeństwo to proces. Przy wdrażaniu bezpiecznego systemu handlu elektronicznego, należy ciągle go monitorować i zabezpieczać. Ale z innej strony, bezpieczeństwo poszczególnych elementów systemu e-commerce trzeba brać pod uwagę w świetle ich znaczenia dla biznesu.

---

[33] B. Pfitzmann, *A General Framework for Formal Notions of Secure" Systems*, Hildesheimer Informatik-Berichte 2012.

[34] PN-ISO/IES 27001:2007. *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

[35] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.26.

Z pojęciem „bezpieczeństwo technologiczne” ściśle związane jest pojęcie „zagrożenie technologiczne”, które jest jego antonimem.

Zagrożenia technologiczne – to zbiór wszystkich zasobów, które przeszkadzają prawidłowemu działaniu komputera, sieci komputerowej, przesyłaniu danych w Internecie itd.

Obecnie przyjmuje się, że właściwym podejściem do zagadnienia zarządzania bezpieczeństwem technologicznym jest ochrona strefowa. Polega ona na podzieleniu całego systemu IT na strefy związane z przetwarzaniem informacji o różnych atrybutach (wartości ekonomicznej i czasie życia) i realizujące odmienne zadania. Znajduje to odzwierciedlenie w obowiązującej dla tej sieci polityce bezpieczeństwa. Należy tu zauważyć, że posiadanie polityki bezpieczeństwa jest wymogiem podstawowym, którego spełnienie umożliwia zarządzanie bezpieczeństwem w organizacji.

Bardzo ważnym efektem dla firm jest analiza wszystkich możliwych zagrożeń i przyjmowanie miary dla zabezpieczenia efektywnego i prawidłowego bezpieczeństwa technologicznego.

Bezpieczeństwo handlu elektronicznego nie ogranicza się na jednym pojęciu. Składa się ono z wielu pojęć, których część jest wymieniona poniżej:

1. Bezpieczeństwo fizyczne serwerów, na których znajduje się aplikacja dla prowadzenia handlu elektronicznego.
2. Bezpieczeństwo systemów operacyjnych, w których jest zainstalowana aplikacja.
3. Bezpieczeństwo transakcji, w których przy przesyłaniu nic się nie zmieni i nikt oprócz odbiorcy i nadawcy nie zmoże przeczytać i odebrać informacji.
4. Bezpieczeństwo serwera DNS i domeny, żeby nikt nie miał możliwości ukraść nazwy domeny lub dokonać przekierowania czytelnika do innej podobnej strony.
5. Bezpieczeństwo aplikacji – utworzenie takiej aplikacji, żeby nie było na nią obcego wpływu, zmian, manipulowania.
6. Długotrwałość działania, innymi słowy takie zbudowanie systemu i nabycie takiej jego odporności, żeby w przypadku ataków mógł on dalej funkcjonować.
7. Bezpieczeństwo organizacyjne, czyli procesy, związane z zarządzaniem aplikacją, zmianami, wszystkimi elementami, dotyczących systemu.
8. Bezpieczeństwo prawne, czyli zarządzanie systemem zgodnie z prawem[36].

[36] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.78.

2.2. Obszary zagrożenia w handlu elektronicznym

Potencjalne zagrożenia w systemie e-commerce można podzielić na kilka grup:

1. Błąd człowieka. Najczęstsze źródło strat czasu oraz pieniędzy. Popełnianie błędów to część ludzkiej natury i wynika ono z nieostrożności, zmęczenia, stresu, braku doświadczenia

i innych aspektów. Nie możemy tych błędów w ogóle wyeliminować, ale możemy je znacznie zredukować przez poprawę warunków pracy, kształtowanie świadomości, ograniczanie uprawień.

2. Katastrofy naturalne. Bardzo trudne do przewidzenia, ale ewentualność ich wystąpienia jest mała. Jednak skutki tych katastrof są bardzo poważne i prowadzą do zawieszenia lub czasowego ograniczenia działalności systemu. Systemy o znaczeniu kontrolnym dla organizacji powinni być multiplikowane i muszą istnieć protestowane procedury bezpieczeństwa.

3. Awaria systemu przez uszkodzenie sprzętu, oprogramowania i infrastruktury. Przed awariami sprzętu jest łatwe i dostępne rozwiązanie – tworzenie kopii bezpieczeństwa w celu zapobiegania utracie danych. Jeżeli chodzi o awarie, związane z wadami oprogramowania, to w tym przypadku należy na bieżąco testować poprawność działania programów w systemie pod kątem bezpieczeństwa, zdolności, odporności na różnego rodzaju usterki. Najbardziej niebezpieczną awarią jest uszkodzenie infrastruktury, ponieważ infrastruktura działa niezależnie od firmy (instalacje telekomunikacyjne, elektryczne, transport). Niestety firma nie może w żaden sposób zapobiec tym awariom.

4. Włamanie do systemu. Polega na atakach ze strony pojedynczych osób lub grup organizowanych. Cele są różne – od otrzymania informacji poufnych do awarii systemu.

5. Niebezpieczne oprogramowanie. Oprogramowanie, które działa w sposób niewłaściwy z zamysłami użytkownika, może ono nieumyślnie zawierać błędy narażające użytkowników

na straty. Ale często usterki są celowo stworzone dla wywołania szkodliwych procesów, które również powodują negatywne skutki.

6. Zagrożenia wywołane przez czynniki pośrednie. Termin czynników pośrednich traktujemy jako ataki fizyczne na infrastrukturę (budynki, firmy usługowe i td), oraz ataki na bezpośrednich partnerów biznesowych[37].

[37] *Systemy e-commerce. Technologie internetowe w biznesie*, Praca zbiorowa pod redakcją Celiny M.Olszak, Katowice, 2004, s.230 -232

Omówiliśmy potencjalne zagrożenia, teraz przejdziemy do szczegółów. Istnieje wiele typów zagrożeń, awarii, luk w środowisku handlu elektronicznego. Nawet w uproszczonym scenariuszu e-commerce - kontakcie pojedynczego użytkownika w pojedynczej witrynie sieci Web, a następnie wprowadzenie karty kredytowej i adresu do wysyłki zakupu jest wiele zagrożeń dla bezpieczeństwa. W rzeczywistości nawet w tym prostym scenariuszu istnieje wiele systemów. Niżej rozpatrzymy najważniejsze zagrożenia, którym powinny przeciwdziałać stosowane środki bezpieczeństwa:

1. Bezpośredni atak polega na tym, że atakujący ma na celu zalogowanie się do aplikacji lub do systemu w ukrytych zamiarach, a nie jak prawidłowy użytkownik. W tym ataku mogą być wykonywane różne czynności, takie jak wykradanie lub odgadywanie haseł, stosowanie systemu operacyjnego lub aplikacji w rodzaju "furtek" (polega na tym, że zwykli użytkownicy mogą ładować i używać programy zawierające wirusy, „konie trojańskie", nawet o tym nie wiedząc). Takie „furtki" powodują usterki w pracy systemu lub pokonywanie procedur uwierzytelniania użytkownika.

Przedstawimy więcej typy ataków bezpośrednich. Ataki techniczne są jednym z najtrudniejszych rodzajów zagrożeń bezpieczeństwa. W szczególności Denial-of-service (DOS) ataki, są prowadzone zwykle w miejscach docelowych lub na ważnych serwerach internetowych, takich jak banki, serwery płatności kartami kredytowymi, duże sklepy internetowe i popularne serwisy społecznościowe.

DOS ataki doprowadzają do ogromnego obciążenia serwerów, sieci lub strony internetowej w celu sparaliżowania normalnej aktywności. Ochrona przed atakami DOS jest jednym z najbardziej skomplikowanych problemów bezpieczeństwa w Internecie dzisiaj. Jedną z głównych trudności w zapobieganiu takich ataków jest dotarcie do źródła ataku, ponieważ ataki często wykorzystują błędne lub fałszywe adresy IP, aby ukryć prawdziwe pochodzenie ataku.

Objawy DOS ataku są następne:

1. Niezwykły spadek wydajności sieci.
2. Niedostępność danej witryny internetowej.
3. Brak możliwości dostępu do dowolnej strony internetowej.
4. Gwałtowny wzrost ilości otrzymanego spamu.

DOS ataki mogą być wykonane na różne sposoby[38]. Ale w zależności od osobliwości działalności, czasu wystąpienia awarii, wywołanej przez atak, straty, powiązane z brakiem

[38] *Security Issues in E-Commerce,* http://webscience.ie/blog/2010/security-issues-in-e-commerce/ [dostep 08.07.2014]

dostępu do zasobów firmy są znaczące. Przy takim ataku największe straty będą u firm, które pracują w trybie ciągłym.

2. Utrata tajności polega na przechwycie danych w czasie transmisji, których potem można użyć w celach kryminalnych. Popularną techniką do uzyskania dostępu do systemu osoby kupującej, jest użycie narzędzia, takiego jak SZATAN, aby wykonać skanowanie portów

na komputerze, który wykrywa punkty wejścia do urządzenia. Na podstawie znalezionych otwartych portów, atakujący może korzystać z różnych technik w celu uzyskania dostępu do systemu użytkownika. Po zakończeniu skanowania atakujący może napisać kod do systemu, o podanie informacji osobistych, takich jak hasła. Niestety urządzenia służące do podsłuchu

w sieci LAN (sniffers) i WAN (datascopes) są już szeroko dostępne i mogą zostać użyte do tych nielegalnych celów.

3. Odgadywanie hasła użytkownika. Ten styl ataku jest wykonywany ręcznie lub automatycznie. Ataki ręczne są pracochłonne, a sukces możliwy jest tylko w tym przypadku, jeśli atakujący wie coś o kliencie. Na przykład, jeśli klient używa imienia swojego dziecka, jako hasło. Zautomatyzowane ataki mają większe prawdopodobieństwo sukcesu, ponieważ prawdopodobieństwo zgadywania ID użytkownika / hasła staje się coraz bardziej istotne. Istnieją narzędzia, które używają wszystkich słów w słowniku, aby sprawdzić identyfikator użytkownika, hasło lub kombinacje, które atakują popularne kombinacje ID użytkownika/hasła.

4. Modyfikacja danych. W czasie transmisji z danymi mogą być wykonywane zmiany. Na przykład po zakupie towarów za 1000$ atakujący zmieni dane tak, że będzie wynikać, że towar był kupiony jedynie za 10$.

5. Maskarada, czyli phishing. Główne narzędzie – to podanie atakującym innej bardzo podobnej strony zamiast uprawnionej. Może to być strona WWW o podobnym wskaźniku zasobów URL (zabezpiecza Uniform Resource Locator). Na przykład, http://www.ibm.com/shop/ będzie zarejestrowany przez atakującego, jako www.ibn.com/shop/ i klient prawdopodobnie nie zauważy różnicy. Maskarada ma na celu skompromitowanie danej firmy lub zbieranie pieniędzy pod fałszywym szyldem. Phishingiem są zwykle atakowane strony internetowego bankingu, internetowe serwisy aukcyjne (eBay), sprzedawcy internetowi (Amazon) i dostawcy usług (PayPal).

6. Zbieranie informacji. To można powiedzieć „zerowy” lub wstępny etap wszystkich powyżej wymienionych ataków. Polega na wyrafinowaniu narzędzi skanujących i systematycznie przeszukujących nasz serwer w celu znalezienia słabych miejsc w systemie zabezpieczeń. Większość tych narzędzi jest w szerokim dostępie i można je nawet darmowo pobrać w Internecie.

7. Inżynieria społeczna. Socjotechnika to sztuka manipulacji ludźmi do wykonywania działań lub ujawnienia poufnych informacji. Ataki inżynierii społecznej obejmują nadzór nad zachowaniem osoby kupującej i zbieranie informacji do wykorzystania przeciwko niej. Na przykład, nazwisko panieńskie matki jest często wspomagającym pytaniem i oczywiście odpowiedź na to pytanie jest jedna. Jeśli w jednym miejscu użytkownik już użył tego pytania, to równie prawdopodobne jest, że klient stosuję ten sam identyfikator i hasło logowania na innych stronach. Inżynieria społeczna stała się poważnym zagrożeniem dla bezpieczeństwa e-commerce, z powodu trudności wykrycia i zwalczania, ponieważ wiąże czynniki "ludzkie", które nie mogą być załatane tak, jak sprzęt lub oprogramowanie, chociaż szkolenie personelu i edukacja może nieco udaremnić atak[39].

Różne są fakty pojawienia poszczególnych zagrożeń. Nie jest możliwym zidentyfikowanie i zlokalizowanie wszystkie obszarów ryzyka, ale trzeba podjąć działania w celu przewidzenia największej liczby możliwych wariantów i zapobieganiu im.

Zagrożenia mogą wystąpić w takich obszarach jak:

1. Sprzęt. Przez uszkodzenie urządzeń, kradzież, nieprawidłowe działanie, powstanie błędów w oprogramowaniu.
2. Oprogramowanie. Dopuszczanie błędów przy napisaniu programów, w używanych algorytmach, niska jakość kodu, luki w systemach zabezpieczeń.
3. Infrastruktura. Uszkodzenia sieci elektrycznych, telekomunikacyjnych, systemów monitoringu i bezpieczeństwa.
4. Procedury bezpieczeństwa. Przez niewłaściwe zaprojektowanie, brak lub niedostateczne przetestowanie, zagrożenia „od wewnątrz”, luki w procedurach bezpieczeństwa[40].

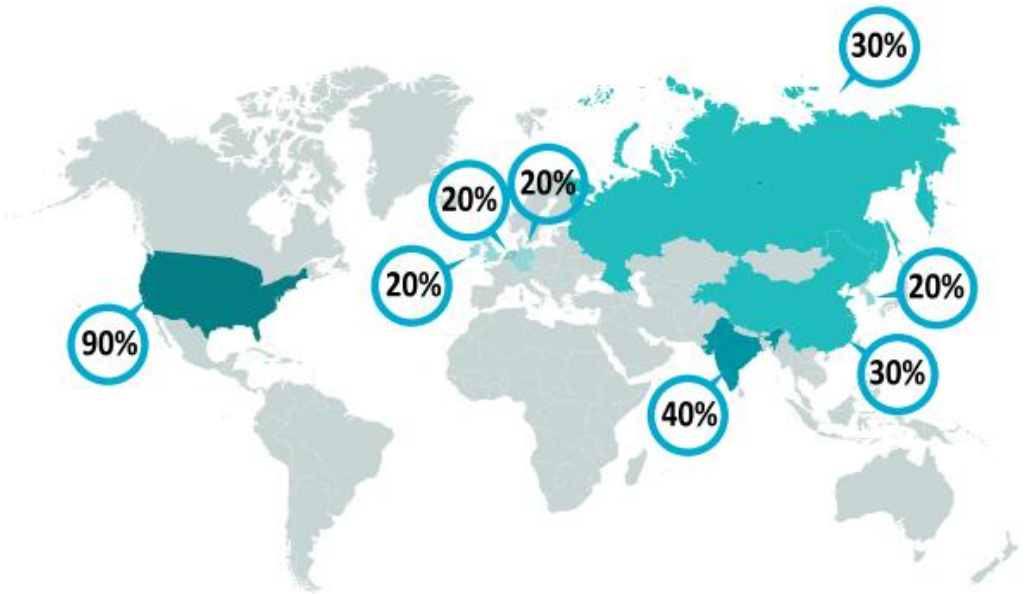
Za raportami najbardziej rozpoznawanych światowych firm zajmujących się monitorowaniem bezpieczeństwa jest kilka krajów kandydujących do tytułu źródła internetowego zła. Na liście znajdują się Stany Zjednoczone, Indie, Rosja, Chiny, Wielka

[39] A.Wawszczyk, *E-gospodarka, Poradnik przedsiębiorcy*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003, s.15.
[40] *Systemy e-commerce. Technologie internetowe w biznesie.* Praca zbiorowa pod redakcją Celiny M.Olszak, Katowice, 2004, s.234

Brytania, Niemcy, Holandia i Korea Południowa. Każdy z tych krajów, chociaż raz był zestawieniu TOP-3 dla najczęstszych źródeł zagrożeń w Internecie, takich jak: rozsyłanie spamu, zlokalizowanie stron phishingowych oraz występowanie infekujących stron[41].

Na rysunku 2.2. pokazana jest mapa najczęściej występujących krajów w zestawieniach top-3 źródeł ataków.

Rysunek 2.2. Mapa najczęściej występujących krajów w zestawieniach TOP-3 źródeł ataków.

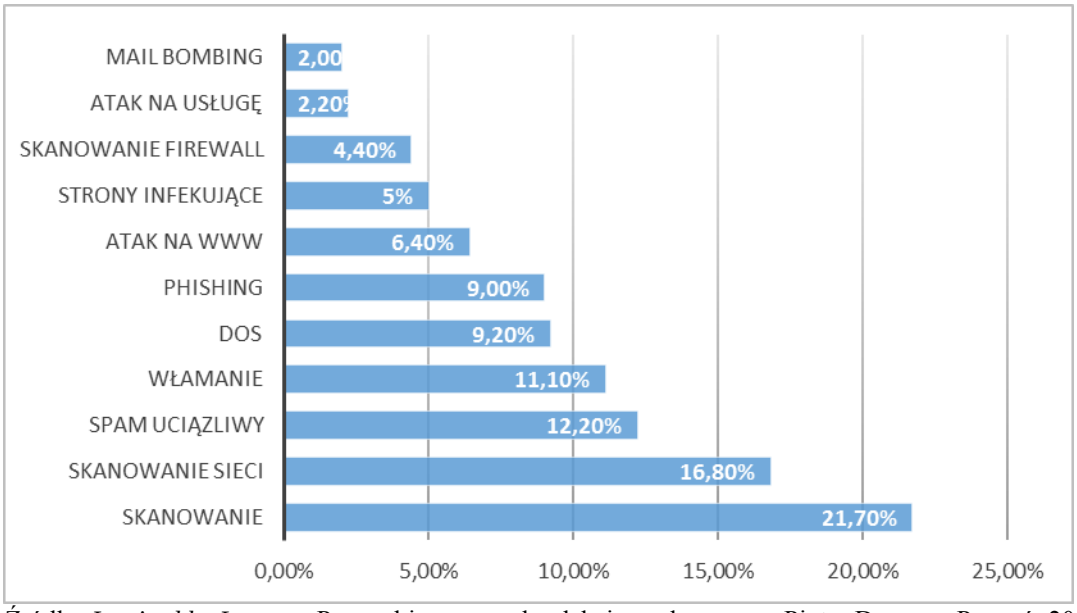


Źródło: Atak i Obrona 2013 Raport: Ataki i metody obrony w Internecie w Polsce, Warszawa 2014, s. 17

Na rysunku 2.3. przedstawmy statystyki najczęściej występujących atak w Internecie.

[41] *Atak i Obrona 2013 Raport: Ataki i metody obrony w Internecie w Polsce*, Warszawa 2014, s.12.

Rysunek 2.3. Najczęściej występujące ataki w Internecie



Źródło: *Inspired by Internet.* Praca zbiorowa pod redakcją naukową mgr Piotra Drygasa, Poznań, 2004, s.23.

Podsumowując, branża handlu elektronicznego stoi w obliczu wyzwań przyszłości w zakresie zagrożeń bezpieczeństwa i musi ich uniknąć. Wraz ze wzrostem wiedzy technicznej i jej szerokiej dostępności w Internecie, przestępcy są coraz bardziej wyrafinowani
w oszustwach i atakach, które mogą wykonywać. Świadomość zagrożeń i realizacji wielowarstwowych protokołów bezpieczeństwa, szczegółowe i otwarte zasady prywatności oraz silnie środki uwierzytelniania i szyfrowania zapewnią konsumentowi pewność i utrzymanie minimalne ryzyko.

2.3. Cele i strategie bezpieczeństwa technologicznego

Nieprawidłowe udostępnianie i użycie dowolnej usługi internetowej stwarza zagrożenie bezpieczeństwa systemu i sieci, do której ta usługa jest podłączona. Reguły, dotyczące czynności, związane z zasobami komunikacyjnymi i komputerowymi są zapisane w strategii bezpieczeństwa firmy lub organizacji. Reguły te obejmują takie zagadnienia, jak ochrona fizyczna, ochrona personelu, ochrona administracyjna i bezpieczeństwo sieci.

Strategia bezpieczeństwa również definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu. Strategia bezpieczeństwa to podstawa wszystkich działań, co do bezpieczeństwa informacyjnego firmy. W strategii są opisane

obszary odpowiedzialności użytkownika, administratorów, sposoby monitorowania skuteczności podjętych zabiegów.

Dla opracowania strategii bezpieczeństwa należy na początku określić cele bezpieczeństwa.

Podczas tworzenia i wdrażania strategii bezpieczeństwa należy precyzyjnie określić jej cele. Cele związane z bezpieczeństwem należą do jednej lub kilku wymienionych kategorii:

1. Ochrona zasobów. Ten cel oznacza zapewnienie dostępu do systemu tylko uprawnionym użytkownikom. Dla osiągnięcia celu należy dokładnie zdefiniować kategorie użytkowników mających dostęp do systemu i określić uprawienia dostępu, który będą miały różne grupy użytkowników.
2. Uwierzytelnianie. Chodzi o sprawdzenie, czy zasób (człowiek lub komputer) przy próbie dostępu do systemu naprawdę jest tym, za co lub kogo się podaje. Niezawodne uwierzytelnianie chroni system przed fałszywymi użytkownikami. Najczęściej do uwierzytelniania są wykorzystane nazwy i hasła użytkowników. Ale istnieje bezpieczniejsza metoda – używanie certyfikatów cyfrowych.
3. Nadawanie uprawnień. Oznacza pewność, że zasób (osoba lub komputer), zalogowany do systemu ma uprawnienia do wykonania żądania. Nadawanie uprawnień to proces określania, kto lub co może uzyskać dostęp do zasobu systemu lub wykonać w systemie określoną czynność.
4. Integralność. Oznacza pewność, że napływające informacje są identyczne z wysłanymi. Wyodrębniają dwie koncepcje integralności: integralność danych i integralność systemu.
   a. Integralność danych oznacza, że dane są zabezpieczone przed nieuprawnionymi zmianami lub manipulacjami.
   b. Integralność systemu: system dostarcza spójne, oczekiwane wyniki przy zachowaniu spodziewanej wydajności.
5. Nieodrzucanie to dowód przeprowadzenia transakcji lub wysłania albo odebrania wiadomości. Nieodrzucanie obsługuje użycie certyfikatów cyfrowych i szyfrowania z kluczem publicznym do podpisywania transakcji, komunikatów i dokumentów. I nadawca i odbiorca zgadzają się, że odbyła się wymiana. W tej operacji za dowód wystarcza opatrzenie danych cyfrowym podpisem.
6. Poufność oznacza pewność, że tajne informacje pozostają prywatne i nie są widoczne dla podglądaczy. To kluczowy element pełnej ochrony danych. Dla poufności jest

zastosowana metoda szyfrowania. Szyfrowanie odbywa się za pomocą certyfikatów cyfrowych i protokołu SSL (Secure Sockets Layer) lub połączenie przez sieć VPN (Virtual Private Network) pomaga zapewnić poufność danych podczas przesyłania ich przez sieci niezaufane.

7. Kontrolowanie działań związanych z bezpieczeństwem. Działania w celu bezpieczeństwa będą bezsensowne, jeżeli nie są monitorowane zdarzenia i efektywność działań zabezpieczających.

Jeśli utworzyliśmy strategię bezpieczeństwa, należy podjąć kroki w celu wdrożenia w firmie reguł strategii bezpieczeństwa. Działania te między innym obejmują szkolenie pracowników oraz instalację sprzętu i oprogramowania niezbędnego do wdrożenia tych reguł[42]. Zabezpieczenie systemu e-handlu to proces ciągły i zabezpieczenia powinny być stale testowane, jak i przez użytkowników oraz administratorów, tak i przez specjalistów zewnętrznych. Również w każdej firmie powinna być własna polityka bezpieczeństwa, którą należy stworzyć na etapie zakładania firmy.

Poprawnie zdefiniowana polityka bezpieczeństwa powinna zawierać:

1. Definicję celów zabezpieczenia systemu informacyjnego.
2. Strukturę organizacyjną oraz zdefiniowanie odpowiedzialności za wszystkie aspekty zabezpieczenia.
3. Opis strategii zarządzania ryzykiem.
4. Określenie wszystkich wymagań zabezpieczenia systemu elektronicznego.
5. Opis wybranych mechanizmów zabezpieczeń.
6. Sposób akredytacji zabezpieczenia systemu informacyjnego, w tym audytu wewnętrznego i zewnętrznego[43].

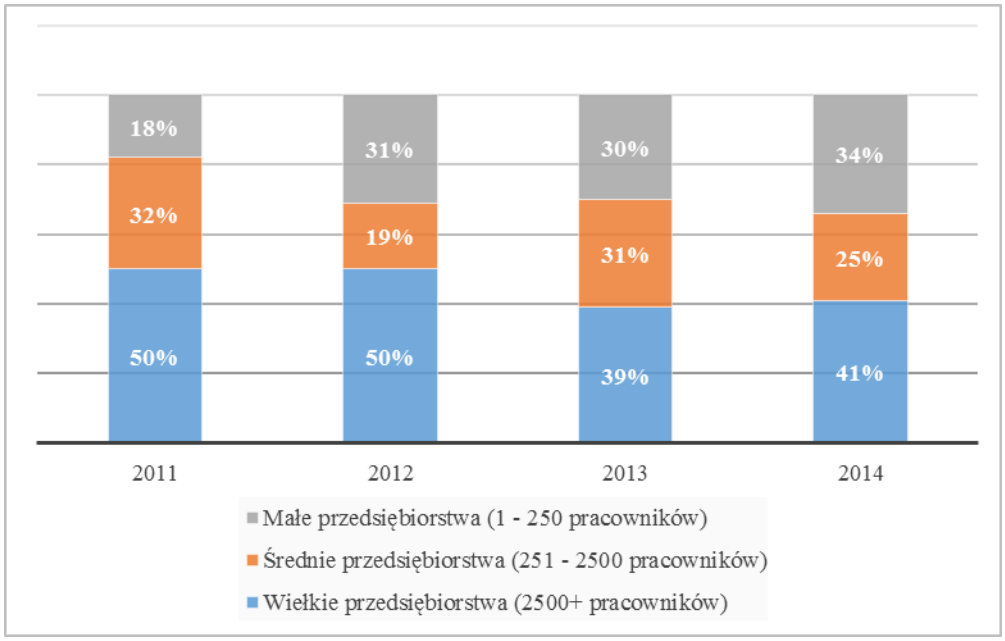
2.4. Zarządzanie bezpieczeństwem w handlu elektronicznym

Według raportu firmy Symantec dotyczącego zagrożeń w Internecie (Internet Security Thred Report)[44] w roku 2014 było 9 bln. na 552 mln. obiektów sieciowych, a 41% ataków było na firmy, zatrudniające powyżej 2500 pracowników, ale w porównaniu z 2011 rokiem zwiększa się również ilość ataków na przedsiębiorstwa małe. Na rysunku 2.4 przedstawimy wyciąg

z raportu o ilości atak w zależności od rozmiaru przedsiębiorstw.

[42] *Bezpieczeństwo Serwery System i bezpieczeństwo internetowe.* Wersja 6 wydanie 1. Wydawnictwo IBM.
[43] *Inspired by Internet.* Praca zbiorowa pod redakcją naukową mgr Piotra Drygasa, Poznań, 2004, s.28.
[44] *Internet Security Thred Report 2015*, Symantek 2015, s.11-15.

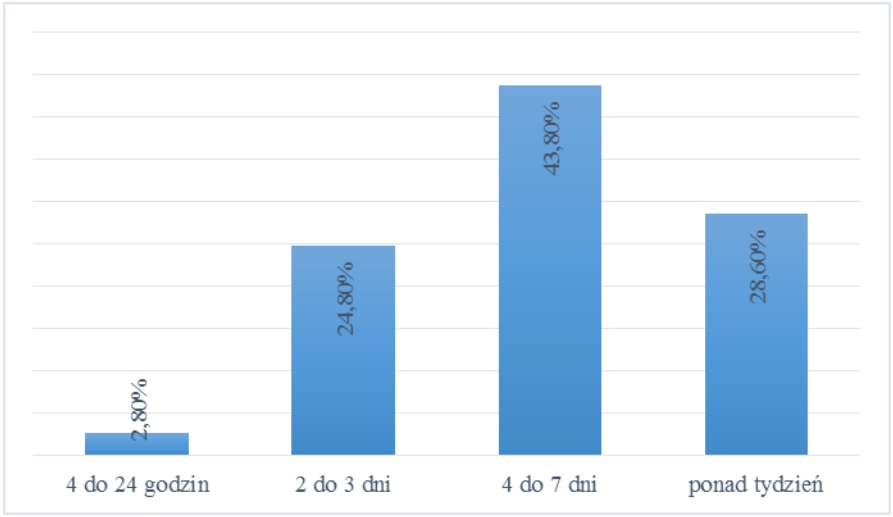
Rysunek 2.4. Podział ataków hostingowych według rozmiaru firmy



Źródło: *Internet Security Thred Report 2015*, Symantek 2015, s.11

Należy wziąć pod uwagę, że awaria systemu internetowego może mieć bardzo poważne efekty negatywne dla przedsiębiorstwa. Według danych firmy Debis Systemhaus GmbH[45] awarię trwającą 2-3 dni jest w stanie przetrwać 70% firm, jednak, gdy awaria jest dłuższa ryzyko upadłości jest już znaczne. Na rysunku 2.5 przedstawimy podział czasu awarii i ryzyka upadłości firm.

Rysunek 2.5. Czas awarii a ryzyko upadłości przedsiębiorstwa



Źródło: *PC World Komputer Pro – Bezpieczeństwo systemów*, SecurITy, nr 2/2003, s.68.

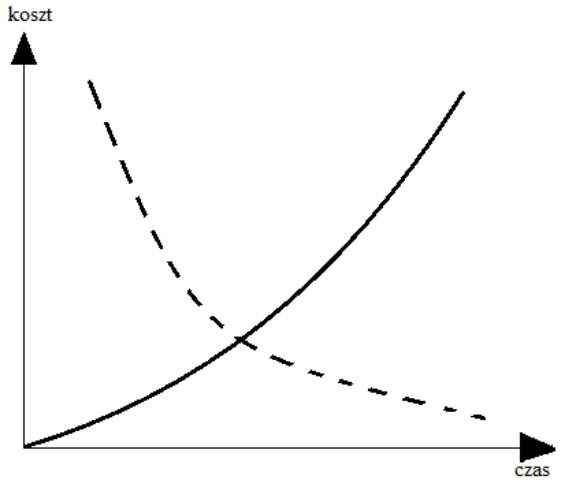
[45] *Debis Systemhaus GmbH Report 2012*, http://www.channelpartner.de/schwerpunkt/Debis%20Systemhaus [dostep 10.07.2014]

Nie istnieją uniwersalne rozwiązania dotyczące zabezpieczenia systemów e-commerce danej firmy. Należy wziąć pod uwagę wiele czynników, takich jak zakres działalności, kultura organizacyjna, wielkość jednostki czy stopień tajności przechowywanych informacji. Dla zarządzania bezpieczeństwem należy korzystać na początku z dwóch narzędzi – analiza wpływu na biznes i analiza ryzyka.

1. Analiza wpływu na biznes.

Analiza wpływu na biznes (BIA-ang.business impact analysis) – to ocena tego, jak przerwa w działaniu określonego procesu wpływa na działalność systemu i firmy. Jest to całościowa analiza procesów, działających w firmie, która wyznacza procesy krytyczne i pokazuje na osi czasu, jakie będą negatywne skutki ich przerywania (rysunek 2.6).

Rysunek 2.6. Wykres analizy wpływu na biznes (BIA)



Źródło: L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.26.

Za pomocą wykresu szacujemy to, co się stanie, jeżeli dany proces nie będzie aktywny minutę, godzinę, dzień itd. W znacznej części przypadków handlu elektronicznego będzie to zależność liniowa. Przykładowo, jeśli średnio sklep internetowy osiąga przychód 10 000 $ dziennie, to przerwa tygodniowa będzie oznaczać, że sklep nie otrzyma około 70 000 $. W przypadku, gdzie firma nie ma wystarczającej kwoty finansowej na przetrwanie takiej przerwy, może to oznaczać nawet bankructwo. Z innej strony, również negatywnym skutkiem jest utrata reputacji i klientów.

Czas, na jaki można wstrzymać proces biznesowy bez istotnych strat dla biznesu, specjaliści wyznaczają terminem RTO (ang. recovery time objective). Dzięki analizie wpływu na biznes (BIA) przedsiębiorcy wiedzą, jakie procesy są najważniejsze w ich działalności i jest w stanie wyznaczyć, jakie zasoby biorą udział w tych procesach. To pozwala na

znalezienie równowagi pomiędzy tym ile firma powinna zainwestować w bezpieczeństwo systemu a potencjalną stratą.

Na wykresie powyżej przedstawiono, w jaki sposób można wyznaczyć, jaką ilość pieniędzy należy inwestować w zabezpieczenie systemu. Linia ciągła przedstawia straty poniesione w rezultacie zawieszenia procesu. Linia przerywana pokazuje ile wynoszą inwestycje w sposób, zapobiegający przerwom w procesach. Oczywiście, im krótsza przerwa jest dopuszczana, tym więcej potrzebujemy inwestycji[46].

2. Szacowanie ryzyka

Analiza ryzyka oznacza zestaw specjalnych działań, skierowany na zredukowanie wpływu ryzyka na funkcjonowanie danego systemu i podejmowanie odpowiednich działań dla zapobiegania i minimalizacji ryzyka.

Wyjaśnijmy pojęcia, jakie pojawiają się w analizie ryzyka. Zagrożenia – w systemie e-commerce to użytkownicy, cyberprzestępcy, hakerzy. Podatności – procesy codzienne, złożoność i jakość systemu. Ryzyko inherentne, inaczej ryzyko pierwotne, czyli poziom zagrożenia, jaki występuje, gdy niema żadnych zabezpieczeń. Zabezpieczenia - działania, podejmowane w celu zmniejszenia ryzyka. Nowy poziom ryzyka, po zastosowaniu zabezpieczeń, nazywa się ryzykiem szczątkowym lub rezydualnym. Gdy możliwość zagrożeń systemu jest na tyle niewielka, że pozwała na zaakceptowanie, to nazywamy ten stan ryzykiem dopuszczalnym. Warto podkreślić, że ryzyko jest nieodłącznym elementem nie tylko handlu internetowego, a całego życia i jego procesów.

Analiza ryzyka to narzędzie, które pozwała racjonalne i celowo wydawać na zabezpieczenia, a w sytuacji, kiedy budżet firmy jest na moment niewystarczający wyznaczać priorytety i w jakiej kolejności nimi zarządzać[47].

2.5. Tradycyjne metody bezpieczeństwa danych w sieci Internet

Pod tradycyjnymi narzędziami dla zabezpieczenia przepływu danych w Internecie rozumiemy szyfrowanie i podpis cyfrowy, o których szczegółowo będziemy mówić w tym rozdziale.

[46] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.28.
[47] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.30-31

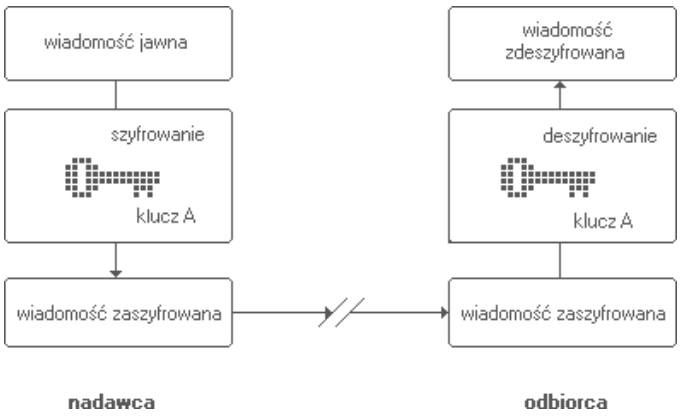
2.5.1. Szyfrowanie

Szyfrowanie już stało się klasyczną metodą bezpieczeństwa. Na świecie stosuje się wiele metod szyfrowania. Głównym celem jest gwarancja poufności danych podczas ich transmisji przez sieć publiczną (Internet). Dlatego jednym z najbardziej efektywnych sposobów ochrony sieci jest szyfrowanie wszystkich danych przesyłanych przez sieć i w taki sposób, żeby dla osoby nieuprawnionej nie było żadnych możliwości do odczytania przesyłanych danych.

1. Szyfrowanie symetryczne

Szyfrowanie symetryczne polega na tym, że do szyfrowania i deszyfrowania używamy tego samego klucza szyfrującego. Ogólny uproszczony schemat szyfrowania niesymetrycznego jest przedstawiony na rysunku 2.7.

Rysunek 2.7. Schemat szyfrowania symetrycznego



Źródło: *Wprowadzenie do PKI*, http://www.signet.pl/pki.html [dostęp 15.07.2014]

Najbardziej powszechnym standardem kryptograficznym jest system DES, który został stworzony w łatach 70 przez firmę IBM. Jest to system symetryczny, który ma klucz prywatny o 56 bitach. Klucz jest rozszerzony do 64 bitów, przy dodawaniu 8 bitów parzystości i w tej formie stosowany jest do szyfrowania danych, dzielonych na bloki mające też po 64 bity. Algorytm pobiera te 64-bitowe bloki danych z kluczem i za pomocą skomplikowanego ciągu operacji dokonywanych na poziomie pojedynczych bitów, takich jak LUB wykluczające (exclussive-OR), z jednoczesnym przesuwaniem bitów[48].

Aktualnie standard DES nie jest już uważany za dostatecznie silny mechanizm, ponieważ obciążony jest wadami. Klucz musi być dostarczonym (poza siecią) do nadawcy i odbiorcy. Ale jest to utrudnione w przypadku informacji z dużą ilością odbiorców, dlatego że

[48] A.Wawszczyk, *E-gospodarka, Poradnik przedsiębiorcy*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003, s.25.

każdy powinien mieć unikalny klucz, a nadawca powinien pamiętać klucz każdego odbiorcy. Sposobem usunięcia tych zasad jest skorzystanie z usług zaufanego pośrednika, który wygeneruje klucze do obu stron i udostępni je.[49]

Algorytm działa w kilku etapach:

1. Tekst jawny, który podlega szyfrowaniu, jest dzielony na bloki 64-bitowe i dalej wykonujemy algorytm dla każdego bloku.
2. Dokonujemy permutację początkową bloku, która ma na celu przestawienie bitów w odpowiedni sposób.
3. Blok wejściowy rozdzielamy na dwie 32-bitowe części: lewą oraz prawą.
4. Wykonujemy 16 cykli jednakowych operacji (funkcje Feistela), podczas których łączymy dane z kluczem. Operacje te wyglądają następująco:
   a. Przesuwamy bity klucza, a następnie wybieramy 48 z 56 bitów klucza.
   b. Rozszerzamy prawą część danych do 48-bitów za pomocą permutacji rozszerzonej.
   c. Sumujemy rozszerzoną prawą połowę o modulo 2 z wybranymi wcześniej (i już przesuniętymi) 48 bitami klucza.
   d. Sumujemy dane dzielone na osiem 6-bitowych bloków i każdy blok podajemy na wejście jednego z S-bloków (pierwszy 6-bitowy blok na wejście pierwszego S-bloku, drugi 6-bitowy blok na wejście drugiego S-bloku, itd.).
   e. Pierwszy i ostatni bit danych określa wiersz, a pozostałe bity kolumnę S-bloku.
   f. Po wyznaczeniu miejsca w tabeli, odczytuje się wartość i zamienia na zapis dwójkowy. Wynikiem działania każdego S-bloku są 4 bity wyjściowe – tworzą one 32-bitowe wyjście S-bloków. Każdy S-Blok ma inną strukturę.
   g. Po wyjściu z S-bloków ponownie przechodzimy permutację w P-blokach
   h. Bity przekształconego bloku sumujemy z bitami lewej połowy danych. W taki sposób zmieniony blok staje się nową prawą połową, a poprzednia prawa połowa staje lewą połową, co oznacza, że cykl dobiegł końca.
5. Po wykonaniu 16 cykli operacji prawa i lewa połowa danych jest łączona w 64-bitowy blok i dokonujemy permutację końcowa[50].

Deszyfrowanie polega na zastosowaniu tych samych operacji w odwrotnej kolejności (różni się od szyfrowania tylko wyborem podkluczy, który teraz odbywa się od końca)[51].

---

[49] *Systemy e-commerce. Technologie internetowe w biznesie*. Praca zbiorowa pod redakcją Celiny M.Olszak, Katowice, 2004, s.236

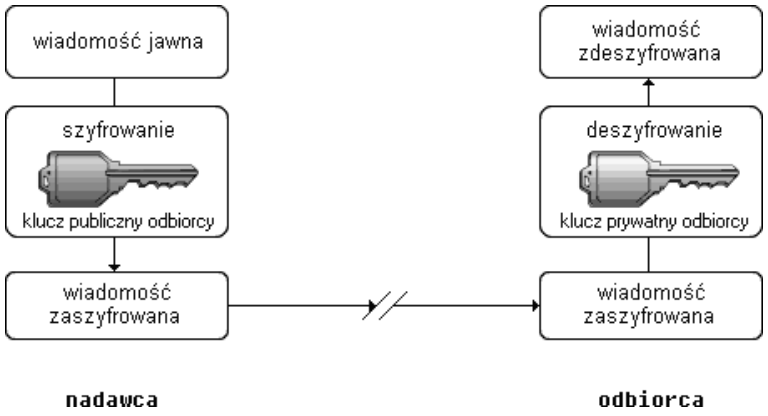
[50] R.Tanas. *Kryptografia*, Poznań 2009, s.44.

2. Szyfrowanie niesymetryczne

Alternatywnym sposobem jest kryptografia z kluczem publicznym. Jest to system, w jakim każdy użytkownik posiada parę kluczy: jeden prywatny i jeden publiczny. Kluczem prywatnym można rozszyfrować wiadomość, która została zaszyfrowana przy użyciu kluczu prywatnego, tak, iż możemy otrzymywać komunikaty od każdego, kto zna nasz klucz publiczny, (które rozszyfrowujemy, używając naszego klucza prywatnego). Możemy także wysyłać zaszyfrowane komunikaty każdemu, kogo klucz publiczny znamy.

Taką kryptografię nazywamy niesymetryczną, ze względu na odmienne klucze używane w ciągu szyfrowania i rozszyfrowywania wiadomości. Na rysunku 2.8 przedstawimy ogólny schemat szyfrowania niesymetrycznego.

Rysunek 2.8. Schemat szyfrowania niesymetrycznego



Źródło: *Wprowadzenie do PKI*, http://www.signet.pl/pki.html [dostęp 15.07.2014]

Stosowanie systemów z kluczem publicznym może odbywać się na dwa sposoby - za ich pomocą można uzyskać dyskrecje: klucz publiczny szyfruje dokument, a z pomocą może go odczytać jedynie właściciel odpowiedniego klucza prywatnego. Podejście to często jest stosowane, jako bezpieczny sposób wymiany kluczy symetrycznych oraz do tworzenia podpisu cyfrowego. Stanowi to podstawę do potwierdzenia, spójności oraz wiarogodności.

Najczęściej wykorzystywanym algorytmem w szyfrowaniu asymetrycznym jest algorytm RSA. Szyfrowanie odbywa się z wykorzystaniem dwóch kluczy szyfrujących. Użytkownik szyfruje swoje posłanie za pomocą klucza prywatnego i publicznego odbiorcy. Wiadomość zaszyfrowaną odbiorca może odczytać przy użyciu swojego klucza prywatnego i przy pomocy klucza publicznego od nadawcy.

Metody dystrybucji kluczy publicznych można podzielić na cztery grupy:

1. Ogłoszenie publiczne.

[51] Ibidem, s. 45-50.

2. Katalog ogólne dostępny.

3. Organ zarządzający kluczami jawnymi (public-key authority).

4. Certyfikaty kluczy jawnych[52].

Algorytm szyfrowania RSA jest następujący:

1. Generacja kluczy. Dla generacji prywatnego i publicznego klucza używamy takiego algorytm:

a. Losowo są wybierane dwie wielkie liczby pierwsze p i q (najlepiej, żeby oba klucze miały wartość w bitach i były odległymi wartościami od siebie).

b. Dalej obliczamy wartość $n = p \cdot q$.

c. Dla n obliczamy wartość funkcji Eulera.

d. Odnajdujemy liczbę e $(1 < e < \varphi(n))$ stosunkowo pierwszej z $\varphi(n)$.

e. Wyliczamy liczbę d, która jest różnicą z antytetycznością liczby e i jest podzielna przez $\varphi(n)$: $d \equiv e^{-1}(mod(\varphi(n))$.

f. Klucz publiczny jest definiowany jako para liczb(n, e), natomiast kluczem prywatnym jest para (n, d).

2. Szyfrowanie i deszyfrowanie. Przed tym, jak zaszyfrowujemy posłanie, dzielimy go na bloki m o wartości liczbowej nie większej niż n. Po tym każdy z bloków szyfrujemy według równania: $c \equiv m^e \, (mod \, n)$. Zaszyfrowana wiadomość składa się z kolejnych bloków c. Ponownie stworzony szyfrogram przekształcamy na tekst jawny, przy szyfrowaniu kolejnych bloków według wzoru:$m \equiv c^d (mod \, n)$.

3. Własności operacji szyfrowania i deszyfrowania. Niech $C_{K1}, D_{K1}, C_{K2}, D_{K2}$ to kolejne szyfrowanie i deszyfrowanie kluczami $K1, K2$. Wtedy mamy: $C_{K1}\big(C_{K2}(M)\big) = C_{K2}\big(C_{K1}(M)\big)$, co oznacza komutatywność operacji szyfrowania, a $D_{K1}\big(D_{K2}(M)\big) = D_{K2}\big(D_{K1}(M)\big)$ - komutatywność operacji deszyfrowania.

4. Podpisywanie i weryfikacja podpisu. RSA również jest używane do przeprowadzenia operacji podpisu. W takim przypadku szyfrujemy skrót wiadomości, używając klucza prywatnego i aktywizujemy taki szyfrogram wraz z oryginalną wiadomością. Odbiorca, która ma klucz publiczny jest w stanie zdeszyfrować wartość funkcji skrótu oraz porównać

[52] A.Wawszczyk, *E-gospodarka, Poradnik przedsiębiorcy,* Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003, s.83.

ją z wyliczoną wartością tejże funkcji z otrzymanej wiadomości. Jeśli obie wartości się zgadzają, to przyjmuje się, że wiadomość została podpisana poprawnie[53].

Jak dotąd nie są znane przypadki odszyfrowania informacji zakodowanych współczesnymi (1024-bitowymi i dłuższymi) kluczami asymetrycznymi bez znajomości odpowiednich kluczy prywatnych. Świadczy to o skuteczności algorytmu RSA w zabezpieczaniu poufnych informacji cyfrowych. Wadą takiego szyfrowania jest czas oczekiwania i niska wydajność, ze względu na obróbkę dużych ilości danych[54].

3. Szyfrowanie hybrydowe

Ze względu bezpieczeństwa i wydajności często są stosowane techniki hybrydowe, które łączy metodę symetryczną z metodą klucza publicznego. W takim wypadku wiadomość jest szyfrowana kluczem publicznym, a przekazanie wiadomości odbywa się przy pomocy szyfrowania asymetrycznego. Techniki hybrydowe najczęściej są używane dla zabezpieczenia poczty elektronicznej (PEN – Privacy Enhanced Mail, PGP – Pretty Good Privacy), również w protokołach WWW (SSL, PCT, S-http). Szyfrowanie hybrydowe likwiduje wady szyfrowania symetrycznego i asymetrycznego, równocześnie przejmując ich zalety[55].

2.5.2. Podpis cyfrowy

Jak już wspomniano, kryptografia z kluczem publicznym, z użyciem pary kluczy (publicznego i prywatnego) stanowi dogodną podstawę technologiczną do wprowadzenia podpisów cyfrowych. Na przykład osoba X zaszyfruje wiadomość, używając własnego klucza prywatnego, a osoba Y jest w stanie rozszyfrować wiadomość za pomocą klucza publicznego od X, to Y może być niemal pewien, że wiadomość pochodzi od X. Ale w przypadku, kiedy wiadomość uprawnia osobę Y do wykonania pewnej czynności (na przykład, pobranie pewnej sumy z konta bankowego X) fakt, że wiadomość została wysłana przez X daje podobny poziom zaufania, jakby w przypadku, gdyby X podpisał własnoręcznie omówiony dokument.

Opisana technika nie jest wygodna w przypadku, kiedy podpis stanowi zaszyfrowaną wersję całej wiadomości, która może być bardzo długa. Ale zazwyczaj szyfrowaniu podlega tylko skrót komunikatu, a nie cała wiadomość.

---

[53] B.Schneier, *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C,* Warszawa, Wydawnictwa Naukowo-Techniczne, 2002, s. 572-581.
[54] *Systemy e-commerce. Technologie internetowe w biznesie.* Praca zbiorowa pod redakcją Celiny M.Olszak, Katowice, 2004, s.237.
[55] Ibidem, s.237-238.

Skrót ten tworzy się przepuszczając cały komunikat przez funkcję jednokierunkową, która ma następujące właściwości.

1. łatwo przekształca test oryginalny na skrót, natomiast niemożliwym jest odtworzenie oryginalnego komunikatu na podstawie jego skrótu.
2. skrót ma standardową długość, niezależnie od rozmiaru oryginalnego komunikatu.
3. każdy symbol autentycznego komunikatu jest znaczący dla zrobienia skrótu, dlatego że zmiana pojedynczego znaku w oryginalnej wiadomości przywodzi do kreowania innego skrótu.
4. funkcja skrótu jest dostatecznie skomplikowana, żeby nawet przy wielokrotnych zmianach oryginalnego tekstu było niemożliwe odzyskanie skrótu.

Ostatnia charakterystyka jest bardzo ważna, ponieważ pozwala na uniemożliwienie nieuprawnionych zmian oryginału.

Algorytm, który jest najczęściej używany do tworzenia podpisu cyfrowego – to algorytm SET. Ten algorytm tworzy skróty długością 20 bajtów, bez zależności ile wynosi autentyczny komunikat. Algorytm również załatwia wymogi jednokierunkowości dla uzyskania 20-bitowego skrótu i odrzucenia dużej części komunikatu, co także pozwala na odnalezienie treści oryginalnej po odczytaniu skrótu.

Kroki modelu algorytmu są następujące:

1. X tworzy wiadomość do przesyłania.
2. X za pomocą programu tworzy 20-bajtowy skrót swojej wiadomości.
3. X szyfruje skrót za pomocą swojego klucza prywatnego i tym samym podpisuje wiadomość cyfrowo.
4. X przesyła podpisaną wiadomość do Y.
5. Y, otrzymawszy wiadomość również generuje jej skrót..
6. Y rozszyfrowuje podpis stosując publiczny klucz X.
7. Y porównuje rozszyfrowany podpis ze swoim lokalnie wygenerowanym skrótem.

Gdy oba teksty są takie same, to Y może mieć pewność, że otrzymana wiadomość była podpisana przez X i nikt inny nie dokonał zmian[56].

[56] A.Wawszczyk, E-gospodarka, Poradnik przedsiębiorcy, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003, s.86-88.

2.6. Metody bezpieczeństwa w systemie handlu elektronicznego

Istnieje wiele możliwych technologii, które mogą przeszkadzać zagrożeniom. W tym rozdziale omówione zostaną sposoby zabezpieczenia, dotyczące systemu handlu elektronicznego bezpośrednio.

2.6.1. Zabezpieczona informacja o systemie

Każda informacja o systemie elektronicznym może być przydatna osobie planującej atak. Szczególnie informacja o:

1. Systemie operacyjnym (rodzaj, wersja, zainstalowane programy),
2. Bazie usług (rodzaj i wersja),
3. Kodzie aplikacji, zabezpieczonych częściach aplikacji,
4. Konfiguracji i zabezpieczeniach systemu.

Znajomość wersji oprogramowania pozwoli cyberprzestępcy znaleźć luki w bezpieczeństwie przez na przykład bazę CVE[57], szczególnie w nowych systemach. Wiedza o rodzaju bazy danych pomoże zastosować atak na kod SQL lub specyficzny atak w zależności od bazy danych (PostgreSQL, MySQL). Na przykład łatwy sposób przy takim rodzaju linku www.strona.com/gallery.php?id=1, który zawiera dane o SQL wpisać na końcu znak apostrofu i w wyniku otrzymamy informację o błędach, wersji bazy danych, funkcjach PHP i czasami nawet o systemie plików. Po wpisaniu niepoprawnego posilania otrzymamy informację o tym, że strona nie została znaleziona i czasami wersję Apache.

Sposób ochrony takich informacji polega na dwóch ścieżkach:

1. Poważne zabezpieczenie plików, mających te informacje i stworzenie pułapek przy ataku. W plikach z informacją wpisać fałszywe odniesienia, żeby wprowadzić przestępcę w błąd.
2. Ukryć parametry kategorii, subkategorii podstron występujące w adresie URL jak i odniesienia do aplikacji i baz danych[58].

2.6.2. Zapasowe kopie danych

Bezpowrotne zagubienie danych jest jedną z krytycznych rzeczy, które mogą zdarzyć się firmie. W niektórych wypadkach może to przywieść nawet do bankructwa firmy. Sprzęt można kupić, a dane niestety nie. Ale problem jest w tym, że o zapasowych kopiach danych wspomina się tylko, kiedy utrata danych już się dokonała.

---

[57] *Baza CVE,* www.cve.mitr.org [dostęp 15.07.2014]

[58] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.62.

Systematyczny i udany proces wykonywania kopii zapasowych oraz testowania poprawności ich zapisu pozwala zmniejszyć ryzyko bezpowrotnej utraty danych.

W jakich sytuacjach może się przydać kopia danych? W każdej, ale szczególnie przy:

1. Awarii sprzętu (między innym nośniki danych, dyski twarde).
2. Utracie danych przez wypadkowe działania pracownika.
3. Sabotażu, czyli utracie danych w wyniku celowego działania pracownika lub osoby obcej.
4. Działaniu oprogramowania złośliwego, których celami mogą być usunięcie, zmiana, zaszyfrowanie danych albo naznaczenie braku uprawnień dla odczytu.
5. Atakach hakerów.
6. Kradzieży sprzętu lub nośników danych.

Dlatego należy robić zapasowe kopie danych biznesowych. Są to bazy danych, pliki, katalogi serwisu handlu elektronicznego. Przy hostingu zajmujemy się tym hostingodawca, ale jeżeli serwery znajdują się w firmie, to odpowiedzialność leży na administratorach. Przy zarządzaniu całym systemem należy również robić kopie zapasowe konfiguracji aplikacji, bazy danych, operacyjnych systemów, urządzeń sieciowych.

Częstość wykonania zapasowych kopii zależy od specyfiki systemu. Jeżeli serwis jest mało aktywny, to wystarczy zrobić backup raz w tygodniu, przy aktywnych serwisach należy robić kopie codziennie, a w niektórych wypadkach co wyznaczoną ilość godzin.

Kopia zapasowa może być nic nie warta, jeżeli była zapisana niepoprawnie. Dlatego okresowo należy sprawdzać czy zapisane wszystkie dane i czy mogą one być otworzone. Trzeba wziąć pod uwagę, że kopię zapasową trzeba przechowywać poza firmą i w odpowiednich warunkach. Trzeba rozumieć, że backup jest także cenny, jak i system e-commerce, dlatego poziom bezpieczeństwa powinien być nie niższy niż dla systemu e-commerce.

Hasła do systemu e-commerce muszą być zapisane i przechowywane. Najlepiej robić to w sposób elektroniczny, a nie tradycyjny (w notesie, karteczkach). Korzyści z zapisywania i przechowywania haseł w sejfie elektronicznym są znaczne. Elektroniczny sejf przedstawia sobą zaszyfrowany plik z hasłami (na przykład, program KeePass). Możemy w nim tworzyć unikalne, złożone hasła dla każdego elementu serwisu i nie martwić o ich zapomnienie. Ale nie wolno zapominać o wykonaniu kopi zapasowych sejfu i przechowywania ich w

bezpiecznym miejscu. Plik z hasłami również musi być zabezpieczony hasłem i przechowywany poza serwerem, na którym znajduje się system lub aplikacja[59].

2.6.3. Bezpieczny hosting

Przy tworzeniu serwisu handlu elektronicznego powstaje dylemat czy zainstalować własny serwer, czy skorzystać z usług firmy hostingowej. Każde z tych rozwiązań ma swoje wady i zalety. Główną zaletą własnego serwisu jest pełna swoboda w jego konfiguracji. Z innej strony ta właściwość to wada, ponieważ właściciel systemu musi samodzielnie zadbać o bezpieczeństwio systemu, ale niestety nie wszyscy mają o tym pojęcia. Oprócz bezpieczeństwa należy zadbać o dostępności serwisu, brak przerw w działaniu i regularnym serwisowaniu. Przy korzystaniu z usług hostingodawcy powyżej zaznaczone rzeczy będą zagwarantowane, ale właściciel nie ma pełnej władzy. Większość małych i średnich serwisów e-commerce korzysta z hostingu, ponieważ ta opcja jest łatwa, wygodna, a czasami i najtańsza.

W przypadku hostingu warto pamiętać o bezpieczeństwie. Właściciel serwisu otrzymuję dostęp do paneli administracyjnych (DirectAdmin). Należy zabezpieczać loginy i hasła od tych paneli, nie zapisywać ich w przeglądarce, nie wpisywać na cudzych komputerach i przy niezabezpieczonym połączeniu internetowym. Hasło do każdego panelu powinno być różne i przechowywane w różnych miejscach. Warto zauważyć, że jeśli dostęp do paneli administracyjnych nie jest chroniony we właściwy sposób, to bezpieczeństwo całego systemu e-commerce może być poważnie zagrożone.

Dodatkowo trzeba wiedzieć o sposobie wgrywania plików na serwer. Najbardziej popularny protokół dla tego – to FTP, który przesyła dane otwartym tekstem, co może powodować odczyt informacji, podmianę plików itd. Dla ochrony danych należy korzystać z szyfrowanych protokołów, a jeżeli takiej opcji nie ma to wgrywać pliki przez panel administracyjny i szyfrować dane (SSL)[60].

2.6.4. Ochrona domeny internetowej

Domena internetowa to pośredni element systemu e-commerce, ale bezpieczeństwo domeny ma poważny wpływ na funkcjonowanie serwera i na jego dostępność dla klientów.

[59] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.82-88.

[60] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.89-92.

Domena internetowa to część adresu DNS (ang. Domain name system) i jest wykorzystywana do oznaczenia komputerów w Internecie. Na przykład amazon.com, ebay.com – to domeny.

Domena niechroniona jest przed kradzieżą, czyli zmianę właściciela i zmiany delegowania serwera nazw, który obsługuje daną domenę. Przy kradzieży można domenę odzyskać, ale kradzież przede wszystkim spowoduje wiele problemów, takich jak niedostępność systemu w Internecie, brak dostępu do systemu itd. Niestety ryzyko przejęcia domeny jest duże, ponieważ wystarczy napisać list lub wysłać faks do podmiotu, rejestrującego domenę. Zmiana delegowania domeny jest bardzo niebezpieczna, ponieważ może powodować przekierowanie użytkowników z prawdziwego serwera na inny. W handlu internetowym przejęcie domeny lub nieuprawniona jej zmiana może mieć bardziej negatywne wyniki, niż włamanie do systemu.

W celu zabezpieczenia domeny należy korzystać z usługi VID[61] (ang. Very important domain), która polega na identyfikacji osoby, wnioskującej o zmianę[62].

2.6.5. Bezpieczeństwo serwera WWW

Na bezpieczeństwo aplikacji internetowej w większej mierze wpływa bezpośrednio bezpieczeństwo serwera WWW, a na nie inne czynniki, takie jak: bezpieczeństwo fizyczne serwera, zabezpieczenie hosta, konfiguracja serwera WWW i zarządzanie płatnościami. Nie możemy mówić o bezpieczeństwie aplikacji internetowej, jeżeli nie weźmiemy pod uwagę następujące czynniki:

1. Zabezpieczenie hosta. Ochronę urządzenia („hosta”), na którym działa serwer WWW należy rozpoczynać od hardeningu (hartowania). Hardening polega na zwiększaniu odporności systemu na ataki. W przebiegu hartowania są zmieniane wszystkie pośrednie hasła i ustawienia, blokowane nieaktualne konta, instalowane polepszenia zabezpieczeń, usuwane jest niewłaściwe programowanie, wyłączane niepotrzebnej usługi i modułu, zamykane otwarte porty i włączane pomocnicze systemy bezpieczeństwa (na przykład firewall). Na serwerze działa tylko to, co jest konieczne. Najlepsze praktyki w hartowaniu to NSA, NIST czy CIS.
2. Firewall. Firewall to ważny element zabezpieczenia serwera WWW. Przy działaniu pozwala izolować serwer od nieproszonych połączeń z Internetu i izolować od sieci lokalnej. Serwer polega umieszczeniu w strefie izolacyjnej, która jest tak zwanym „przedpokojem”

[61] *Usługa VID*, www.nask.pl/files/p/Very_Important_Domains.pdf [dostęp 15.07.2014]
[62] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.92-95.

sieci komputerowej. W tej strefie są usługi, które musza być widoczne dla gości: serwer WWW, serwer z bazami danych, system e-mail oraz DNS.

Przy konfiguracji serwera WWW, który będzie dostępny z Internetu, należy kierować się podstawową zasadą, że co nie jest dozwolone, jest zabronione i trzeba zakazywać wszystko, dozwalając tylko to, co jest niezbędne.

3. Aktualizacje aplikacji. Dla dotrzymania wysokiego poziomu bezpieczeństwa należy na czas usuwać i naprawiać błędy, usterki w oprogramowaniu. Dlatego należy śledzić strony, które umieszczają takie informacje, między innym CVE, VUPEN i dokonywać potrzebne aktualizacje. Inny sposób skorzystania z nienadzorowanych aktualizacjach bezpieczeństwa, które są wykonane za pomocą mechanizmu unattended-upgrades. Ten sposób pozwała na automatyczne i bez ingerencji administratora systemu instalowanie poprawek.

4. Konfiguracja serwera. Jak było już zaznaczone, informacja o serwerze może umożliwić atak. Dlatego należy wyłączyć informację o serwerze, która zwykłe się pojawia przy generacji stron błędów i listowania katalogów FTP.

5. Chrootowanie. Dobrym sposobem na wzmacnianie bezpieczeństwa serwera WWW będzie chrootowanie go. Chrootowanie to ograniczenie procesom serwera dostępu do systemu plików przez wydzielenie nowego przypisywanego zestawienia plików. Taka konfiguracja pozwoli na blokowanie analizy atakowanego systemu. Są dwa sposoby na chrootowanie: manualne stworzenie dedykowanego środowiska lub zautomatyzowanego wykonanie (na przykład, przez moduł mod_security).

6. Zabezpieczanie plików konfiguracyjnych. Zabezpieczanie plików konfiguracji systemu przed możliwością ich zmiany jest dobrą praktyką bezpieczeństwa serwera WWW. Nie jest to rozwiązanie doskonałe, ponieważ przy otrzymaniu uprawień root, można to zabezpieczenie wyłączyć, ale w wielu wypadkach takie zabezpieczenie chroni modyfikacje konfiguracji. Istnieje pakiet TripWire, który pozwała na odwzorowanie systemu plików i dopisaniu do nich cyfrowych sygnatur. Nie jest to zabezpieczenie przed atakiem, ale pozwała zlokalizować plik lub folder, gdzie zmiany były wykonane.

7. Ochrona przed atakami DOS. Jednym z podstawowych sposobów do zabezpieczenia serwerów WWW przed atakami DOS (ang. denial of service) jest program Fail2Ban. Ten program pozwała zauważać szkodliwe działania i zakazywać jakiekolwiek aktywności z danego IP-adresu na czas określony lub na stale. Między innym program skutecznie chroni przed skanowaniu serwera botami sieciowymi. Dla małych i średnich firm e-commerce

Fail2Ban jest dobrym sposobem, ponieważ nie daje wielkiego obciążenia serwera. Ale w wielkich przedsiębiorstwach e-commerce trzeba używać innych narzędzi[63].

2.6.6. Bezpieczeństwo baz danych

Dane aplikacji e-commerce są zwykle przechowywane w bazach danych. Teoretycznie tworzenie bazy danych powinno być na innym serwerze niż system e-commerce, ale w praktyce mamy do czynienia z tym, że system e-commerce i baza danych są na jednym serwerze. Dla zabezpieczenia bazy danych na serwerze należy przy instalacji bazy danych usunąć konta anonimowe i bazę testową, które tworzą się automatycznie. Warto również zadbać

o odpowiednie ustawienia w pliku konfiguracyjnym bazy danych.

1. Eksport i import danych. Przy użyciu hostingu właściciel bądź administrator serwera będzie używał myPHPAdmin jako narzędzia zarządzania bazą danych przez przeglądarkę.

Również jest opcja eksportu całej bazy danych do pliku. Należy to robić w celu stworzenia kopii zapasowych, ale trzeba zadbać o bezpieczeństwo pliku, ponieważ nie jest on chroniony.

2. Połączenie z bazą. Każde połączenie z bazą danych powinno odbywać się przez dodanie głównego pliku, który inicjuje połączenie z bazą (na przykład, polacz.php). Ten plik musi być we właściwy sposób zabezpieczony. Uprawienia do tego pliku powinny być nadane tylko administratorowi, właścicielowi i serwerowi.

3. Szyfrowanie danych. Szyfrowanie wszystkich informacji, które znajdują się w bazie danych nie znajduje kompromisu pomiędzy wydajnością serwera oraz jego bezpieczeństwem. Przed procesem szyfrowania trzeba określić, jakie dane należy szyfrować, ponieważ szyfrowanie całej ilości plików przywodzi do znacznego obciążenia systemu.

4. Przechowywanie danych. Po jakimś czasie informacja gromadzona w bazach danych przestaje być aktualna i stałe gromadzenie takich danych obciąża system i obniża wydajność samej bazy danych. Można rozwiązać problem usunięciem nieaktualnych plików, lub stworzeniem drugiej bazy danych, na którą będą przeniesione pliki nieaktualne z systemu e-commerce[64].

[63] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.97-123.

[64] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.125-132.

2.6.7. Bezpieczna transmisja danych

Bezpieczeństwo transmisji danych składa się na integralności i poufności danych. Integralność polega na staraniach, żeby nikt nie zmienił danych przy przebiegu transmisji, a poufność ma na celu zachowanie transmitowanych informacji w tajemnicy. Głównym elementem bezpiecznej transmisji danych jest szyfrowanie. Szyfrowanie to metoda zapisu jawnej treści w taki sposób, żeby stała ona nieczytelna dla wszystkich oprócz nadawcy i odbiorcy. Szczegółowo szyfrowanie zostało opisane w rozdziale 2.5.1. Teraz skupimy się na osobliwościach szyfrowania przy prowadzeniu handlu elektronicznego.

Serwis e-commerce przy uruchomieniu szyfrowanego przepływu danych SSL pomiędzy nim a użytkownikiem będzie używał: kryptografii asymetrycznej w celu wymiany kluczy do szyfrowania symetrycznego, kryptografii symetrycznej w celu wymiany informacji, kodów uwierzytelniania wiadomości dla zachowania gwarancji, że nikt nie zamieni przesyłanych wiadomości.

Szyfrowanie ma na celu zapobiegania podsłuchaniu transmisji, nieuprawnionej zmianie treści wiadomości. Szyfrowanie jest również wymagane przez prawo, należy go używać, żeby chronić dane osobowe w Internecie. Szyfrowanie ma miejsce i w takich procesach, jak zdalne administrowanie portalem, dodanie plików do systemu, komunikacja między serwerami. Należy traktować szyfrowanie w systemach e-handlu, jako inwestycje w reputacje i zaufanie serwerów przez użytkowników.

1. Szyfrowanie informacji webowej. Przy otwieraniu strony internetowej przez przeglądarkę jest wysyłane żądanie strony i jej otrzymanie. Ale dla szyfrowania jest potrzebne wcześniejsza wymiana kluczami. Dlatego SSL stosuje szyfrowanie asymetryczne, przy którym przeglądarka prosi serwer o wysyłaniu klucza publicznego, przy otrzymaniu klucza szyfruje dane, i przesyła je do serwera. Serwer ze swojej strony odszyfrowuje dane i obie strony mają możliwość przełączenia na szyfrowanie symetryczne.
2. Instalacja SSL. Dla szyfrowania danych na serwerze jest niezbędne zainstalowanie aplikacji, która pozwała na wykorzystanie protokołu SSL (na przykład, OpenSSL).
3. Generowanie klucza i pliku żądania. Po instalacji SSL należy w pierwszej kolejności wygenerować klucz prywatny. Po tym trzeba zrobić jego kopię zapasową, ponieważ bez tego klucza nie jest możliwe używanie certyfikatu SSL. Za pomocą wygenerowanego klucza tworzymy plik żądania certyfikatu (CSR – ang. Certyficate signing request). Plik CSR jest zwykłym plikiem tekstowym, po generacji musimy go podpisać. Podpisać certyfikat można na dwa sposoby: przez samodzielne podpisanie certyfikatu lub przy pomocy centrum

certyfikacyjnego (VeriSign, Thawte). Niezależnie od wybranego sposobu podpisu transmisja będzie szyfrowana. Certyfikat podpisany przez centrum certyfikacyjny ma większe korzyści dla systemu e-commerce, między innym tworzy lepszy wizerunek firmy w oczach użytkownika, ponieważ przeglądarka zawsze będzie weryfikować tę stronę jak z połączeniem SSL i witryna będzie bardziej odporna na fałszowanie. Zaufany certyfikat jest niezbędny dla przedsiębiorstw, dbających o reputację firmy, marki, serwisu, wielkiej ilości klientów, przy biznesie z relacjami B2C lub C2C.

4. Komunikacja przez pocztę elektroniczną. W systemie handlu elektronicznego jest niezbędna komunikacja z klientem przez e-mail. Mogą być wysyłane różne wiadomości, jak dane do rejestracji, szczegóły zamówienia i opłaty. Są to informacje poufne, czyli również powinny być zabezpieczone i szyfrowane. Dobrym przykładem zabezpieczenia informacji, przesyłanej przez serwery pocztowe, jest umieszczenie jej w załączniku w postaci zabezpieczonego hasłem pliku PDF. Hasło może być takie same jak i przy logowaniu do systemu, lub inne[65].

2.6.8. Bezpieczne sesje

Jeżeli mówimy o sesjach internetowych, to pierwszym podstawowym pojęciem będą cookies. Cookies służą dla przechowywania informacji o sesji, jak również i przechowywania informacji o użytkownikowi. Dane w cookies są chronione w formacie tekstowym i mieszczą następującą informacje: nazwa i skojarzona z nią wartość, okres ważności cookie, domena, ewentualnie atrybut bezpieczny. Sesje można realizować i w inny sposoby, jak na przykład przez przekazywanie identyfikatora sesji w adresie URL lub przez ukrycie pola formularza.

Należy zwrócić uwagę, że pliki cookies są przesyłane za pomocą tego samego protokołu, co i strona, na której są dostępne. Bezpieczeństwo danych, które są zapisywane, zależą od bezpieczeństwa komputera, na którym są one przechowywane. Dlatego nie trzeba zapisywać w tych plikach ważnych informacje.

1. Sesje w aplikacji. Istotnym problemem systemu e-commerce jest to, że HTTP jest protokołem bezstanowym i nie ma pojęcie sesji, czyli każde odwołanie do serwera jest uznawane za nową sesję. Ale proces komunikacji systemu e-commerce z użytkownikiem ma wiele odwołań. Sesja przedstawia sobą proces, przy którym strony otwierane przez danego użytkownika muszą być połączone. Jeżeli ten proces zostanie przerwany, to użytkownik będzie zmuszony rozpocząć proces od nowa. Dlatego, że protokół HTTP nie potrafi stworzyć,

[65] L.Kępa, P.Tomasik, S.Dobrzyński, Bezpieczeństwo systemu e-commerce, Helion 2012, s.133-163.

przetrwać i zakończyć sesji, muszą te rozwiązania być zainstalowane w samej aplikacji systemu e-handlu.

2. Identyfikator sesji w cookies. Identyfikatory sesji mogą być przesyłane przez URL, przez formularze ukryte lub przez cookies. Użytkownik, przekazując URL komuś, może również udostępnić i identyfikator sesji, który może być cenną zdobyczą dla cyberprzestępcy. Dlatego, pierwsza metoda nie jest rekomendowana. Najlepszym rozwiązaniem są sesje, które bazują na cookies. Informacja o takich sesjach jest trwała i nawet po zamknięciu przeglądarki pozostaje. Ochrona przez atakami na sesje składa się z następujących działań:

   a. Kontrola z czasem trwania sesji (na przykład zamknięcie sesji po jakimś czasie nieaktywności).
   b. Unikanie długotrwałych sesji.
   c. Zastosowanie jakościowego i silnego algorytmu tworzenia identyfikatora sesji, żeby zminimalizować ryzyko odgadnięcia.
   d. Brak przyjmowania innych identyfikatorów, niestworzonych systemem.
   e. Zmiana identyfikatora sesji po jakimś czasie.
   f. Konieczne wymaganie autentyfikacji użytkownika przy krytycznych operacjach.
   g. Przechowywanie identyfikatorów sesji w bazie danych zamiast w systemie plików[66].

Podsumowując, dla bezpiecznego prowadzenia handlu w Internecie należy dbać najpierw o bezpieczeństwo technologiczne. Istnieje wielu zagrożeń dla systemu e-handlu, ale należy uważać, że nie jest możliwym zabezpieczyć się przede wszystkim. Dlatego należy przeanalizować ryzyko i wyznaczyć priorytety bezpieczeństwa. Klasycznymi podejściami bezpieczeństwa internetowego są szyfrowanie i podpis elektroniczny. Ale handel elektroniczny ma swoją specyfikę i należy również stosować specjalne metody bezpieczeństwa, takie jak ochrona domeny internetowej, ochrona bazy danych, wybór bezpiecznego hostingu, ochrona serwera www i td. Stosowanie takich technik bezpieczeństwa pozwoli zwiększyć odporność systemu handlu elektronicznego przed zagrożeniami.

[66] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.185-196.

Rozdział 3
Bezpieczeństwo prawne handlu elektronicznego

Wirtualizacja życia gospodarczego doprowadziła do stworzenia zestawu nowych regulacji prawnych dotyczących praktycznych mechanizmów, umożliwiających prowadzenie działalności handlowych w Internecie, związanych z zawieraniem transakcji drogą elektroniczną. Elektroniczna konwersja danych również sprawia masowe problemy prawne ze względu na redukcję dokumentów papierowych i zamianą ich komunikatów przekazywanych i przechowywanych w formie elektronicznej.

Poniższy fragment pracy ma na celu wyjaśnić kluczowe zagadnienia prawne powiązane z handlem elektronicznym i ustawy prawne, co do bezpieczeństwa prawnego w Internecie.

3.1. Generalne inicjatywy międzynarodowe, dotyczące handlu elektronicznego

W opracowaniu ram prawnych handlu elektronicznego biorą udział liczne instytucje międzynarodowe. Najważniejsze z nich to:

1. Unia Europejska,
2. Organizacja Współpracy Gospodarczej i Rozwoju (OECD),
3. Organizacja Narodów Zjednoczonych (ONZ).

3.1.1. Regulacje Unii Europejskiej

Normowanie europejskie zaczął zaprezentowany w czerwcu 1994 r. Raport Bangemanna „Europa a globalne społeczeństwa informatyczne".

W kwietniu 1997 r. odsłonił się komunikat Komisji Europejskiej nazwany „Inicjatywa europejska w gospodarce elektronicznej". W nim zostały opracowane zagadnienia dotyczące: liberalizacji rynku informatycznego, ustanowienie ram prawnych i procedur administracyjnych oraz stworzenia otwartego i konkurencyjnego otoczenia gospodarczego, wspierającego rozwój rynku elektronicznego w Europie[67].

[67] *Oficjalny portal Unii Europejskiej*, http://www.europa.eu.int/information_society/eerope/index_en.htm [dostęp 10.10.2014]

Ten dokument określa działalność UE w zakresie technologii, regulacji i wspierania działań gospodarczych w handlu elektronicznym. Istnieje niezwłoczna potrzeba stworzenia na poziomie UE stałych granic prawnych dla działania handlu elektronicznego w celu uniknięcia konfliktowości poszczególnych krajowych regulacji, które mogą utrudniać dalszy rozwój.

Normy prawne powinny odnosić się do każdego elementu działalności gospodarczej począwszy od zakładania działalności w Internecie poprzez promocje i podpisanie umów, a kończąc płatnościami elektronicznymi, zasadami zwrotu towaru, wystawienia faktur. Z innej strony powinny one uwzględniać handel elektroniczny jak całość ze względu na zapewnienie bezpieczeństwa danych, ochronę własności intelektualnej, ochronę konsumenta, jego prywatności i budowę neutralnego otoczenia podatkowego.

Formowanie zaufania wśród przedsiębiorstw i klientów musze opierać się na implementacji bezpiecznych technologii, m.in. podpis cyfrowy, certyfikaty bezpieczeństwa i stworzenia prawnych i instytucjonalnych granic wspierających te technologie.

Kolejny ważny międzynarodowy akt prawny w zakresie bezpieczeństwa internetowego - to Dyrektywa 2000/31/EC Parlamentu Europejskiego i Rady Europy. Dyrektywa akceptuje niektóre kwestie prawne, związane z usługami społeczności informacyjnej, a przede wszystkim handlem elektronicznym na Wspólnym Rynku z dnia 8 czerwca 2000 r[68]. Ten akt prawny odnosi się przede wszystkim do dziedzin związanych z elektronicznym handlem:

1. Określanie krajowych przepisów dotyczących usług społeczeństwa informacyjnego na wspólnym rynku.

2. Ustalenie siedziby dostawców usług, informacji handlowej – reklamy i marketingu, umów elektronicznych, odpowiedzialności pośredników.

3. Określenie zasad postępowania w sądowym i pozasądowym rozwiązywaniu sporów.

Dyrektywa odnosi się do wszystkich umów mających za swój przedmiot tzw. usługi społeczeństwa informacyjnego, a wszelkie usługi, odpłatne i nieświadczone na odległość, bez równoczesnej obecności stron umowy, przy użyciu środków internetowych służących Normowaniu europejskiemu został zaprezentowany w czerwcu 1994 r. Raport Bangemanna „Europa a globalne społeczeństwa informatyczne".

[68] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (Directive on electronic commerce), Official Journal L 178, 17/07/2000 p. 0001-0016.

Dyrektywa odnosi się do wszystkich umów mających za swój przedmiot tzw. usługi społeczeństwa informacyjnego, a same wszelkie usługi, odpłatne i nieświadczone na odległość, bez równoczesnej obecności stron umowy, przy użyciu środków internetowych służących przetwarzaniu danych oraz składowaniu danych, na indywidualne wymaganie konsumenta. Kraje członkowskie UE zostały obowiązane do szczególnego przeglądu swej legislacji

i dokonania w niej koniecznych zmian w celu stworzenia zasad prawnych dla swobodnego rozwoju gospodarki elektronicznej w kraju. Kluczową zasadą jest umożliwienie zawierania prawnie powiązanych umów przy zastosowaniu zasobów elektronicznych[69].

3.1.2. Deklaracja OECD

W październiku 1998 r. w Ottawie odbyła się konferencja OECD, na której była przyjęta deklaracja, aktywizująca rozwój globalnej gospodarki elektronicznej.

Najważniejsze zagadnienia deklaracji to m.in.:

1.Rządy powinny wspierać konkurencję w gospodarce elektronicznej oraz redukować lub eliminować niepotrzebne ograniczenia jej rozwoju.

2. Akceptowane przez rządy zasoby interwencyjne powinny być proporcjonalne, zdecydowane, konsekwentne i przewidziane, a także być neutralne technologiczne.

3. Przedsiębiorcy odgrywają rolę centralną w rozpatrywaniu i implementacji rozwiązań dla istniejących trudnych sytuacji w gospodarce elektronicznej i powinny współpracować bezpośrednio z rządami.

4. Koniunktura gospodarki elektronicznej zależy od osiągnięcia powszechnego dostępu do infrastruktury informatycznej.

5. Skuteczna konkurencja na rynkach informatycznych powinna zapewniać obniżkę kosztów przy strategicznym działaniu, poprawę jakości i rozszerzenie dostępu do infrastruktury informatycznej[70].

[69] A.Wawszczyk, *E-gospodarka, Poradnik przedsiębiorcy*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003, s.12.
[70] B.Gregor, M.Stawiszyński, *E-commerce,* Bydgość 2002, s.293.

3.1.3. Modelowe prawo o handlu elektronicznym ONZ

Agencja Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego (UNCITRAL) sformułowała tekst Jednolitego Prawa Elektronicznego Przesyłania Danych (EDI). Ta ustawa prezentuje sobą wzorzec, na którym powinny opierać się w swoich normach prawnych państwa należące do ONZ (i inne zainteresowane kraje).

Ustawa była przyjęta w czerwcu 1996 r. i została zatwierdzona Zgromadzeniem Ogólnym ONZ. Postanowienie obejmuje zestaw uznawanych powszechnie reguł i zasad, które pozwalają na usunięcie barier prawnych, powiązanych z tradycyjnym uregulowaniem handlu dokumentami papierowymi.

Jest to dokument, służący jako punkt odniesienia dla wielu szczegółowych regulacji przyjmowanych tak w organizacjach międzynarodowych, jak i na poziomie lokalnym. Ważny akcent w dokumencie skierowany na rozwój międzynarodowego handlu elektronicznego. W tej ustawie, jak i we wszystkich podobnych dokumentach organizacji międzynarodowych, podchodzi się do handlu elektronicznego, jako do zjawiska ogarniającego ogromne zagadnienie ze sfery międzynarodowego obrotu towarowego[71].

3.2. Wybrane międzynarodowe prawne rozwiązania, dotyczące handlu elektronicznego

W tej części omówimy niektóre rozwiązania prawne, które dotyczą handlu elektronicznego. Szczególnie zwrócimy uwagę na normy prawne, dotyczące opodatkowania i cła, podpisów elektronicznych, ochrony konsumentów, danych osobowych i własności intelektualnej.

3.2.1. Rozwiązania prawne, dotyczące opodatkowania i cła

Generalne postulaty stosujące opodatkowania i cła są bardzo podobne w dokumentach OECD oraz Unii Europejskiej. Odnoszą się do nich:

1. Neutralność. Opodatkowanie powinno być sprawiedliwe i równoległe pomiędzy handlem elektronicznym a tradycyjnym handlem, żeby zapobiec podwójnemu opodatkowaniu lub nieumyślnego braku opodatkowania.
2. Skuteczność. Polega na tym, żeby koszty płacenia podatków były zminimalizowane.
3. Prostota. Reguły opodatkowania powinny być jasne i proste do zrozumienia;

[71] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warszawa, 2004, s.64.

4. Racjonalność. Opodatkowanie musi być właściwe wysokie w odpowiednim czasie, a potencjalne zagrożenia w postaci uchylania się od płacenia podatków musi być zminimalizowane.

5. Elastyczność. Systemy opodatkowania powinny być elastyczne, dynamiczne i być na czasie za rozwojem technologicznym i handlowym.

W przypadku podatków i ceł w umowach gospodarki elektronicznej praktyczna realizacja teoretycznych zasad nie jest łatwą sprawą. Składają się na to następujące czynniki:

1. Trudność identyfikacji podmiotów dokonujących transakcji.
2. Trudność ustalenia lokalizacji podmiotu.
3. Trudność w dostępie do dokumentów umożliwiających wymierzenie podatku w stosunku do podmiotów znajdujących się poza jurysdykcją organów podatkowych.

Z powodów wymienionych powyżej w krajach rozwiniętych zaczyna dominować pogląd, że należy całkowicie zwolnić z cła towary dostarczane drogą elektroniczną. Rezygnacja z oclenia doprowadzi do szybkiego rozwoju globalnego handlu elektronicznego oraz nada relacjom handlowym w sieci bardziej stabilny i przewidywalny charakter[72].

3.2.2. Rozwiązania dotyczące podpisów elektronicznych

W 1999 r. była przyjęta Dyrektywa Parlamentu Europejskiego i Rady w sprawie podpisu elektronicznego. Aby umożliwić wykonanie czynności prawnych, dla których wymagana jest forma pisemna, niezbędne staje się wprowadzenie takich instrumentów prawnych, które pełniłyby funkcje analogiczne do podpisu własnoręcznego. Zgodnie z art. 5, ust. 1 wyżej wspomnianej dyrektywy „państwa członkowskie mają zapewnić takie warunki, aby zaawansowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i złożony przy pomocy właściwego, bezpiecznego urządzenia spełniał, w odniesieniu do danych zapisanych w formie elektronicznej, prawne wymagania stawiane podpisom własnoręcznym składanym na papierze oraz aby mógł służyć, jako dowód w procesach prawnych”[73].

3.2.3. Ochrona konsumenta

Polecenia OECD od grudnia 1999 r. zawierają zasady, które rządy krajów członkowskich powinny wprowadzać do przepisów krajowych regulujących zakres stosunków umownych między firmą a konsumentem. Zasady te zobowiązują przedsiębiorców do stosowania odpowiednich praktyk handlowych i marketingowych, sprowadzających się

[72] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warszawa, 2004, s.65-66.
[73] Ibidem, s. 66-68.

w znacznej mierze do stworzenia konsumentowi „komfortu informacyjnego" w procesie transakcyjnym. Chodzi głównie o:

1. Udzielanie konsumentowi pełnych, zrozumianych i łatwo dostępnych informacji na temat oferowanych towarów i usług, warunków umowy, płatności, warunków gwarancji, warunków odstąpienia od umowy.
2. Udzielanie konsumentowi pełnych, zrozumianych i łatwo dostępnych informacji na temat firmy, pozwalających na jej łatwą identyfikację (nazwa przedsiębiorcy, siedziba)[74].

3.2.4. Ochrona prywatności

Łamanie prywatności związane z rozwojem gospodarki elektronicznej i popularnością komunikowania się poprzez sieć Internet dotyczy najczęściej następujących wypadków:

1. Stworzenie profilów osobowościowych bez wiedzy i zgody osób zainteresowanych.
2. Bezprawnego monitoringu korespondencji elektronicznej.
3. Rozpowszechniania nieautoryzowanych informacji.

Zagadnienie ochrony prywatności zostało dostrzeżone przez unijnych prawodawców, czego wynikiem są dwie regulacje:

1. Dyrektywa 95/46/EC o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie takich danych;
2. Dyrektywa 97/66/EC regulująca przetwarzanie danych osobowych oraz ochronę prywatności w sektorze telekomunikacyjnym[75].

3.2.5. Ochrona prawa własności intelektualnej

Gospodarka elektroniczna i związana z nią wirtualizacja produktów tworzą warunki sprzyjające łamaniu praw własności intelektualnej. Wynika to z łatwości przesyłania, przechowywania i rozpowszechniania produktów cyfrowych w sieci Internet.

Dodatkową zasadą sprzyjającą nadużyciom jest fakt, iż w warunkach gospodarki sieciowej staje się bardziej złożonym problem określenia, w którym kraju nastąpiło naruszenie prawa autorskiego. Te problemy spowodowały powstanie koncepcji terytorialnego „prawa cyberprzestrzeni". Obecnie jednak wydaje się, iż sposobem w skutecznej ochronie praw autorskich może być kodowanie. Żeby kodowanie spełniło swoje zadanie, kraje

[74] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warszawa, 2004, s.67.
[75] Ibidem, s.68.

członkowskie WIPO (World Intellectual Property Organization)[76] są zobowiązane do wprowadzenia
w swoich systemach prawnych zakazów następujących działań:

1. Usuwanie urządzeń zabezpieczeń technicznych, które utrudniają eksploatacje wytworów bez pozwolenia.
2. Usuwania oraz modyfikacji informacji identyfikującej na kopiach lub przy udostępnieniu publicznym.
3. Rozpowszechniania utworów w przypadku usunięcia informacji identyfikującej[77].

3.3. Prawo wobec handlu elektronicznego

Dyskutując o problemie bezpieczeństwa handlu elektronicznego, należy zaznaczyć, że bezpieczeństwo systemu to nie tylko bezpieczna aplikacja, bezpieczny serwer, bezpieczne dane, to również bezpieczne funkcjonowanie całego biznesu. Przedsiębiorca, który prowadzi działalność gospodarczą podlega rozmaitym aktom prawnym, które regulują w różne sposoby go biznes. Nieznajomość prawa szkodzi, dlatego prawo warto znać w tym zakresie, w jakim dotyczy ono biznesu. Dlatego bezpieczeństwo systemu handlu elektronicznego składa się także z bezpieczeństwa prawnego.

Prawo nie tylko stawia wymagania, ale chroni biznes przedsiębiorcy. Są przepisy, na podstawie, których cyberprzestępca może ponieść karę za swoje nieuprawnione działania.

Dla handlu elektronicznego obowiązują następujące klasy aktów prawnych:

1. Obrót elektroniczny (reguły handlowania przez Internet).
2. Prawa konsumentów (zawieranie umów drogą internetową).
3. Przetwarzanie danych osobowych (dane osobowe osób fizycznych).
4. Przepisy, które chronią system handlu elektronicznego i informacje w nim.
5. Reguły handlu z zagranicą wskazujące, przepisów których państw należy stosować w danej sytuacji[78] (chodzi o przypadek, gdy konsument jest obywatelem innego państwa, który składa zamówienie za granicą).
6. Przepisy ogólne i specjalistyczne, dotyczące prowadzenia działalności gospodarczej w Internecie.

---

[76] *World Intellectual Property Organization*, http://www.wipo.int/portal/en/index.html, [dostęp 15.11.2015]
[77] M.Niedźwiedziński, *Globalny handel elektroniczny.* Warszawa, 2004, s.69-70.
[78] *Ustawa z dnia 4 lutego 2011 r. prawo prywatne międzynarodowe oraz Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I).*

Przedsiębiorca powinien określić zakres przepisów, które będą dotyczyły go biznesu oraz dowiedzieć i stosować wynikające z nich prawa i obowiązki:

1. Prawa i obowiązki dostawcy (na przykład hostingu, aplikacji).
2. Prawa i obowiązki usługobiorcy, konsumenta, użytkownika systemu (na przykład obowiązki informacyjne).
3. Inne prawa i obowiązki (na przykład dotyczące obowiązków rejestracyjnych).

Akty prawne, które mają największy wpływ na działalność handlu elektronicznego w kraju są następujące:

1. Ustawa o świadczeniu usług drogą elektroniczną.
2. Ustawa o ochronie danych osobowych.
3. Ustawa o ochronie praw konsumenta.
4. Ustawa o warunkach sprzedaży konsumenckiej.
5. Kodeks cywilny.
6. Ustawa o prawie autorskim i ochronie własności intelektualnej.
7. Ustawa o podpisie elektronicznym.

Powyżej wymienione akty prawne są różne w poszczególnych krajach, ale są stworzone na bazie międzynarodowych aktów prawnych (deklaracja ONZ (UNCITRAL), deklaracja OECD, regulacje UE).

Teraz skupmy się na dokumentach prawnych, które tworzy właściciel serwisu handlu elektronicznego, a konkretnie: regulamin serwisu, zawarcie umowy i prawach, które wynikają z nich[79].

3.3.1. Regulamin serwisu

Regulamin to zbiór obowiązków, nakazów, zakazów, normujących zachowanie się konsumenta w serwisie internetowym. Regulaminy określają wewnętrzne zasady postępowania i życia organizacji, instytucji lub grup osobowych. Brak regulaminu lub nie jakościowe jego przygotowanie pociąga za sobą zagrożenia bezpieczeństwa.

Regulamin daje korzyści obu stronom – klient będzie wiedział, na jakich zasadach zawiera umowę, przedsiębiorca będzie mógł „wyłączyć" swoją odpowiedzialność w niektórych zakresach. Regulamin powinien być dostępny dla każdego (najlepiej umieszczony na stronie internetowej sklepu internetowego).

[79] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.33-36.

Dobry regulamin powinien być dostosowany do specyfiku prowadzonego handlu w Internecie i musi mieć następujące części:

1. Postanowienia ogólne.

W tej części należy umieszcza się informację o podmiocie prowadzających e-commerce (dane firmy), rodzaj i zakres prowadzonej działalności e-commerce, kto może korzystać ze sklepu, informacje o prawach autorskich, zakazie dostarczania przez usługobiorcę treści o charakterze bezprawnym, wymagania techniczne dla korzystania z systemu e-commerce.

2. Definicje.

W tej części należy wyjaśnić kluczowe pojęcia używane w regulaminie, takie jak usługodawca, użytkownik, zamówienie, umowa itd.

3. Warunki zawierania umowy.

W tej części należy omówić wszystkie warunki umowy, między innym warunki do spełnienia przez klienta (na przykład dokonanie wyboru towaru lub usługi, przekazanie danych niezbędnych do transakcji, akceptacja regulaminu), przez usługodawcę, określenia chwili zawarcia umowy, w tym procedury składania zamówienia.

4. Płatności.

Tu znajdą się postanowienia, dotyczące sposobu i terminu płatności. W większości krajów nie można przymuszać klienta do zapłaty z góry.

5. Realizacja umowy.

W tej części znajdą się w szczególności zasady dotyczące dostawy, czyli określenie sposobu dostawy, odbioru i związanych z tym kosztów. Zwykle towar powinien dotrzeć do klienta w ciągu 30 dni od złożenia zamówienia.

6. Gwarancja i postępowania reklamacyjne.

W tym rozdziale trzeba omówić zasady gwarancji i szczegóły dotyczące postępowania reklamacyjnego (sposobu złożenia reklamacji, elementów niezbędnych do jej złożenia, przedmiotu, okoliczności, prawa klienta i td).

7. Odstąpienie lub rozwiązanie umowy.

Tu powinni być omówione zasady, dotyczące odstąpienie od umowy i zwrotu towaru (w jaki sposób odstąpić od umowy, w jaki termin, jakie obowiązki z tego wynikają, w jaki sposób zwrócić towar, w ciągu ilu dni i td).

8. Ochrona danych osobowych.

W regulaminie powinni być omówione zasady o ochronie danych osobowych, ale nie trzeba pisać dużo. Lepiej stworzyć osobny dokument, tzw. Polityka prywatności, i tak szczegółowo opisać wszystkie zagadnienia o ochronie danych osobowych.

9. Postanowienia końcowe.

Ta część powinna wskazywać zasady wprowadzenia zmian w regulaminie, zasady rozstrzygania sporów, informację o przepisach prawnych, na których bazując był składany ten regulamin[80].

3.3.2. Przetwarzanie danych osobowych

Przy prowadzeniu handlu elektronicznego jak i tradycyjnego, jest niezbędne przetwarzanie danych osobowych, w związku z czym należy podlegać ustawie o chronie danych osobowych. Zgodnie z ustawami międzynarodowymi oto informacje, które podlegają przetwarzaniu:

1. Nazwisko i imię (imiona) usługobiorcy.
2. Numer identyfikacyjny, numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość.
3. Adres zameldowania.
4. Adres do korespondencji.
5. Dane służące do weryfikacji podpisu elektronicznego.
6. Adresy elektroniczne usługobiorcy.

Dodatkowo mogą być przekazane za zgodą usługobiorcy dane niezbędne dla celów reklamy, badania rynku, zachowania i preferencji użytkowników.

Należy pamiętać, że te dane są danymi poufnymi i trzeba dołożyć wszelkich działań, zabezpieczających te dane:

1. Zmiana hasła co 30 dni i używanie odpowiednich reguł, dotyczących hasła (na przykład, minimalnie 8 znaków, używanie liter różnego stylu itd).
2. Stosowanie szyfrowania przy przesyłaniu danych przez Internet.
3. Stosowanie firewalla, programów antywirusowych na komputerach.
4. Wykonywanie zapasowych kopii danych.

[80] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce,* Helion 2012, s.33-36.

3.3.3. Zawarcie umów przez Internet

Internetyzacja życia gospodarczego przywiodła do zawarcia umów drogą elektroniczną i powstania pojęcia elektronicznego oświadczenia woli. Oświadczenia elektroniczne również posiadają moc prawną przy demonstracji dostatecznej woli osoby, która składa takie oświadczenie. Dla efektywnego złożenia oświadczenia woli w formie elektronicznej niewymagane jest zapisanie tych danych w systemie informatycznym odbiorcy. Wystarczy tylko możliwości zapoznania się z treścią oświadczenia. Nieskuteczne przesłanie oświadczenia z powodu braku dostępu do sieci, czy wadliwego jej działania powoduje, że nie zostaje ono złożone.

Po otrzymaniu oświadczenia woli umowa może być zawarta w drodze:

1. Złożenia oferty oraz jej przyjęcia.

Mówimy o ofercie, kiedy posiada ona oświadczenie chęci zawarcia umowy i dokładny opis wszystkich warunków. Nie przyjmujemy za ofertę skierowane do wielu osób lub do konkretnej osoby ogłoszenia, reklamy, cenniki i inne informacje.

2. Negocjacji.

W wyniku prowadzonych negocjacji może również dojść do umowy. W takim przypadku, kiedy strony prowadzają negocjacje w celu zawarcia umowy, to umowa zostaje zawarta przy porozumieniu obu stron.

3. Przetargu (aukcji, przetargu pisemnego).

W Internecie istnieje dużo serwisów aukcyjnych, ale w przypadku korzystania z takich serwisów będziemy zawierali umowę w trybie złożenia oferty i jej przyjęcia, a nie w trybie przetargu.

W umowie między innym powinny być zapisane wszystkie zasady, jak i w regulaminie serwisu internetowego, o czym dokładnie pisaliśmy w rozdziale 3.3.1. Umowa nie może obciążać konsumenta obowiązkiem zapłaty ceny lub wynagrodzenia przed otrzymaniem towaru lub usługi. Również musi określać miejsce i sposób składania reklamacji, które nie będzie powodować nadmiernych trudności lub kosztów po stronie konsumenta.

Podsumowując, należy zaznaczyć, że międzynarodowe normy prawne, dotyczące regulacji handlu elektronicznego nadal formułują się. Jest powiązane po-pierwsze z szybkim rozwojem e-handlu, a po-drugie z odmiennymi ustawami prawnymi w poszczególnych krajach. Wiedza krajowych norm prawnych, dotyczących działalności, prowadzonej w

Internecie, posiadanie regulaminu sklepu, polityki prywatności, prawidłowo napisanej umowy pozwoli przedsiębiorcy zabezpieczyć swój biznes.

Rozdział 4
Analiza bezpieczeństwa handlu elektronicznego w Polsce i Ukrainie

Polska i Ukraina - kraje sąsiadujące, które mają różny stan rozwoju ekonomicznego i politycznego. Komercja elektroniczna w tych krajach również znajduję się na odmiennych poziomach. Celem poniższego rozdziału jest porównanie stanu rozwoju handlu elektronicznego w Polsce i Ukrainie, analiza poziomu bezpieczeństwa handlu w sieci, uregulowań prawnych celem znalezienia lepszych praktyk i określenia dalszych perspektyw rozwoju.

4.1. Ocena obecnego stanu handlu elektronicznego

W tym rozdziale przeanalizujemy stan obecny handlu elektronicznego za następującymi elementami:

1. Ogólna charakterystyka rynku.
2. Charakterystyka e-konsumenta.
3. Rozmiar i struktura rynku.
4. Wybór 50 największych sklepów internetowych w kraju za kategoriami: elektronika i AGD, zdrowie i uroda, kultura i rozrywka, moda i sklepy specjalistyczne.

4.1.1. Obecny stan handlu elektronicznego w Polsce

1. Ogólna charakterystyka rynku

Polski rynek handlu elektronicznego stałe rośnie, chociaż w ostatni parę lat tempo zrostu powoli zwalniają się. Udział sektora elektronicznego w polskim PKB stanowi 1,6 – 1,7%.

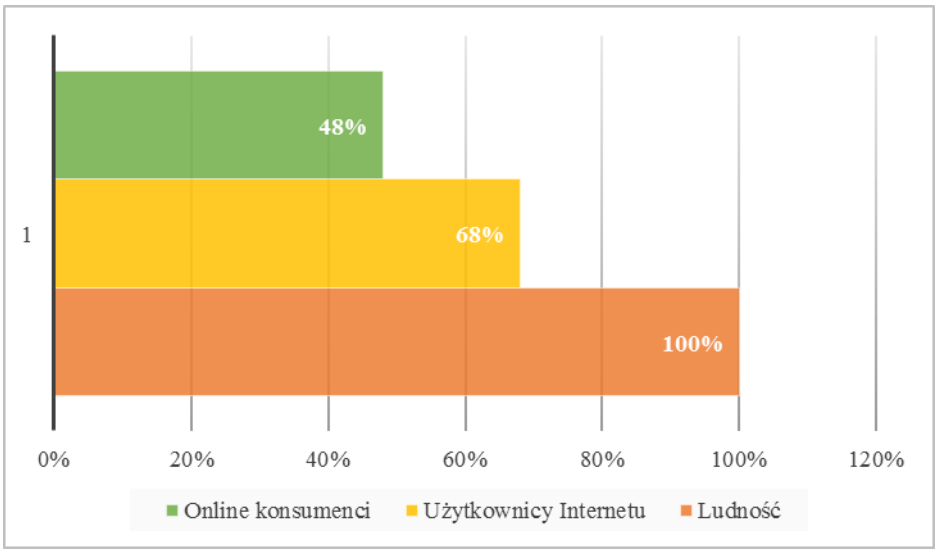
W ostatnich łatach udział sprzedaży w Internecie stanowi około 2,2% od całej sprzedaży w polskim przemyśle. Cała wartość polskiego rynku elektronicznego stanowi około 7,3 mld

EUR[81]. W porównaniu z pozostałymi krajami UE Polska posiada nie najlepsze pozycji. Na przykład udział sprzedaż e-commerce w ogólnym handlu w Niemczech stanowi 10%, we Francji 8,7%, we Włochach – 6,2%. W Czechach, Węgrach i Slowacji odnoszenie handlu elektronicznego do całego handlu jest prawie na takim poziomie jak w Polsce, ale Polska posiada pierwsze miejsce za ilością użytkowników, robiących zakupy w sieci. W 2014 roku wzrost w porównaniu z 2013 r. był 16%.

2. Polski e-konsument

W Polsce 38,5 mln osób ludności, z nich 26,2 mln os.są użytkownikami Internetu, z których 12,6 mln.os. aktywnie robią zakupy w sieci. Większość użytkowników sieci to przeważnie ludzie w wieku 18-50 lat. Za danymi GUS więcej niż 70% gospodarstw domowych mają komputer i dostęp do Internetu. Na rysunku 4.1 przedstawimy procentowe statystyki tego podziału[82]. Więcej niż 54% są użytkownikami sieci spolecznościowych, a 25% posiadają smartfona.

Rysunek 4.1. Procentowy podział użytkowników Internetu w Polsce, %



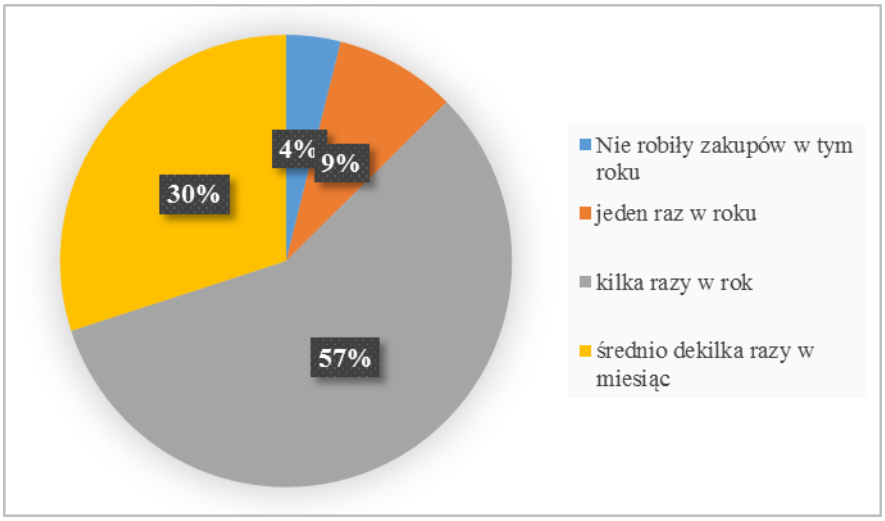
Zródlo: *ECommerce Poland Executive Summary Raport 2014*, s.24

Większość e-konsumentow w Polsce robi zakupy, co najmniej 3 razy w roku. Tylko 16% ludzi w ogóle nie mieło żadnego doświadczenia kupna przez Internet. Około 40% robią zakupy w Internecie już minimalnie 3 lata, 28% w ciągu 1-3 lat, a 17,6% w ciągu ostatniego roku. Na rysunku 4.2 pokazane są poszczególne statystyki częstotliwości zakupów w sieci

[81] *Rynek elektroniczny w Polsce.* Opracowane przez Agnieszkę Garbacz. Departament Informacji Gospodarczej Polska Agencja Informacji i Inwestycji Zagranicznych S.A., 2010, s.3.
[82] *ECommerce Poland Executive Summary Raport 2014*, s.22

przez polskich użytkowników internetowych. W podziale na wiek, to najchętniej robią zakupy ludzie w wieku 31-50 (42,8% robią zakupy kilka razy w rok i 28% co miesiąc), a mniej chętniej osoby w wieku więcej 65 łat (40,8% osób nigdy nie robili zakupów w sieci) i osoby w wieku mniej 18 łat (32% nie robili w ogóle zakupów w sieci)[83].

Rysunek 4.2. Częstotliwość robienia zakupów w sieci



Zródlo: *ECommerce Poland Executive Summary Raport 2014*, s.28

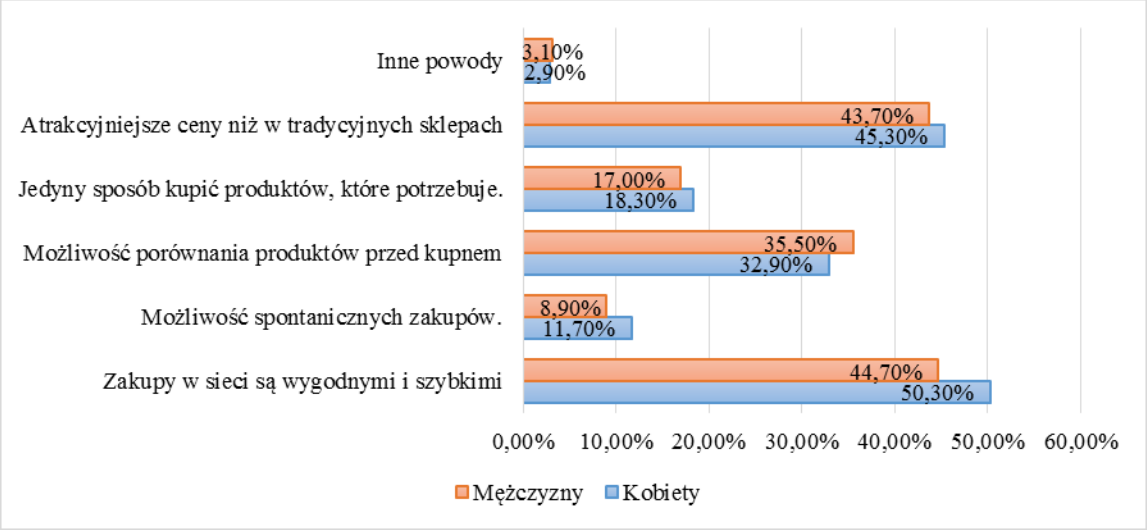
Motywacja konsumentów do zakupów w sieci jest następująca:

1. Zakupy w sieci są wygodnymi i szybkimi.
2. Możliwość spontanicznych zakupów.
3. Możliwość porównania produktów przed kupnem.
4. Jedyny sposób kupić produktów, które potrzebuje.
5. Atrakcyjniejsze ceny niż w tradycyjnych sklepach.
6. Inne powody.

Na rysunku 4.3. przedstawimy podział procentowy i według płci wyżej podanych motywacji. Jak wynika z rysunku, najchętniej w Internecie robią zakupy kobiety, a głównym powodem dla zakupów w sieci jest niższa cena niż w sklepie tradycyjnym, i szybkość i łatwość zakupów.

[83] Ibidem, s.22

Rysunek 4.3. Motywacja robienia zakupów w sieci



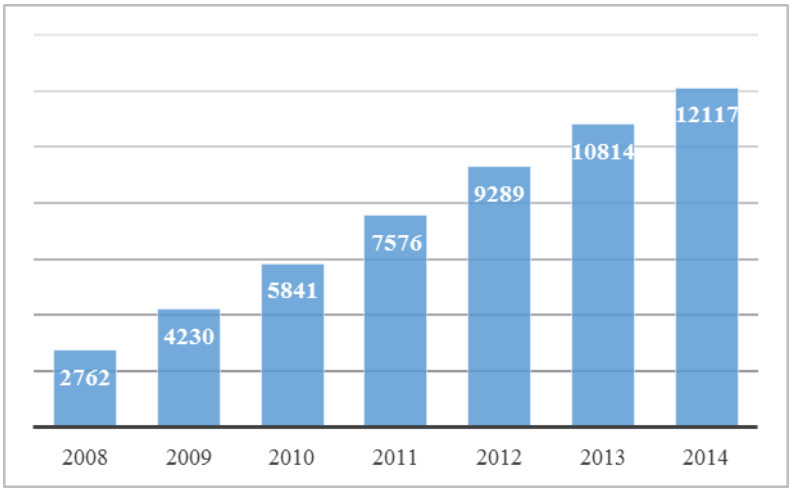
Zródlo: *ECommerce Poland Executive Summary Raport 2014*, s.8

3. Rozmiar i struktura rynku

Polski rynek e-commerce szybko i stabilnie rośne, za 2014 rok największy wzrost był w dziedzinie elektronicznej, (23%), jedzenia (14%) i sklepów książkowych (9%). W szczególności nie jest dziwnym wzrost liczby sklepów spożywczych, rynek tych produktów ma największy potencjał. Na rysunku 4.4. przedstawimy statystyki wzrostu liczby sklepów internetowych[84].

Rysunek 4.4. Wzrost liczby sklepów internetowych za 2008-2014 rr.

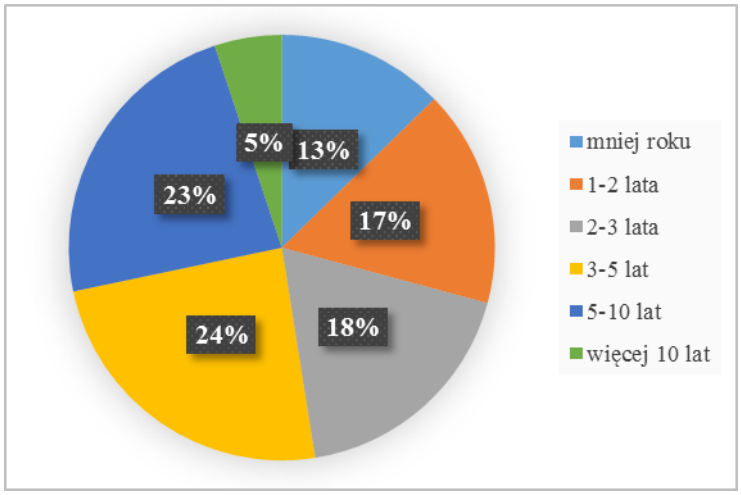
[84] *E-gospodarka w Polsce. Stan obecny i perspektywy.* Zeszyty naukowe Uniwersytetu Szczecińskiego nr 597, Szczecin 2010, s.28.



Zródło: *Raport E-handle Polska*, 2014, s.13.

Jeżeli chodzi o wiek sklepów, więcej 50% rynku składają skłepy w wieku 3 – 10 łat. Jest to dobrze dla konsumentów, ponieważ mają wielką szansę trafić na doświadczony sklep. Na rysunku 4.5 przedstawimy szczególne statystyki:

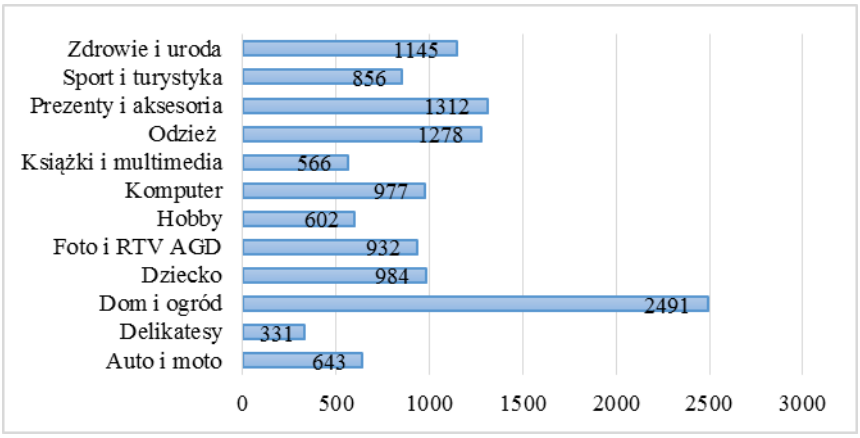
Rysunek 4.5. Podział sklepów internetowych za wiekiem



Zródło: *Raport E-handle Polska*, 2014, s.15.

46% procent ze sklepów internetowych mają sprzedaży offline w sklepach tradycyjnych. Najliczniej reprezentowaną w polskim handlu elektronicznym jest branża Dom i Ogród (około 2500 sklepów), a najmniejszą reprezentację mają Delikatesy (około 330 sklepów). Według badań 85% sklepów są opłacane, ale 40% maja obroty poniżej 10 tys.zł. Poszczególny podział na rysunku 4.6.

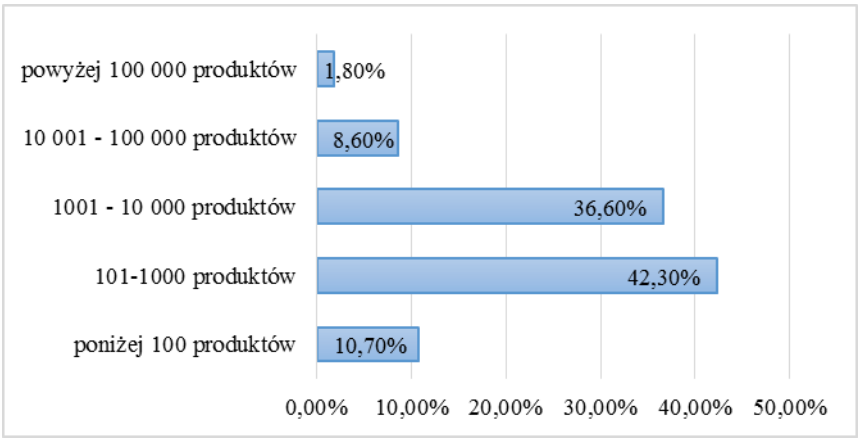
Rysunek 4.6. Polski rynek e-commerce za branżami



Zródło: *Raport E-handle Polska*, 2014, s.17.

85% polskich sklepów internetowych to mikro i małe przedsiębiorstwa. Jeżeli chodzi o kraj handlu, to 99,8% sklepów udostępniają swoją ofertę polskim konsumentom, 33,1% również do krajów UE, 9,6% do innych krajów. Jeżeli chodzi o ofercie, to na rysunku 4.7 jest przedstawiony podział sklepów według oferowanych produktów.

Rysunek 4.7. Rozmiar oferty polskich sklepów internetowych



Zródło: *Raport E-handle Polska*, 2014, s.20.

Średnia wartość konsumenskiego koszyka to około 150 zł. Oczywiście, że wartości koszyków przekładają się na przychody sklepów, ale ich rentowność i zyski zależą od marży handlowej jaką udaje im się uzyskać. Średnia marża handlowa polskich sklepów internetowych to 21,7%, ale większość sprzedawców uzyskuje ją poniżej 20%[85].

Najczęściej akceptowane metody platnośći – to przelew bankowy i płatność za pobraniem. Przy płatnościach około 70% sklepów korzystaja z serwisów platniczych, takich jak PayU, eCard, Przelewy24. 10% sklepów obsługuję przelewy w walucie obcej. Średni czas

[85] *Raport E-handle Polska*, 2014, s.11-21.

dostarczania towarów – to 3 dni roboczych, najczęściej polskie sklepy korzystają z usług Siodemka, Poczta Polska, UPS i DHL[86].

4. TOP-50 polskich sklepów internetowych.

Postanowiliśmy wybrać 50 największych sklepów za rankingami konsumenckimi. Najbardziej znanym rankigiem sklepów internetowych w Polsce jest ranking Money.pl[87]. W tabeli 4.1 przedstawimy TOP 10 polskich sklepów internetowych według w następujących kategoriach:

Tabela 4.1. Top-50 polskich sklepów internetów według kategorii

	Elektronika AGD	Zdrowie i uroda	Kultura i rozrywka	Moda	Sklepy specjalicstyczne
1	komputronik.pl	iperfumy.pl	matras.pl	eobuwie.com.pl	selgros24.pl
2	mediamarkt.pl	i-apteka.pl	merlin.pl	zalando.pl	dom-ogrod.com
3	saturn.pl	tanie-leczenie.pl	gandalf.com.pl	czasnabuty.pl	bdsklep.pl
4	euro.com.pl	apteka-melissa.pl	empik.com	sarenza.pl	rockmetalshop.pl
5	redcoon.pl	aptekaslonik.pl	helion.pl	answear.com	leroymerlin.pl
6	electro.pl	aptekaslonik.pl	taniaksiazka.pl	bonprix.pl	smyk.com
7	morele.net	cefarm24.pl	ravelo.pl	deichmann.com	chocolissimo.pl
8	oleole.pl	aptekagemini.pl	inbook.pl	topsecret.pl	motointegrator.pl
9	neo24.pl	yves-rocher.pl	bonito.pl	sizeer.com	muve.pl
10	agito.pl	doz.pl	pwn.pl	spartoo.pl	endo.pl

Źródło: Opracowanie własne.

Podsumowując, polski rynek e-commerce jest rozwięty, rozwój jest stabilny, chociaż ostatnie 2 lata ten trend zmniejsza się. W Polsce istnieje około 12 000 sklepów internetowych, połowa z nich jest na rynku od około 5 lat. 14,6% użytkowników robi zakupy w Internecie, około 57% z nich robi zakupy kilka razy w roku. Więcej 85% sklepów jest rentownych, 42% sklepów ma w ofercie około 1000 produktów.

4.1.2. Obecny stan handlu elektronicznego w Ukrainie

1. Ogólna charakterystyka

[86] *E-commerse Polska 2014,* Gemius dla E-commerce Polska, s. 5-9.
[87] *Ranking Sklepów internetowych 2014.* http://ranking.money.pl/ [dostęp 18.03.2015]

Handel elektroniczny w Ukrainie to jedna z najszybciej rozwiających się dziedzin ekonomii państwa. W porównaniu z krajami Europy Środkowo-Wschodniej, pojawienie się sektora biznesu elektronicznego odbyło się dużo późno. Tylko w 2012 roku handel elktroniczny w Ukrainie przeszedł z fazy zarodka do fazę rozwoju. W 2014 roku czastka handlu elektroniczznnego stanowiła tylko 1,3% od ogólnej sprzedaży. Ale z innej strony handel elektroniczny w 2014 roku w porównaniu z 2013 r wzrósł do 30%, i taka tendencja wzrostu prognozowana jest na następne lata[88]. W tabeli 4.2. są przedstawione liczbowe dane rozwoju
e-commerce w Ukrainie za 2010 – 2014 r. I prognoza rozwoju na 2015-2017 r.

Tabela 4.2. Statystyki i prognoza rozwoju e-commerce w Ukrainie

	2010	2011	2012	2013	2014	2015	2016	2017
Rozmiar rynku e-commerce, mld.$	0,4	0,6	0,55	0,73	1,1	1,59	2,37	3,24
Penetracja handlu elektronicznego, %	0,6	0,7	1,0	1,1	1,3	1,6	2,3	2,9

Zródło: Opracowanie wlasne.

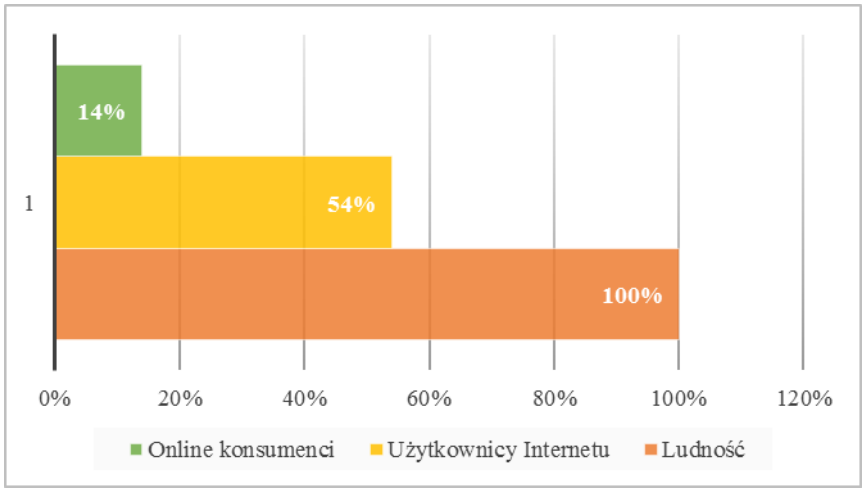
Ale już za danymi z początku 2015 roku rynek e-commerce zmniejszał się do 17%. To jest powiązane z niespójnym ekonomicznie i politycznie stanem w 2014 r., utratą części terytoriów, obywatele kupują mniej. W 2017 roku jest oczekiwany rozmiar rynku e-commerce w 3.24 mld.$[89].

2.Ukraiński e-konsument

Penetracja Internetu w Ukrainie jest na poziomie 54% (około 22 mln osób), ale tylko 58% gospodarstw domowych ma komputer w domu[90]. Około 4 mln osób robi zakupy w Internecie kilka razy w rok. Na rysunku 4.8 pokazany jest procentowy podział użytkowników Internetu
i osób, robiących zakupy w Internecie w Ukrainie.

Rysunek 4.8. Procentowy podział użytkowników Internetu w Ukrainie, %

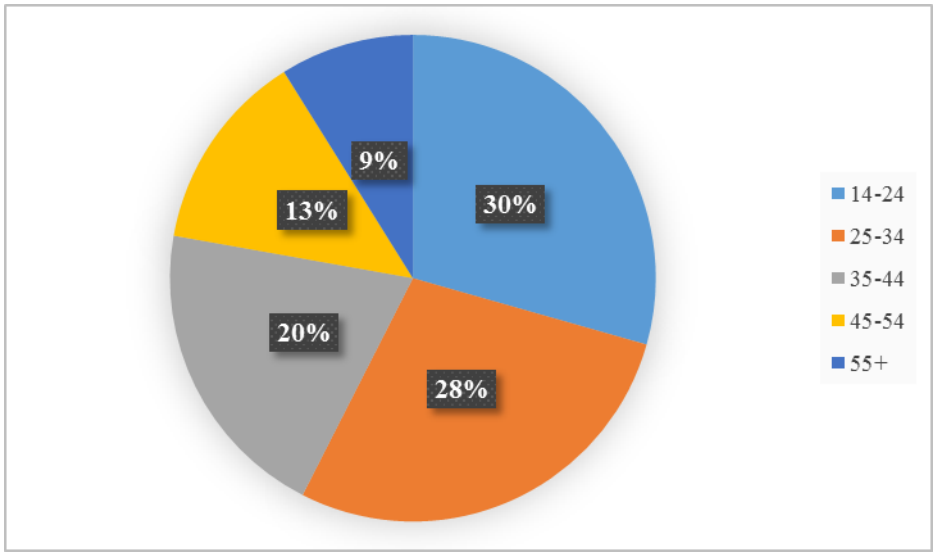
[88] V.Pavlova, *O problemie rozwoju handlu elektronicznego w Ukrainie.*, Dziennik ekonomiczny, №1 (2014).
[89] *Prognoza rozwoju rynku e-commerce 2014-2017 rr.,* Prom.ua dla emarketing,ua, 2013, s.2.
[90] *Rynek telekomunikacyjny*, Państwowy Urząd statystyczny Ukrainy, 2014, s.12.



Źródło: *Rynek telekomunikacyjny*, Państwowy Urząd statystyczny Ukrainy, 2014, s.12.

Względem podziału konsumentów według wieku jest średnio 20% w takich kategoriach wiekowych: 14-24, 25-34, 35-44. Liczba osób powyżej 55 lat, którzy korzystają z Internetu wynosi mniej niż 9%. Dokładniej statystyki podziału ze względu na wiek przedstawiono na rysunku 4.9.

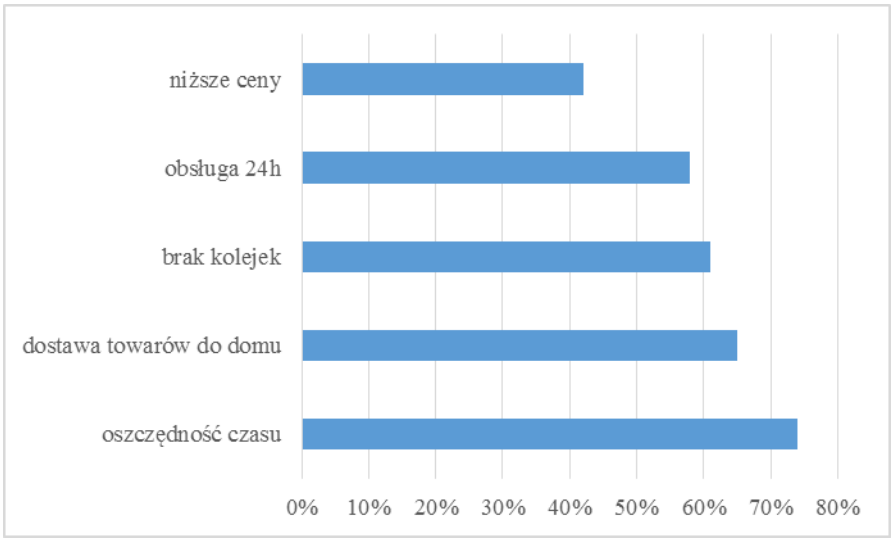
Rysunek 4.9. Podział ukraińskich użytkowników Internetu za wiekiem.



Źródło: *Państwowy Urząd statystyczny Ukrainy*. Rynek telekomunikacyjny, 2014, s.18.

Dlaczego ukraińscy użytkownicy decydują się na zakupy w Internecie? Większość kupuje, bo w Internecie oszczędza czas i ma możliwość dostawy „pod drzwi". Szczegóły motywacji konsumentów w Ukrainie przedstawione na rysunku 4.10.

Rysunek 4.10. Motywacja ukraińskich konsumentów do zakupów w Internecie



Źródło: Opracowanie własne

Najpopularniejszymi towarami, które ukraińcy kupują w Internecie są: komputery, elektronika, telefony komórkowe. Dla zakupów w Internecie 88% ukrainców wybierają serwisy aukcyjne i serwisy ogloszeniowe, 85% - prównywarki cen w Internecie i 55% - serwisy dyskontowe . W Ukrainie więcej kobiet niż mężczyzn robi zakupy w Internecie (odpowiednio 52,4% do 47,6%). 83,7% użytkowników robi zakupy przy pomocy komputera, z urządzeń mobilnych korzysta tylko 16,3%. 34% płaci kartą za zakupy, 59% użytkowników nadal płaci gotówką w banku lub przy odbiorze. 78% towarów jest dostarczanych za pomocą firm, nadających przesyłki expresowe, a tylko 6% wybierają pocztę w celu dostarczania towarów. Za danymi badań prom.ua przeciętny e-konsument w Ukrainie to kobieta w wieku 29 łat, która dokonuje zakupów w popularnych sklepach internetowych, płatności dokonuje gotówką rzadko kartą platniczą.

Podział zamówień internetowych ścisle zależy od wielkości miast, w których mieszka konsument. Przeważnie robią zakupy w Internecie mieszkańcy wielkich miast, takich jak Kijów (40%), Donieck (8%), Odesa (7%), Charków i Dniepropetrowsk (6%), Lwów (5%). Na pozostałe miasta przypada tylko 30% wszystich zakupów internetowych[91].

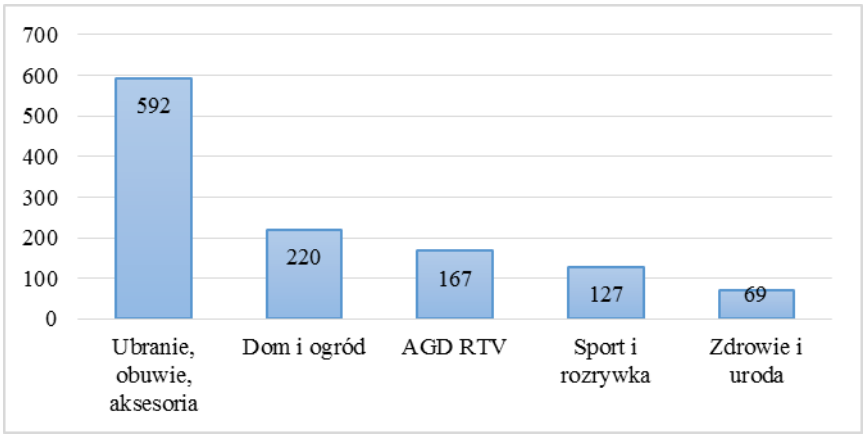
3. Rozmiar i struktura rynku

W 2014 roku ogólny rozmiar rynku internetowego w Ukrainie wyniósł 2 mld. $. W Ukrainie pracuje około 8 000 sklepów internetowych, i tylko 300 z nich posiada stabilne pozycje na rynku i jest rentownych. Oferta sklepów internetowych jest szeroka, ale większość

[91] *Charakterystyka rynku handlu elektronicznego w Ukrainie 2013*.Raport badawczy dla ain.ua., 2014, s.12-18

sklepów nie może pozwolić sobie wydatki na marketing i logistykę. Na rysunku 4.11. przedstawimy pięniżny obrót towarów w sektorze B2C w 2014 r. w Ukrainie.

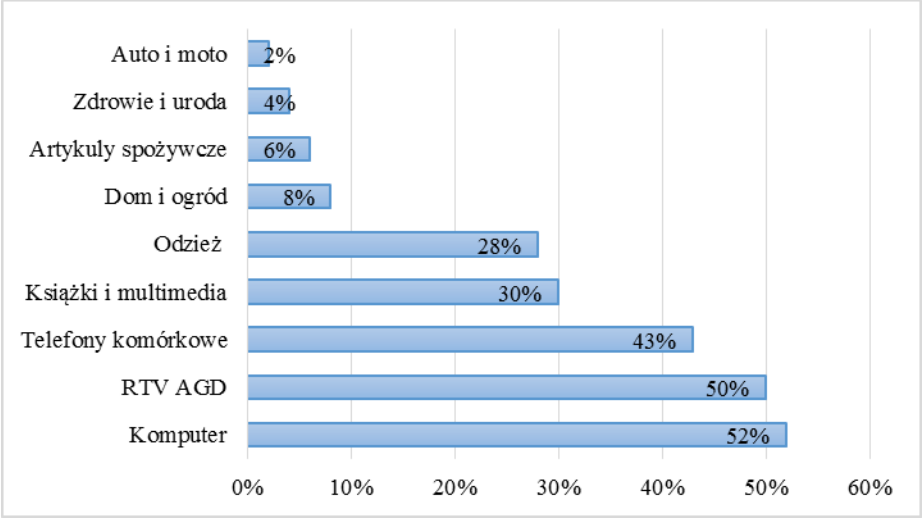
Rysunek 4.11. Obrót towarów w Internecie za kategoriami, mln. UAH



Żródło: Opracowanie własne

Na rysunku 4.12 przedstawiony podział towarów, które najczęsciej kupują w sieci ukraincy. Najchętniej ukraincy kupują komputery, technikę dla domu, telefony komórkowe.

Rysunek 4.12. Podział towarów, które najczęsciej kupują ukraińcy



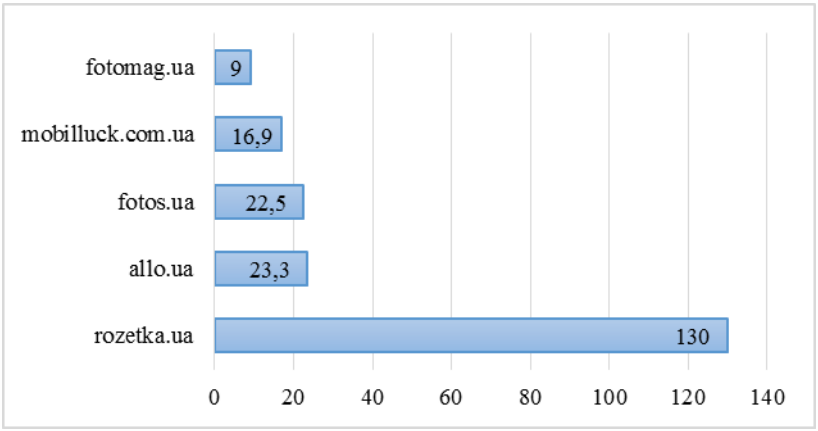
Zródło: *E-commerce w Ukrainie. Realność i perspektywy.* V.Galochkin, Chernivcy, 2014, s.23.

Największy sklep internetowy w Ukrainie to rozetka.ua, który wcześniej specjalizował się tylko w technice komputerowej, teraz rozszerzył ofertę i sprzedaje również odzież, obuwie, artykułu domowe itd. Spzedaż sprzętu elektronicznego w 2014 roku wyniosła 11% od całej sprzedaży w tym sektorze[92]. Statystyka dochodów największych sklepów

[92] *E-commerce w Ukrainie. Realność i perspektywy.* V.Galochkin, Chernivcy, 2014, s.21-28.

intrenetowych
w 2014 roku jest przedstawiona na rysunku 4.13.

Rysunek 4.13. Dochody największych sklepów internetowych w Ukrainie w 2014 roku, mln. UAH



Zródło: *E-commerce w Ukrainie. Realność i perspektywy.* V.Galochkin, Chernivcy, 2014, s.25.

Jak wynika z rysunku na ukraińskim rynku elektronicznym obserwowana jest monopolia (poszczególnie w segmencie AGD, RTV).

4.TOP-50 ukraińskich sklepów internetowych

Określimy 50 największych i popularnych sklepów internetowych w Ukrainie za rankingiem Prom.ua[93]. Dla kategorii sklepy specjalistyczne wyszukiwaliśmy sklepy internetowe ręcznie, ponieważ dany ranking nie ma takiego podziału. Wyniki przedstawimy w tabeli 4.3.

Tabela 4.3. Top-50 ukraińskich sklepów internetów według branży

	Elektronika AGD	Zdrowie i uroda	Kultura i rozrywka	Moda	Sklepy specjalicstyczne
1	rozetka.com.ua	beauty-life.com.ua	bukva.ua	bonprix.ua	e-esco.com.ua
2	allo.ua	avon.com.ua	yakaboo.ua	leboutique.com.ua	winauto.ua
3	fotos.ua	parfumeria.ua	nashformat.ua	modnakasta.ua	aqua-club.com.ua
4	foxtrot.com.ua	eva.dp.ua	bookclub.ua	lamoda.ua	autobazar.ua
5	mobilluck.ua	enjee.ua	librabook.com.ua	shopnow.com.ua	rst.ua
6	comfy.ua	watsons.com.ua	bookzone.com.ua	shopart.ua	auto.ria.ua

[93] *Ranking ukraińskich sklepów internetowych*, www.shops.prom.ua [dostęp 22.04.2015]

7	citrus.ua	ua.oriflame.com	petrovka.ua	helen-marlen.ua	infocar.ua
8	eldorado.ua	makeup.com.ua	knigoland.com.ua	stylepit.ua	olx.ua
9	fotomag.ua	cosmetic.com.ua	knigka.ua	www.witt-international.ua	agromat.ua
10	sokol.ua	beautystore.com.ua	book-mania.com.ua	fame.ua	prom.ua

Źródło: Opracowanie własne.

Rynek handlu elektronicznego w Ukrainie znajduje się w faziu rozwoju. W ostatnich latach tempo rozwoju zmniejszyło się, co jest powiązane z trudną sytuacją w kraju. Ale z każdym rokiem większa liczba osób decyduje się na robienie zakupów w Internecie i z każdym rokiem rośnie liczba firm sprzedających w Internecie.

4.2. Bezpieczeństwo technologiczne

Głównym podmiotem handlu elektronicznego jest sklep internetowy. W rozdziale 2 omówiliśmy teoretyczne i techniczne aspekty bezpieczeństwa technologicznego. W tym rozdziale prowadzimy badanie na temat bezpieczeństwa sklepów internetowych w Polsce i Ukrainie.

4.2.1. Metodologia badania

Bezpieczny sklep internetowy – to ten, który chroni swoich konsumntów przed zagrożeniami. Do głównych zagrożeń odnosimy kradzieży przesyłanych danych. Działalność sklepów internetowych polega na przetwarzaniu danych osobowych klientów, które uważają, że te poufne dane są we właściwy sposób chronione. Bezpieczny sklep internetowy musi szanować zaufanie klientów.

Sprawdzimy ile sklepów w Ukrainie i Polsce gwarantuję bezpieczeństwo swoim klientom. Wybierzmy TOP 50 sklepów do badania. Na etapie 1 sprawdzimy posiadanie zainstalowanego certyfikatu SSL (jego ważność, czy jest zaufany dostawca, czy jest poprawny klucz szyfrowania). Na drugim etapie sprawdzmy czy zmienia się adres strony na bezpieczny, przy logowaniu konsumenta do serwisu i na innych stronach, gdzie następuję wprowadzenie poufnych danych. Trzeci etap – analiza używania znaków bezpieczeństwa i informowanie o tym klientów. I na ostatnim etapie ocenimy działalność sertyfikatu SSL strony.

1. Etap 1

Przeskanujemy wszystkie adresy internetowe narzędziem SSL Labs. SSL Labs to niezależne narzędzie, które pomaga sprawdzić konfigurację certyfikatów SSL w danym sklepie internetowym.

Po badaniu przyznaje oceny certyfikatów (skala od 0 do 100) i pokazuje uwagi (tabela 4.4):

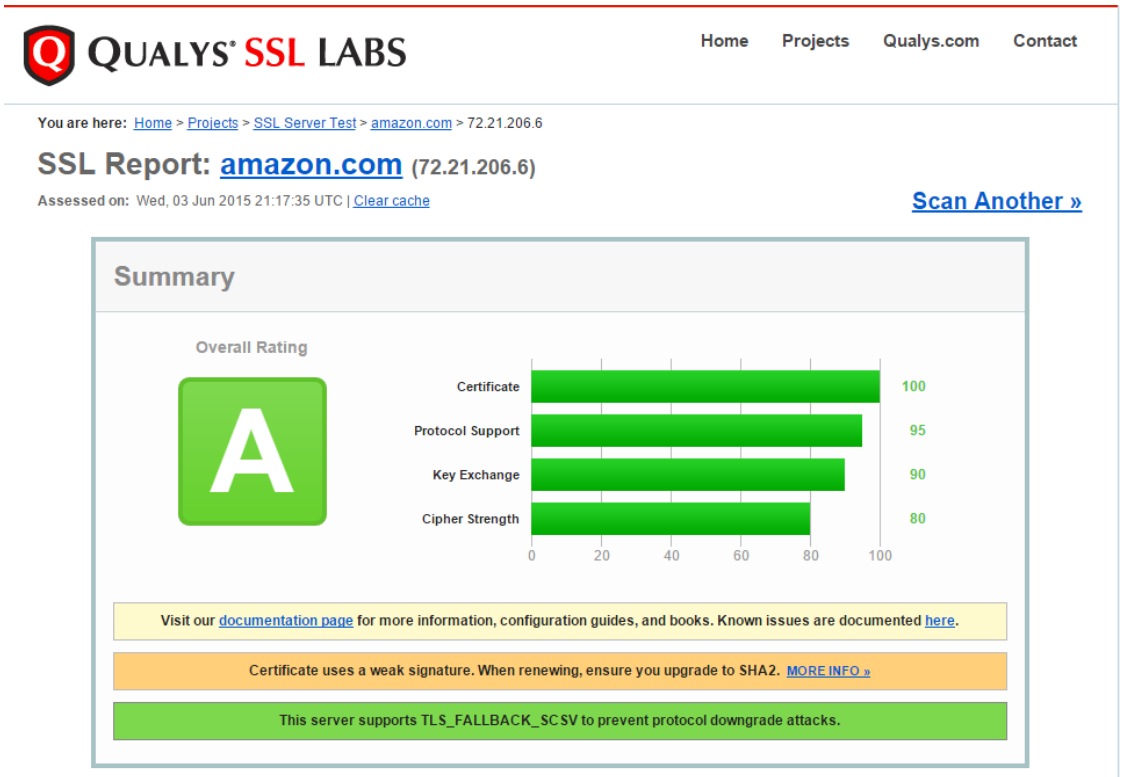
Tabela 4.4. Oceny certyfikatów według SSL

F	E	D	C	B	A
<20	≥20	≥35	≥50	≥65	≥80

Zródło: opracowanie własne

Na rysunku 4.14 pokażemy przykladowy zrzut ekranu z analizą SSL Labs.

Rysunek 4.14. Wynik badania SSL Labs dla strony amazon.com



Zródło: Narzędzie SSL Labs. https://www.ssllabs.com [dostęp 25.04.15]

SSL Labs również wydaje szczególną informację o datę ważności certyfikatu, poziom zaufania do wystawcy, ustawienia serweru w trzech kategoriach:

1. Obsługa protokolu SSL – 30%.

Każdy serwer używa różnych protokołów SSL, ale jednak nie wszystkie są na jednym poziomie efektywności. Jak przykład, protokoł SSL 2.0 był stworzony 12 lat temu i nie jest aktualny do używania dzisiaj. Narzedzie SSL Labs ocenia protokół wedlug takich zasad: sumujemy ocenę najsilniejszego protokołu z najsłabszym i dzielimy przez 2. Oceny protokołow według SSL Labs są przedstawione w tabeli 4.5:

Tabela 4.5. Oceny protokolów wedlug SSL Labs

Protokoł	SSL 2.0	SSL 3.0	SSL 4.0	TLS 1.0	TLS 1.1	TLS 1.2
Ocena	20%	80%	90%	90%	95%	100%

Zródło: opracowanie własne

2. Obsługa wymiany kluczy – 30%.

Obsługa wymiany kluczy dzieli się na dwa etapy: zapewnianie i sprawdzenie bezpieczeństwa wygenerowanych kluczy (tak publicznego, jak i prywatnego) i sprawdzenie efektywności ich wymiany. Sprawdzenie bezpieczeństwa kluczy polega na liczeniu bitów, od 2011 roku najkrótszym kluczem jest uznawany 2048 –bitowy. Oczywiście im więcej bitów posiada klucz prywatny, tym bardziej skomplikowany jest proces jego rozszyfrowania. W tabeli 4.6. są oceny narzędzia SSL Labs co do kluczy:

Tabela 4.6. Oceny procentowe kluczy

Dostępność klucza	Brak klucza	Słaby klucz	Krótszy niż 512 bitów	Limit 512 bitów	Krótszy niż 1024 bitów	Krótszy od 2048 bitów	Krótszy od 4096 bitów	Dłuższy lub równy 4096 bitów
Ocena	0%	0%	20%	40%	40%	80%	90%	100%

Zródło: opracowanie własne

3. Obsługa szyfrowania – 40%.

Im lepszy algorytm szyfru, tym lepsze i bezpieczniejsze szyfrowanie połączenia i mniejsza szansa na zakończenie połączenia. Każdy serwer może osługiwaćkilka różnych szyfrów, dlatego narzędzie SSL Labs daje najmniejszą ilość punktów najsłabszym. Obliczanie

wyniku końcowego tu jest podobnie do obliczania wyniku obsługi protokołu SSL, a sumujemy ocenę najlepszego szyfru na tym serwerze z najgorszym i dzielimy przez 2. W tabeli 4.7. przedstawimy procentowe oceny szyfrowania[94]:

Tabela 4.7. Procentowe oceny szyfrowania według SSL Labs

Jakość szyfrowania	Brak	Poniżej 128-bitów (40-56)	128 – 256 bitów (128,168)	256 bitów lub więcej
Ocena	0%	20%	80%	100%

Wynik końcowy po badaniu SSL Labs uwzględnia również konfigurację serwera WWW, zabezpieczenie domeny internetowej. Dopasowanie nazwy serwera do domeny itd.

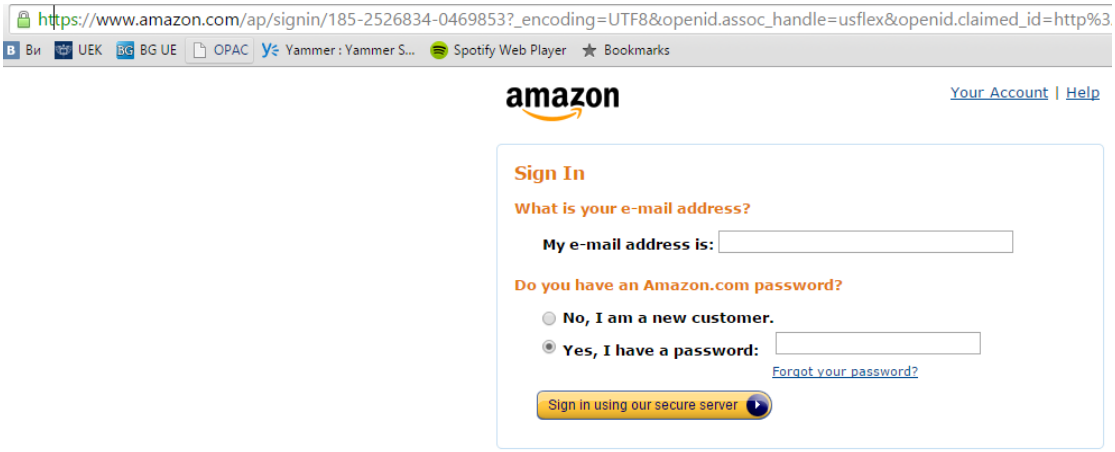
Moim zdaniem narzędzie SSL Labs jest dobrym narzędziem dla sprawdzenia bezpieczeństwa sklepów intrenetowych. Ale dla lepszej oceny nasze badane sklepy internetowe były przetestowane przez narzędzia CertyfikatySSL.pl i SSL4Less.ru

Etap 2

Kolejnym etapem badania będzie wpisywanie domeny sklepu internetowego do przeglądarki. W taki sposób sprawdzimy czy zmienia się protokół serwera http:// (zwykły protokol) na https:// (bezpieczny protokół) na takich stronach, jak logowanie użytkownika, rejestracja użytkownika w serwisie, wysyłanie zamówienia, czyli wtedy, kiedy użytkownik wprowadza poufne dane do systemu. W taki sposób możemy sprawdzić ile sklepów podaje swoim klientom nieprawdziwe informacje co do bezpieczeństwa transakcji[95]. Przykladowo przedstawimy okno z trybem https:// na rysunku 4.15.

Rysunek 4.15. Okno logowania na srtonie amazon.com w trybie „security”

[94] *Bezpieczeństwo zakupów w polskich sklepach internetowych*, Raport certyfikatyssl.pl, marzec 2013, s.14-18
[95] *Bezpieczeństwo zakupów w polskich sklepach internetowych*, Raport certyfikatyssl.pl, marzec 2013, s.19-20



Źródło: amazon.com

Opisane wyżej dwa etapy pomogą określić ogólną sytuację, dotyczącą bezpieczeństwa zakupów w Internecie w Polsce i Ukrainie.

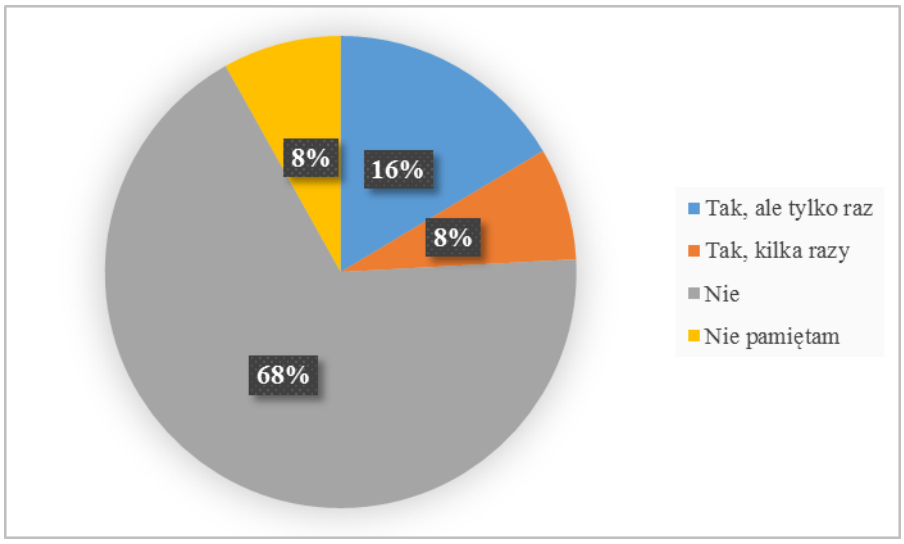
4.2.2. Ocena bezpieczeństwa technologicznego handlu elektronicznego w Polsce

1. Ocena bezpieczeństwa w sieci według konsumenta

Według konsumentów bezpieczeństwo zakupów w Internecie to jeden z najważniejszych kryteriów korzystania ze sklepów internetowych. Z badań, prowadzonych przez Ceneo, wynika, że 16% użytkowników sklepów internetowych, chociaż raz miał nieprzyjemną sytuację z zamówieniem (rysunek 4.16). 7% użytkowników miało więcej niż jedną taką sytuacje. Można pomyśleć, że 7% to niewielka liczba, ale co trzecia ofiara handlu elektronicznego była niezadowolona z towaru, a 4% w ogóle nie otrzymało towaru[96].

[96] *Bezpieczeństwo i zaufanie.Filary polskiego e-commerce*.Badania ceneo.pl, luty 2013, s.8-12

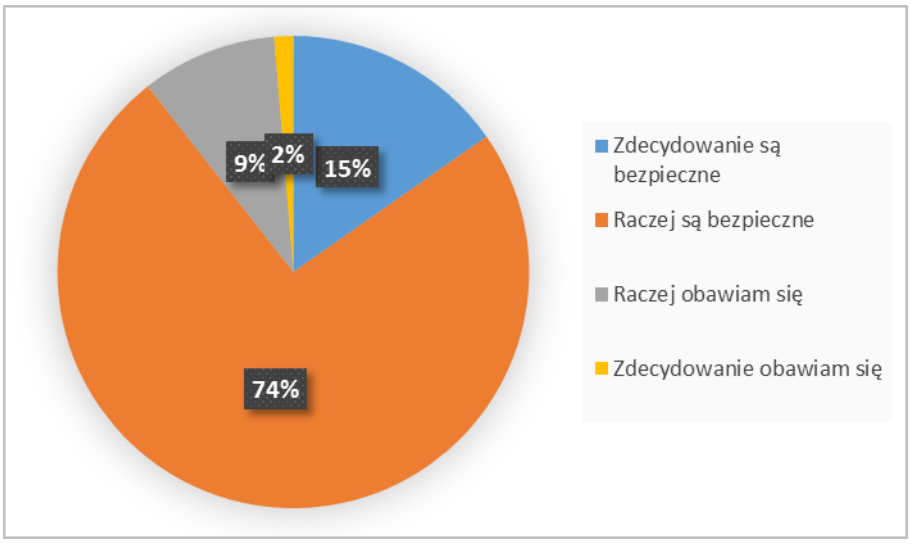
Rysunek 4.16. Statystyka konsumentów o oszuctwach w sieci



Zródło: *Bezpieczeństwo i zaufanie.Filary polskiego e-commerce*.Badania ceneo.pl, luty 2013, s.10

Na rysunku 4.17. są odpowiedzi badanych na pytanie „Twoim zdaniem zakupy online są?".

Rysunek 4.17. Statystyka opinii konsumentów według bezpieczeństwa zakupów w Internecie



Zródło: *Bezpieczeństwo i zaufanie.Filary polskiego e-commerce*.Badania ceneo.pl, luty 2013, s.14

Według danych z wykresu tylko 15% internautów uważa zakupy w Internecie za bezpiecznie, większa ilość osób (74%) myśli, że raczej są bezpieczne, a 2% obawia się zakupów w sieci. Dla 90% użytkowników kwestia bezpieczeństwa transakcji jest najgłówniejsza przy wyborze sklepu internetowego dla dokonania zakupu. Chodzi tu również

o bezpieczny przelew gotówki i dostarczanie zamówienia w terminie. Pozostale czynniki, którymi kierują się konsumenci – to opinie znajomych, uznawalność marki, dokładny opis towarów, łatwość korzystania z serwisu.

2. Wyniki badania

Dane badanie było prowadzone wśród 50 nawiększych i najpopularniejszych sklepów internetowych w Polsce. Lista sklepów w rozdziale 4.1.2.3. Wyniki badania rynku przedstawimy w tabeli 4.8.

Tabela 4.8. Wyniki badania bezpieczeństwa 50 sklepów elektronicznych w Polsce

Kategoria	*Sklep*	*Ocena certyfikatu SSL*	*Klucz szyfrowania*	*Ważność certyfikatu*	*Https://*	*Centrum autoryzacji*
Elektronika i AGD	komputronik.pl	B	2048	ważny	tak	Certum Extended Validation CA
	mediamarkt.pl	A	2048	ważny	tak	Certum Organization Validation CA SHA2
	saturn.pl	A	2048	ważny	tak	Certum Organization Validation CA SHA2
	euro.com.pl	C	2048	ważny	tak	Certum Domain Validation CA SHA2
	redcoon.pl	A	2048	nieważny	tak	GeoTrust SSL CA - G4
	electro.pl	F	2048	nieważny	tak	RapidSSL CA
	morele.net	A	2048	ważny	tak	COMODO Domain Validation Secure Server CA 2
	oleole.pl	C	2048	ważny	tak	Certum Level II CA
	neo24.pl	F	4096	ważny	nie	RapidSSL CA
	agito.pl	C	2048	ważny	tak	GeoTrust SSL CA - G2
Zdrowie i uroda	perfumeria.pl	C	2048	ważny	tak	Certum Domain Validation CA SHA2
	iperfumy.pl	C	2048	ważny	tak	thawte EV SSL CA
	i-apteka.pl	A	4096	ważny	tak	RapidSSL CA
	tanie-leczenie.pl	B	4096	ważny	tak	AlphaSSL CA - G2
	apteka-melissa.pl	missmatch				
	aptekaslonik.pl	missmatch				
	cefarm24.pl	B	2048	ważny	tak	Certum Level IV CA

	aptekagemini.pl	F	2048	ważny	tak	RapidSSL CA
	yves-rocher.pl	B	2048	ważny	tak	Certum Organization Validation CA SHA2
	doz.pl	B	2048	ważny	tak	RapidSSL CA
Kultura i rozrywka	matras.pl	C	2048	ważny	tak	Certum Organization Validation CA SHA2
	merlin.pl	A-	2048	ważny	tak	GeoTrust SSL CA - G3
	gandalf.com.pl	C	2038	ważny	tak	Certum Trusted Network CA
	empik.com	B	2048	ważny	tak	Thawte SSL CA
	helion.pl	B	4096	ważny	tak	DOMENY SSL OV Certification Authority
	taniaksiazka.pl	B	2048	ważny	tak	Certum CA
	ravelo.pl	B	2048	ważny	tak	Certum Extended Validation CA SHA2
	inbook.pl	C	2048	ważny	tak	DOMENY.PL DV Certification Authority
	bonito.pl	B	2048	ważny	tak	GeoTrust SSL CA - G2
	pwn.pl	C	4096	ważny	tak	Certum Domain Validation CA SHA2
Moda	eobuwie.com.pl	C	2048	wa xny	tak	RapidSSL SHA256 CA - G3
	zalando.pl	A	2048	ważny	tak	COMODO RSA Extended Validation Secure Server CA
	czasnabuty.pl	A	2048	ważny	tak	Certum Level IV CA
	sarenza.pl	A	2048	ważny	tak	GlobalSign Domain Validation CA - SHA256 - G2
	answear.com	B	2048	ważny	tak	thawte SSL CA - G2
	bonprix.pl	A	2048	ważny	tak	thawte SSL CA - G2
	deichmann.com	C	2048	ważny	tak	TeleSec ServerPass CA 1
	topsecret.pl	C	2048	ważny	tak	RapidSSL SHA256 CA - G3
	sizeer.com	C	4096	ważny	tak	RapidSSL CA
	spartoo.pl	B	2048	ważny	tak	COMODO RSA Extended Validation Secure Server CA
Sklepy specjalicstyczne	selgros24.pl	B	2048	ważny	tak	Gandi Standard SSL CA 2
	dom-ogrod.com	B	4096	ważny	tak	AlphaSSL CA - G2
	bdsklep.pl	A	2048	ważny	tak	RapidSSL SHA256 CA - G3
	rockmetalshop.pl	C	2048	ważny	tak	Certum Domain

						Validation CA SHA2
	leroymerlin.pl	B	2048	ważny	tak	RapidSSL CA
	smyk.com	B	2048	ważny	tak	Certum Level II CA
	chocolissimo.pl	C	2048	ważny	tak	Certum Level IV CA
	motointegrator.pl	B	2048	ważny	tak	GeoTrust EV SSL CA - G4
	muve.pl	A	2048	ważny	tak	Certum Organization Validation CA SHA2
	endo.pl	C	2048	ważny	tak	Certum Level IV CA

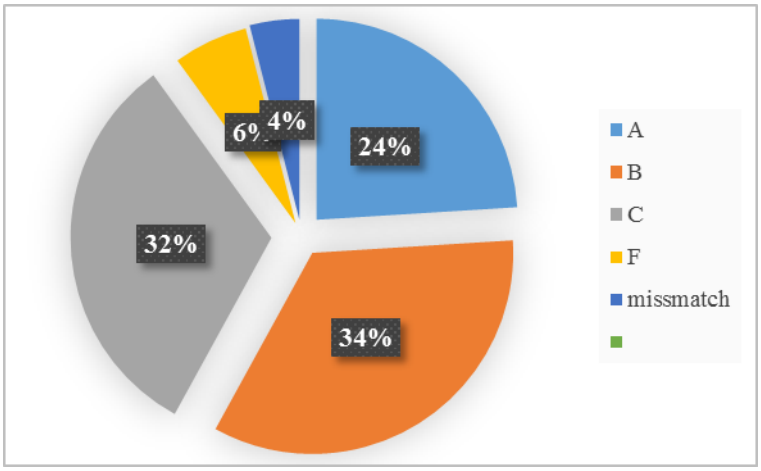
Zródło: Opracowanie własne

3. Objaśnienie wyników

Wszystkie sklepy zostały przeskanowane za pomocą narzędzia SSL Labs i wspomogających narzędzi dla obiektywnego wyniku: CertyfikatySSL.pl i SSL4Less.ru. Niektóre ze stron z powodu problemów technicznych nie było dostępnych w czasie badania, dlatego dla nich przeprowadziliśmy nowe badanie dzień później. Również sprawdziliśmy ręcznie wszystkie strony biorąc pod uwagę przedmiot posiadania bezpiecznego trybu https:// na stronach rejestracji, logowania i wypelnienia danych do zamówienia.

Z przeanalizowanych 50 sklepów najwyższą ocenę certyfikatów (A>80%) dostało tylko 12 sklepów. Oceny B i C otrzymało odpowiednio 17 i 16 sklepów. Najgorszą ocenę certyfikatu (F) otrzymały 3 sklepy, a 2 sklepy dostały „missmatch", co znaczy, że certyfikat nie jest połączony z podaną domenę. Ważny certyfikat bezpieczeństwa ma 45 sklepów, 2 z nich minął termin ważności klucza. Procentowe statystyki podziału ocen certyfikatów podamy na rysunku 4.18.

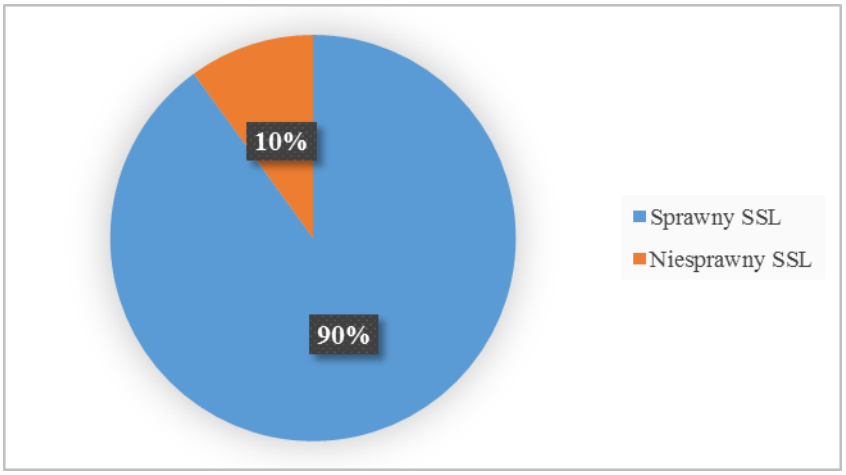
Rysunek 4.18. Procentowy podział ocen bezpieczeństwa sertyfikatów SSL polskich sklepów



Zródło: opracowanie własne

Należy wspomnieć, że za sprawne SSL przyjmujemy te, które mają ocenę A, B i C, chociaż SSL Labs uważa za sprawne tylko z ocenami A i B. Wtedy z danych badania wynika, że 45 sklepów posiada sprawny certyfikat SSL, a tylko 5 – nie. Na rysynku 4.19 przedstawiony jest procentowy podział wyników.

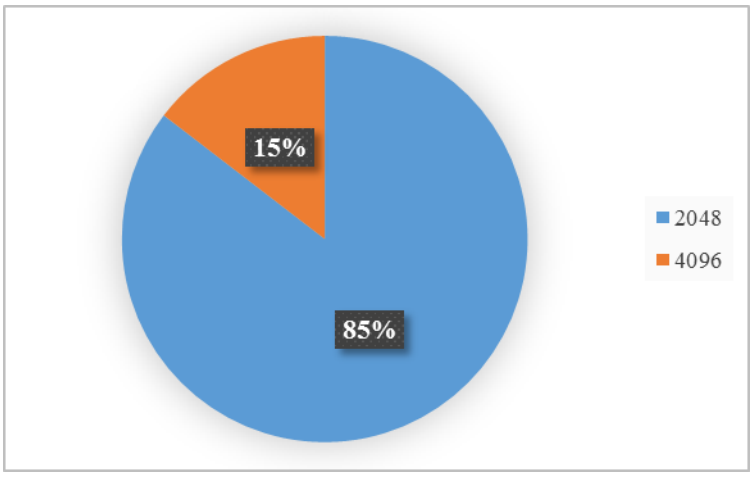
Rysunek 4.19. Procent posiadania sprawnych i niesprawnych certyfikatów SSL



Zródło: opracowanie własne

Standardową długość klucza (2048 bit) ma 41 sklepów internetowych, a długość klucza powyżej 4096 bit tylko 7 sklepów. Jak mówiliśmy wcześniej, im więcej bitów ma klucz, tym trudniej go złamać. Na rysunku 4.20 przedstawimy procentowe statystyki długości kluczu.

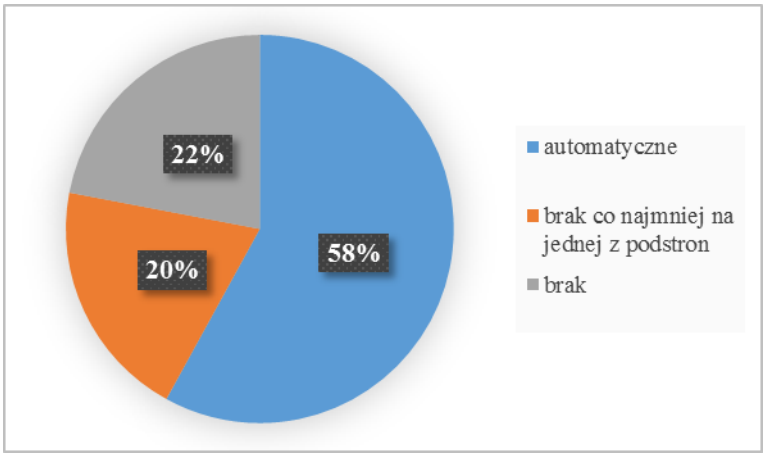
Rysunek 4.20. Podział polskich sklepów internetowych za długością kluczy



Zródło: Opracowanie własne

Sprawdziliśmy posiadanie automatycznego przekierowania na bezpieczny tryb https:// na stronach rejestracji, logowania i wypełnienia danych osobowych przy zamówieniu. Mieliśmy tu trzy kategorie – „tak" - przekierowanie nastąpiło i działa sprawny certyfikat, „tak*" – przekierowanie nastąpiło i jest certyfikat, ale są inne czynniki, które nie pozwalają na bezpieczną transmisję lub brak przekierownaia na jedną lub więcej podstron i „nie" – brak przekierowania. Za wynikami badania 29 sklepów ma bezpieczną transmisję danych, 10 - ma prawie bezpieczną transmisję i 11 sklepów nie posiada przekierowania w tryb bezpieczny. Na rysunku 4.21 przedstawimy procentowy podział wyników badania:

Rysunek 4.21. Procentowy podział posiadania certyfikatu SSL na stronach poufnych



Zródło: Opracowanie własne

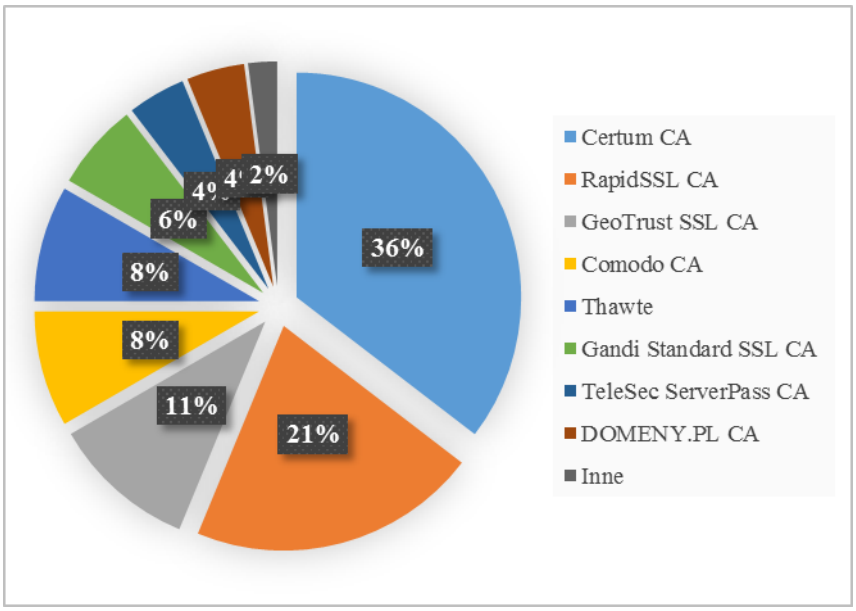
Każdy z przeanalizowanych sklepów w wyszukiwarce SSL Labs również miał wpis w Centrum Certyfikacji. Za godne zaufania centrum certyfikacji uważamy to, które na postawie

nadanych dokumentów niezależnie i obiektywnie sprawdza tożzamość danej firmy. Najczęściej wybieranymi centrumami certyfikacji w naszym badaniu są następujące:

1. Certum CA – 17;
2. RapidSSL CA – 10;
3. GeoTrust CA – 5;
4. Comodo CA – 4;
5. Thawte – 4;
6. Gandi Standard CA – 3;
7. TeleSec CA – 2;
8. Domeny.pl – 2;
9. Inne -1.

Jak widać większa część sklepów preferuję korzystanie z usług centrów certyfikacji w Polsce (Cenrtum CA) i UK (RapidSSL CA). Na rysunku 4.22 pokazane są procentowe udziały wyboru centrum certyfikacyjnych przez polskie sklepy.

Rysunek 4.22. Procentowy udział wybieranych centrum certyfikacyjnych przez polskie sklepy



Zródło: Opracowanie własne

Przeanalizowaliśmy w jakim sektorze znajdują się najbezpieczniejsze sklepy. Najlepszą kategorią okazała się kategoria „Sklepy specjalistyczne”. 7 sklepów z tej kategorii mają ocenę certyfikatów bezpieczeństwa A lub B.

4. Podsumowanie

Polski rynek e-commerce rozwija się bardzo dynamicznie. Z wielu badań, prowadzonych przez różne agencje nie wynika, że użytkownicy Internetu czują siebie bezpiecznie. Oczywiście jeżeli chodzi o bezpieczeństwio w Internecie, to tu większość zależy od użytkownika, na jakich stronach przebywa, jakie pliki pobiera, czy ma na komputerze program antywirusowy i inne czynniki. Ale w przypadku sklepów internetowych, to odpowiedzialność leży na właścicielu sklepu, bo on sam musi dbać o bezpieczeństwo transmisji i bezpieczne przechowywanie danych osobowych. Prowadzone badanie pokazało, że znaczna część sklepów (90%) chroni swoich użytkowników. Problemem nadal są niskie oceny certyfikatów, lub nieważność certyfikatów na niektórych stronach, chociaż było wybrane 50 najpopularnejszych sklepów, z których korzysta większość polaków.

85% sklepów mają standardową dlugość klucza (2048 bitów), ale są jeszcze lepsze standardy, na przykład długość 4096 bitów, jaką posiadają 15% sklepów. Jedynie 58% sklepów ma automatyczne przekierowanie stron poufnych (a same strony rejestracji, logowania do serwisu i strona wysyłania danych do zamówienia) na tryb bezpieczny https://.

Ogólnie sytuacja wygląda dobrze, ale jeżeli chodzi o badane sklepy, to były wybrane jak najbardziej zaufane przez konsumentów, dlatego moim zdaniem powinny posiadać najlepsze standardy bezpieczeństwa dla zachowania zaufania swoich klientów.

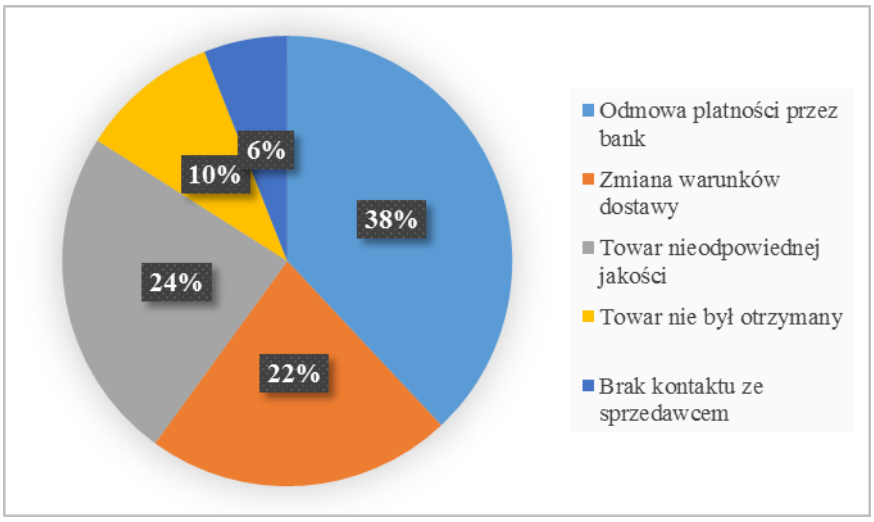
4.2.3. Ocena bezpieczeństwa technologicznego handlu elektronicznego w Ukrainie

1. Ocena bezpieczeństwa według konsumentów

Zakupy w Internecie stały się popularne 3-4 lata temu i na dzień dzisiejszy tylko 14% użytkowników Internetu w Ukrainie regularnie kupuje w Internecie. Należy zwrócić uwagę, że najczęściej Ukraińcy kupują towary AGD, RTV, komputery, telefony komórkowe, innymi słowy kupują rzadko. Za danymi strony price.ua[97] zakupy w Internecie za bezpieczne uważa tylko 8% badanych. Taka mała liczba wynika z faktu, że większość (47%) użytkowników miało problem z płatnością, dostawą towaru, jakością kupionego towaru. Czasopismo internetowe „Internet w liczbach" przedstawia takie statystyki problemów, powstających w sieci przy zakupach (rysunek 4.23):

[97] *Ocena bezpieczeństwa sklepów internetowych w Ukrainie,* http://price.ua/index/firms.html [dostęp: 12.04.2015]

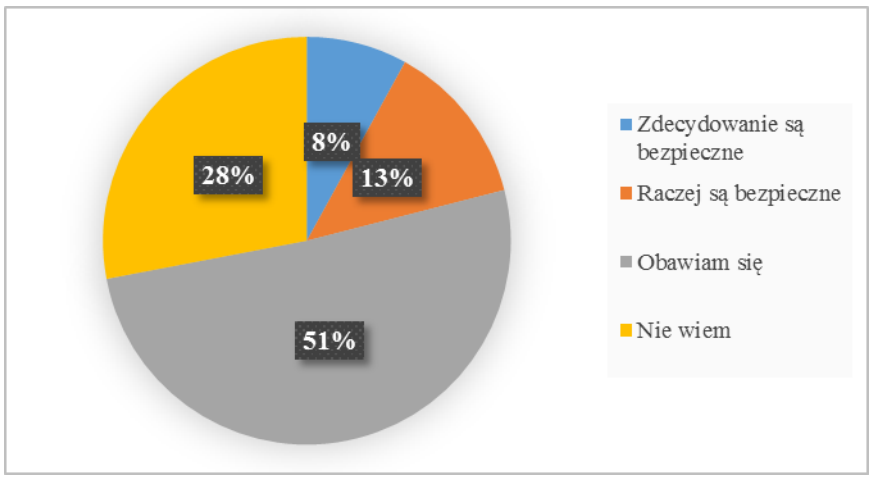
Rysunek 4.23. Statystyka najczęściej występujących problemów przy zakupach



Zródło: Opracowanie własne na podstawie http://price.ua/index/firms.html [dostęp: 12.04.2015]

Na rysunku 4.24. przedstawimy statystyki bezpieczeństwa zakupów według strony prom.ua. Ze statystyk wynika że 51% ukraińskich konsumentów obawia się robić zakupy w Internecie, i tylko 8% użytkowników Internetu uważa zakupy w sieci za bezpieczne.

Rysunek 4.24. Statystyka opinii konsumentów według bezpieczeństwa zakupów w Internecie



Zródło: Opracowanie własne na podstawie http://price.ua/index/firms.html [dostęp: 12.04.2015]

Również serwis price.ua podaje takie dane z badań „Co waszym zdaniem jest najważniejsze przy zakupach w Internecie?". 83% konsumentów wybrało opcję „bezpieczeństwo transakcji", dla 78% - „możliwość wyboru różnych form płatności", 54% zaznaczyło opcję szybkiej dostawy. Inne czynniki, które wpływają na decyzję kupna w Internecie – to cena, jakość towaru, łatwa obsługa sklepu.

2.Wyniki badania

W rozdziale 4.1. wybraliśmy 50 największych sklepów internetowych w Ukrainie z uwagi na rózne kategorie. Prowadzyliśmy badania na posiadanie certyfikatu SSL, jego długość, jakość i automatyczne przekierowanie na tryb bezpieczny na stronach rejestracji, logowania do serwisu i składania zamówienia. Wyniki badania rynku przedstawimy w tabeli 4.9.

Tabela 4.9. Wyniki badania bezpieczeństwa 50 sklepów elektronicznych w Ukrainie

Kategoria	*Sklep*	*Ocena certyfikatu SSL*	*Klucz szyfrowania*	*Data ważności certyfikatu*	*Https://*	*Centrum autoryzacji*
Elektronika i AGD	rozetka.com.ua	B	2048	ważny	tak	RapidSSL SHA256 CA
	allo.ua	B	2048	ważny	nie	COMODO Extended Validation Secure Server CA
	fotos.ua	F	1024	ważny	nie	self-signed
	foxtrot.com.ua	no connect			nie	
	mobilluck.ua	missmutch			nie	
	comfy.ua	B	2048	ważny	nie	COMODO Extended Validation Secure Server CA
	citrus.ua	B	2048	ważny	tak	RapidSSL SHA256 CA
	eldorado.com.ua	T	no	no	nie	no
	fotomag.com.ua	No secure protocols supported			nie	
	sokol.ua	C	2048	ważny	nie	GeoTrust SSL CA
Zdrowie i uroda	beauty-life.com.ua	B	2048	wazny	nie	RapidSSL SHA256 CA
	avon.com.ua	F	2048	ważny	tak	Equifax / Equifax Secure Certificate Authority
	parfumeria.ua	B	2048	ważny	nie	thawte DV SSL CA - G2

	eva.dp.ua	F	2048	ważny	nie	RapidSSL SHA256 CA
	enjee.ua	no connect			nie	
	watsons.com.ua	B	2048	wa zny	nie	thawte DV SSL CA - G2
	ua.oriflame.com	C	2048	ważny	nie	GeoTrust SSL CA
	makeup.com.ua	A	2048	ważny	nie	COMODO RSA Domain Validation Secure Server CA
	cosmetic.com.ua	No secure protocols supported			nie	
	beautystore.com.ua	no connect			nie	
Kultura i rozrywka	bukva.ua	No secure protocols supported			nie	
	yakaboo.ua	C	2048	ważny	nie	GeoTrust SSL CA
	nashformat.ua	missmatch				
	bookclub.ua	T	2048	ważny	nie	Thawte DV SSL CA
	librabook.com.ua	T	2048	ważny	nie	Thawte DV SSL CA
	bookzone.com.ua	F	2048	ważny	nie	GeoTrust Extended Validation SSL CA - G2
	petrovka.ua	no connect			nie	
	knigoland.com.ua	missmatch			nie	
	knigka.ua	no connect			nie	
	book-mania.com.ua	T	no	no	nie	
Moda	bonprix.ua	A	2048	ważny	tak	thawte SSL CA - G2
	leboutique.com.ua	C	2048	ważny	tak	Go Daddy Secure Certificate Authority - G2
	modnakasta.ua	F	2048	ważny	nie	GeoTrust Extended Validation SSL CA - G2
	lamoda.ua	A	2048	ważny	nie	RU-CENTER High Assurance Services CA
	shopnow.com.ua	B	2048	ważny	nie	COMODO RSA

						Extended Validation Secure Server CA
	shopart.ua	B	2048	ważny	tak	COMODO RSA Extended Validation Secure Server CA
	helen-marlen.ua	C	4096	ważny	tak	COMODO RSA Extended Validation Secure Server CA
	stylepit.ua	C	2048	ważny	nie	COMODO RSA Domain Validation Secure Server CA
	www.witt-international.ua	F	2048	ważny	nie	WebSpace-Forum Server CA
	fame.ua	no connect			nie	
Sklepy specjalistyczne	e-esco.com.ua	F	2048	ważny	nie	GeoTrust SSL CA - G3
	winauto.ua	C	2048	ważny	nie	COMODO RSA Domain Validation Secure Server CA
	aqua-club.com.ua	B	2048	ważny	tak	COMODO RSA Domain Validation Secure Server CA
	autobazar.ua	T	2048	nieważny	nie	Go Daddy Secure Certification Authority
	rst.ua	F	2048	ważny	nie	Go Daddy Secure Certificate Authority - G2
	auto.ria.ua	F	2048	ważny	nie	Go Daddy Secure Certificate Authority - G2
	infocar.ua	C	2048	ważny	nie	COMODO RSA Domain Validation Secure

						Server CA
	olx.ua	A	2048	ważny	tak	thawte EV SSL CA - G2
	agromat.ua	F	2048	ważny	nie	Go Daddy Secure Certificate Authority - G2
	prom.ua	A	2048	ważny	tak	thawte EV SSL CA - G2

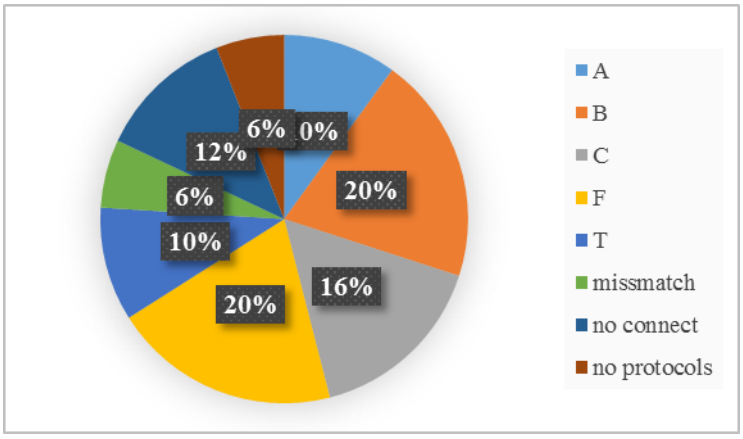
Zródło: Opracowanie własne

2. Objaśnienie wyników

Jak w badaniu polskich sklepów, ukraińskie sklepy również zostały przeanalizowane za pomocą narzędzia SSL Labs, CertyfikatySSL.pl i SSL4Less.ru. W razie braku dostępu do strony przez narzędzie SSL Labs, przprowadziliśmy analizę strony następnego dzień. Wszystkie strony sprawdziliśmy ręcznie na przedmiot posiadania przekierowania na tryb bezpieczny stron logowania, rejestracji i wysyłania zamówień do serwera.

Z przeanalizowanych 50 sklepów najwyższą ocenę certyfikatów (A>80%) ma tylko 5 sklepów. Oceny B i C otrzymało odpowiednio 10 i 8 sklepów. Najgorszą ocene certyfikatu (F) otrzymało 10 sklepów, a ocenę T (niezaufany certyfikat) ma 5 sklepów. Nie udało się w żaden sposób sprawdzić certyfikatów dla 5 sklepów, brak połączenia z domeną (missmatch) ma 3 sklepy. Żadnego certyfikatu bezpieczeństwa nie mają 3 sklepy. Ważny certyfikat bezpieczeństwa ma 31 sklepów, 1 ma nieważny certyfikat. Procentowe statystyki podziału ocen certyfikatów podamy na rysunku 4.25.

Rysunek 4.25. Procentowy podział ocen bezpieczeństwa sertyfikatów SSL ukraińskich sklepów

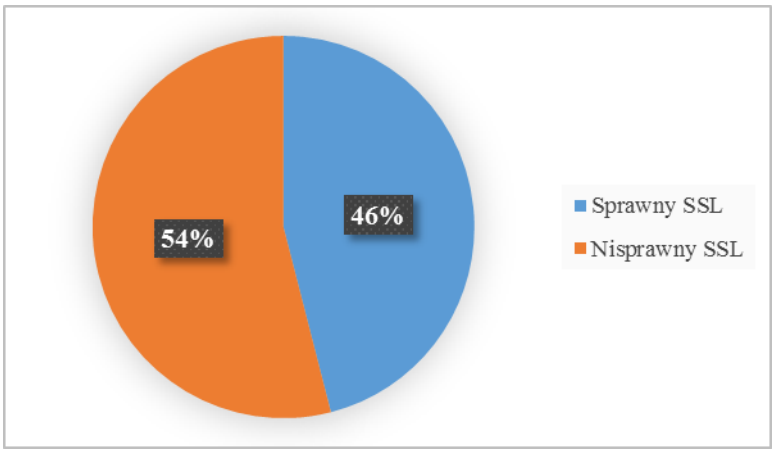


Zródło: Opracowanie własne

W naszym badaniu za sprawne certyfikaty uznajemy te, które mają ocenę A, B lub C. Wtedy z otrzymanych danych badania ukraińskiego segmentu e-handlu wynika, że 23 sklepy posiadają sprawny certyfikat SSL, a 27 - ma niesprawny certyfikat.

Na rysynku 4.26 przedstawiony jest procentowy podział wyników ilości sprawnych i niesprawnych certyfikatów, posiadanych przez ukraińskie sklepy internetowe.

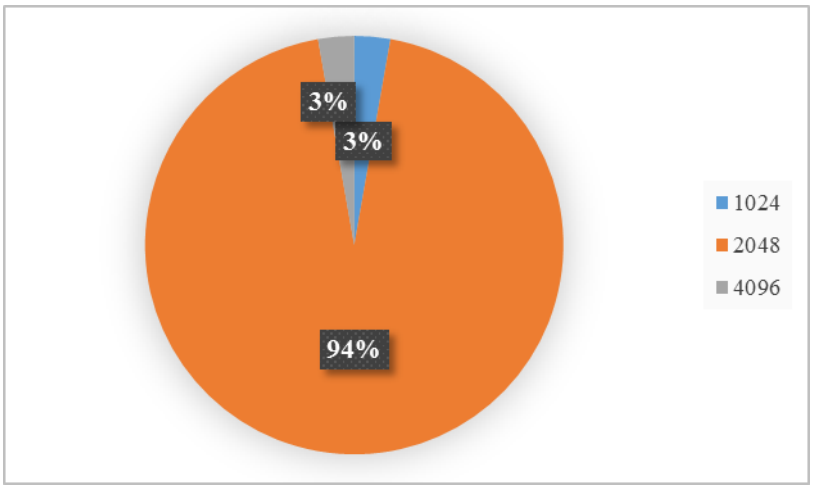
Rysunek 4.26. Procent posiadania sprawnych i niesprawnych certyfikatów SSL



Zródło: Opracowanie własne

Jak omówiono wcześniej, standardową długością klucza jest 2048 bit. Za wynikami badania wśród ukraińskich sklepów internetowych jeden sklep ma długość klucza 1024 bit i również jeden ma 4096 bit. Pozostale 34 sklepy mają standardową długość kluczy. Na rysunku 4.27 przedstawimy procentowe statystyki długości kluczu.

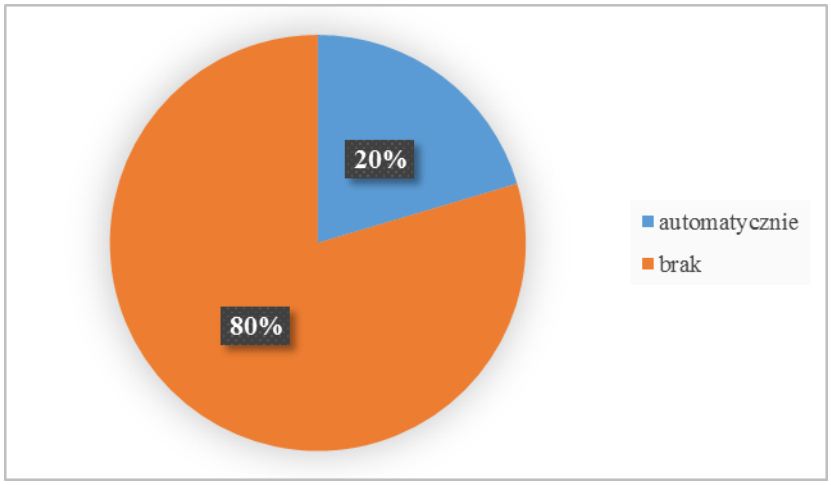
Rysunek 4.27. Podział ukraińskich sklepów internetowych za długością kluczy



Zródło: Opracowanie własne

Na stronach rejestracji, logowania i wysyłania zamówienia automatycznie przekierowanie są na tryb bezpieczny https:// ma jedynie 10 stron ukraińskich sklepów internetowych, przeważająca ilość (34 sklepy) nie posiada takiego przekierowania. Na rysunku 4.28 przedstawimy procentowy podział wyników badania:

Rysunek 4.28. Procentowy podział posiadania certyfikatu SSL na stronach poufnych



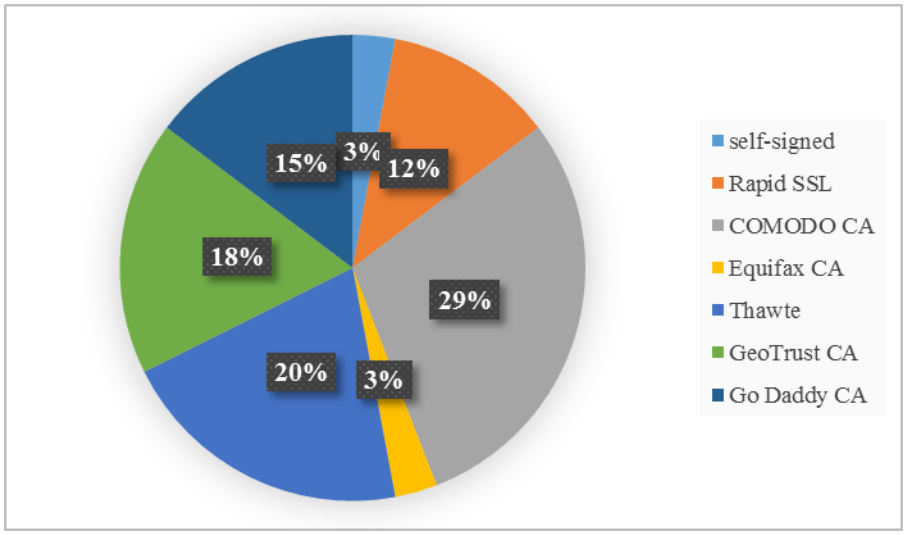
Zródło: Opracowanie własne

W wyszukiwarce SSL Labs w wynikach analizy również jest podana informacja o centrum autoryzacji, który ten certyfikat wydał. Najczęściej wybieranymi centrumami certyfikacji w naszym badaniu są następujące:

1. Comodo CA – 10;
2. Thawte – 7;
3. GeoTrust CA – 6;
4. Go Daddy CA – 4;
5. Rapid SSL – 4;
6. Equifax -1.

Ze statystyk wynika, że większa część ukraińskich sklepów internetowych korzysta z centrum autoryzacji Comodo CA. Jeden sklep został podpisany przez siebie (self-signed). Na rysunku 4.29 pokazane są procentowe udziały wyboru centrów certyfikacyjnych przez polskie sklepy.

Rysunek 4.29. Procentowy udział wybieranych centrum certyfikacyjnych przez polskie sklepy



Zródło: Opracowanie własne

Przeanalizowaliśmy w jakiej kategorii znajdują się najbezpieczniejsze sklepy. Najlepszą kategorią według naszych statystyk stała się kategoria „Moda". 5 sklepów z tej kategorii ma ocenę certyfikatów bezpieczeństwa A lub B.

3. Podsumowanie

Ukraiński rynek e-commerce rozwija się z mniejszym tempie niż rynki e-commerce rozwiętych krajów. Zakupom w Internecie nie ufa prawie 51% użytkowników Internetu w Ukrainie. Z wyników badania, które przeprowadziliśmy dla ceny bezpieczeństwa ukraińskich sklepów internetowych, wynika że konsumenci maja wszystkie podstawy dla braku zaufania. Dla analizy wybraliśmy 10 najpopularniejszych sklepów internetowych w pięciu kategoriach. Z tych pięćdziesięciu sklepów tylko 31 ma ważne certyfikaty bezpieczeństwa,
i tylko 23 z nich posiada sprawne certyfikaty, co stanowi mniej niż polowę wszystkich badanych sklepów. 80% procent ukraińskich sklepów internetowych nie ma przekierowania na tryb bezpieczny na stronach, gdzie użytkownik wpisuje poufne informacji. Nistety są sklepy, które nie posiadają nawet standardowej długości kluczu w 2048 bit, chociaż większość ma taką długość kluczy i nawet jeden sklep ma długość klucza w 4096 bit.

Niestety sytuacja wygląda w nienajlepszy sposób, ponieważ takie złe zabezpieczenie rozwiązuje ręce cyberprzestępcom. Właściciele sklepów również powinni rozumieć, że

nieposiadanie żadnych zabezpieczeń stanowi zagrożenie nie tylko dla użytkowników, ale również dla biznesu.

4.3. Ocena bezpieczeństwa prawnego handlu elektronicznego

4.3.1. Metodologia badania.

W naszym badaniu bezpieczeństwa prawnego postanowiono zbadać czy sklepy internetowe posiadają politykę prywatności i regulamin na swojej stronie, czy jest on dostępny użytkownikowi, czy go treść odpowiada normom prawnym, obowiązującym w kraju.

Postanowiliśmy ocenić jakość regulaminu sklepu w taki sposób (tabela 4.10).

Tabela 4.10. Ocena jakości regulaminu sklepu internetowego

Kryterium	Ocena
Brak regulaminu	0
Regulamin umieszczony na stronie, ale nie posiada wszystkich niezbędnych informacji zgodnie z obowiązującymi normami prawa	1
Regulamin umieszczony na stronie, posiada wszystkie niezbędne krótkie informacje zgodnie z obowiązującymi normami prawa	2
Regulamin umieszczony na stronie, posiada wszystkie niezbędne i pełne informacje zgodnie z obowiązującymi normami prawa	3

Zródło: Opracowanie własne

Podstawowymi elementami regulaminu, o którym pisaliśmy w rozdziale 3 są:

1. Postanowienia ogólne.
2. Definicje.
3. Warunki zawierania umowy.
4. Płatności.
5. Realizacja umowy.
6. Gwarancja i postępowania reklamacyjne.
7. Odstąpienie lub rozwiązanie umowy.
8. Ochrona danych osobowych.
9. Postanowienia końcowe.

Różnice i reguły napisania regulaminu sklepów internetowych w Ukrainie i Polsce będą omówione dalej.

Co do polityki prywatności nie ma ogólnych międzynarodowych norm i szablonów, dlatego ocenialiśmy posiadanie lub brak polityki prywatności na stronie sklepu.

4.3.2. Ocena bezpieczeństwa prawngo handlu elektronicznego w Polsce

1. Normy prawne dotyczące handlu elektronicznego

Polskie akty prawne, które mają największy wpływ na funkcjonowanie handlu elektronicznego są następujące:

1. Ustawa o świadczeniu usług drogą elektroniczną (UŚUDE),
2. Ustawa o ochronie danych osobowych (UODO),
3. Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
4. Ustawa o ochronie praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny,
5. Ustawa o szczególnych warunkach sprzedaży konsumenckiej,
6. Kodeks cywilny,
7. Ustawa o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym,
8. Ustawa o ochronie baz danych,
9. Ustawa o podpisie elektronicznym,
10. Ustawa o świadczeniu usług na terytorium Rzeczypospolitej Polskiej[98].

Ustawa, która najbardziej wpływa na biznes, prowadzony przez Internet, to UŚUDE. Określenie świadczenia usługi drogą elektroniczną zostało zdefiniowane w art. 2 pkt 4. UŚUDE i wygląda tak: wykonanie usługi świadczonej bez jednocześnie obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową,
i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia lipca 2004 r. – Prawo

[98] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.22.

telekomunikacyjne. UŚUDE reguluje świadczenie usług we wszystkich modelach e-commerce (B2C, B2B,C2C, A2A).

Dla sklepów internetowych wynika z nią obowiązek przygotowywania regulaminu (art.8):

1. Usługodawca:

a. Określa regulamin świadczenia usług drogą elektroniczną, zwany dalej „regulaminem"

b. Nieodpłatnie udostępnia usługobiorcy regulamin przed zawarciem umowy o świadczenie takich usług, a także – na jego żądanie – w taki sposób, który umożliwia pozyskanie, odtwarzanie i utrwalenie treści regulaminu za pomocą systemu teleinformatycznego, którym posługuje się usługobiorca.

Usługodawcą jest prowadzący system, a usługobiorcą, co wydaje się oczywiste, klient czy raczej użytkownik systemu. UŚUDE nakazuje każdemu podmiotowi, świadczącemu usługi drogą elektroniczną sporządzić regulamin, brak regulaminu może prowadzić do odpowiedzialności karnej. Przy stworzeniu regulaminu należy pamiętać o obostrzeniu prawnym, które wynika z art.8 ust. 2 UŚUDE zgodnie z którym usługobiorca nie jest związany tymi postanowieniami regulaminu, które nie zostały mu nieodpłatnie udostępnione przez usługodawcę przed zawarciem umowy. Regulamin zgodnie z prawem należy udostępniać na żądanie w sposób, który umożliwia pozyskanie, odtwarzanie i utrwalenie treści.

Regulamin zgodnie z art.8 ust 3. określa co najmniej:

1. Rodzaje i zakres usług, świadczonych drogą elektroniczną,

2. Warunki świadczenia usług drogą elektroniczną, między innym:

a. wymagania techniczne niezbędne do współpracy z systemem teleinformatycznym, którym posługuję się usługodawca.

b. zakres dostarczania przez usługobiorcę treści o charakterze bezprawnym.

3. Warunki podpisania i rozwiązywania umów o świadczenie usług drogą elektroniczną.

4. Tryb postępowania reklamacyjnego.

Przy stworzeniu regulaminu należy uważać na niedozwolone zapisy w umowie, które definiuje Kodeks cywilny w art.385:

1. Zapisy, które wyłączają lub w znaczny sposób ograniczają odpowiedzialność względem konsumenta za niewykonane lub nienależne wykonanie zobowiązania.
2. Zapisy, które wyłączają obowiązek zwrotu konsumentowi uiszczonej zapłaty za świadczenie, niewykonane w całości lub częściowe, jeżeli konsument zrezygnuje z zamówienia.
3. Zapisy, które pozbawiają konsumenta do uprawnienia do rozwiązania umowy, odstąpienia od niej lub jej wypowiedzenia.
4. Zapisy, które przewidują obowiązek wykonania zobowiązania przez konsumenta mimo niewykonania lub częściowego wykonania usługi.
5. Zapisy, które wyłączają jurysdykcję sądów polskich lub poddają sprawę pod rozstrzygnięcie sądu polubownego polskiego lub zagranicznego albo innego organu.

Sąd Ochrony Konkurencji i Konsumentów może uznać w regulaminie taki zapis niedozwolonym i wtedy on nie wiąże konsumenta.

Przy prowadzeniu handlu przez Internet jest niezbędne przetwarzanie danych osobowych osób fizycznych, które reguluje Ustawa o ochronie danych osobowych (UODO). Przy zbieraniu danych osobowych od osób fizycznych sklep internetowy musi spełnić obowiązek informacyjny, który wynika z art.24 ust. 1 UODO. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator bazy danych osobowych jest zobowiązany poinformować tą osobę o:

1. Adresie swojej siedziby i pełnej nazwie (w przypadku osoby fizycznej to imię, nazwisko i miejsce zamieszkania).
2. Celu zbierania danych;
3. Prawie dostępu do treści swoich danych oraz ich poprawiania;
4. Dobrowolności lub obowiązku podania danych (również należy zaznaczyć podstawę prawną).

Często obowiązek informacyjny jest spełniany w ramach uzyskania zgody na przetwarzanie danych osobowych przy rejestracji nowego użytkownika lub składaniu zamówienia. Ogólne zasady przechowywania danych osobowych sklep internetowy musi rozmieszczać na swojej stronie na podstronie „Polityka prywatności”[99].

2. Wyniki badania

[99] L.Kępa, P.Tomasik, S.Dobrzyński, *Bezpieczeństwo systemu e-commerce*, Helion 2012, s.26.

Przeprowadziliśmy badanie 50 największych i najpopularniejszych sklepów internetowych na temat posiadania polityki prywatności, regulaminu, jakości jego treści. Zgodnie z wynikami badania regulamin umieszczony jest na stronie 48 z 50 sklepów. Jeżeli chodzi o jakość treści, to była również wzięta pod uwagę ostatnia aktualizacja treści, ponieważ od 25.12.2014 roku w Polsce obowiązują nowe zasady. Jeżeli ostatnia aktualizacja regulaminu była przed 25.12.2014r., to nadawaliśmy takiemu sklepu ocenę 1. Pozostałe oceny są wystawione zgodnie metodologii badania w 4.3.1. Ogólne oceny są w tabeli 4.11.

Tabela 4.11. Wyniki oceny regulaminów polskich sklepów internetowych

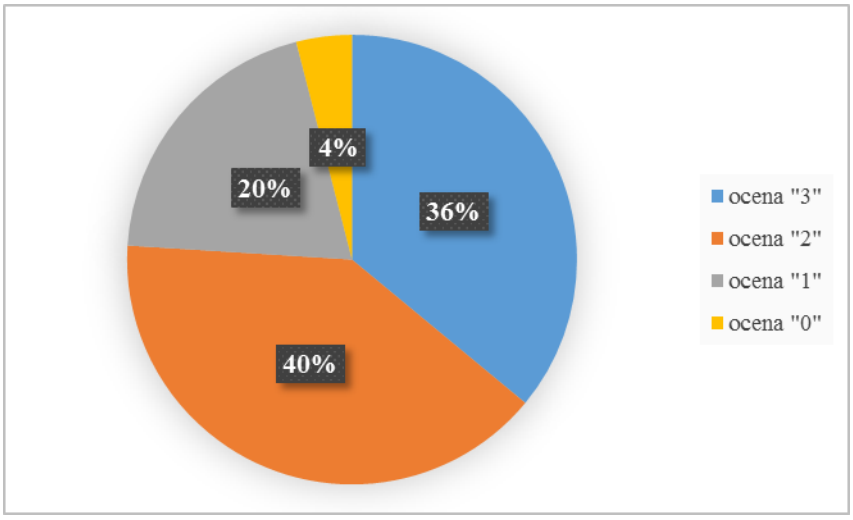
Kategoria	Elektronika i AGD				
Sklep	komputronik.pl	mediamarkt.pl	saturn.pl	euro.com.pl	redcoon.pl
Ocena regulaminu	2	3	3	3	3
Sklep	electro.pl	morele.net	oleole.pl	neo24.pl	agito.pl
Ocena regulaminu	2	2	3	2	1
Kategoria	Zdrowie i uroda				
Sklep	perfumeria.pl	iperfumy.pl	i-apteka.pl	tanie-leczenie.pl	apteka-melissa.pl
Ocena regulaminu	2	1	1	1	1
Sklep	aptekaslonik.pl	cefarm24.pl	aptekagemini.pl	yves-rocher.pl	doz.pl
Ocena regulaminu	1	2	2	3	2
Kategoria	Kultura i rozrywka				
Sklep	matras.pl	merlin.pl	gandalf.com.pl	empik.com	helion.pl
Ocena regulaminu	3	2	2	3	2
Sklep	taniaksiazka.pl	ravelo.pl	inbook.pl	bonito.pl	pwn.pl
Ocena regulaminu	3	3	2	1	3
Kategoria	Moda				
Sklep	eobuwie.com.pl	zalando.pl	czasnabuty.pl	sarenza.pl	answear.com
Ocena regulaminu	3	3	2	3	2
Sklep	bonprix.pl	deichmann.com	topsecret.pl	sizeer.com	spartoo.pl
Ocena regulaminu	0	2	2	0	2
Kategoria	Sklepy specjalistyczne				
Sklep	selgros24.pl	dom-ogrod.com	bdsklep.pl	rockmetalshop.pl	leroymerlin.pl
Ocena	3	1	3	1	3

regulaminu					
Sklep	smyk.com	chocolissimo.pl	motointegrator.pl	muve.pl	endo.pl
Ocena regulaminu	3	2	1	2	2

Zródło: Opracowanie własne

Jak wynika z tabeli 18 sklepów maj pełnie i szczególnie uzupełniony regulamin, 20 sklepów ma regulaminy, odpowiadające normom polskiego prawa, 10 sklepów ma źle uzupełniony lub nieaktualizowany regulamin. 2 sklepy nie mają regulaminu, umieszczonego na swojej stronie. Na rysunku 4.30 przedstawimy procentowy podział wyników badania.

Rysunek 4.30. Procentowy podział wyników analizy regulaminów polskich sklepów internetowych



Zródło: Opracowanie własne

Z wykresu wynika, że 76% polskich sklepów internetowych mają regulaminy, odpowiadające normom polskiego prawa.

W tabeli 4.12 są przedstawione wyniki badania o posiadaniu przez sklep polityki prywatności.

Tabela 4.12. Wyniki badania posiadania polityki prywatności przez polskie sklepy internetowe

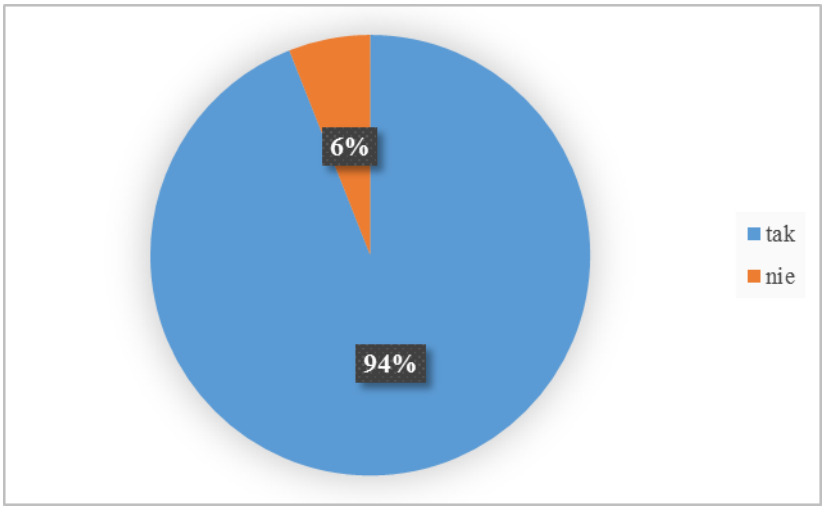
Kategoria	Elektronika i AGD				
Sklep	komputronik.pl	mediamarkt.pl	saturn.pl	euro.com.pl	redcoon.pl
Polityka prywatności	tak	tak	tak	tak	tak
Sklep	electro.pl	morele.net	oleole.pl	neo24.pl	agito.pl

Polityka prywatności	nie	tak	tak	tak	tak
Kategoria	Zdrowie i uroda				
Sklep	perfumeria.pl	iperfumy.pl	i-apteka.pl	tanie-leczenie.pl	apteka-melissa.pl
Polityka prywatności	tak	tak	nie	tak	tak
Sklep	aptekaslonik.pl	cefarm24.pl	aptekagemini.pl	yves-rocher.pl	doz.pl
Polityka prywatności	tak	tak	tak	tak	tak
Kategoria	Kultura i rozrywka				
Sklep	matras.pl	merlin.pl	gandalf.com.pl	empik.com	helion.pl
Polityka prywatności	tak	tak	tak	tak	tak
Sklep	taniaksiazka.pl	ravelo.pl	inbook.pl	bonito.pl	pwn.pl
Polityka prywatności	tak	tak	tak	tak	tak
Kategoria	Moda				
Sklep	eobuwie.com.pl	zalando.pl	czasnabuty.pl	sarenza.pl	answear.com
Polityka prywatności	tak	tak	tak	tak	tak
Sklep	bonprix.pl	deichmann.com	topsecret.pl	sizeer.com	spartoo.pl
Polityka prywatności	tak	tak	tak	nie	tak
Kategoria	Sklepy specjalistyczne				
Sklep	selgros24.pl	dom-ogrod.com	bdsklep.pl	rockmetalshop.pl	leroymerlin.pl
Polityka prywatności	tak	tak	tak	tak	tak
Sklep	smyk.com	chocolissimo.pl	motointegrator.pl	muve.pl	endo.pl
Polityka prywatności	tak	tak	tak	tak	tak

Zródło: Opracowanie własne

Z wyżej podanych danych wynika, że 47 sklepów ma umieszczone na swojej stronie politykę prywatności i jedynie 3 sklepy nie ma. Procentowy podział wyników przedstawimy na rysunku 4.31.

Rysunek 4.31. Procentowy podział analizy posiadania polityki prywatności na stronie internetowej sklepu w Polsce.



Zródło: Opracowanie własne

Podsumowując, polskie sklepy internetowe są zabezpieczone prawne, ponieważ więcej niż 90% sklepów mają umieszczaną na swojej stronie regulamin sklepu i politykę prywatności. Należy również sklepom zwracać uwagę na aktualizację norm prawnych w kraju i w czas robić zmiany w regulaminach i umowach, ponieważ to pozwoli w przyszlości uniknąć odszkodowań i problemów. Właściciele sklepów powinni rozumieć, im szczególnie napisany jest regulamin, tym więcej zaufania ma on u konsumentów i tym więcej niezbędnej informacji może znaleść w nim użytkownik.

4.3.3. Ocena bezpieczeństwa prawnego handlu elektronicznego w Ukrainie

1. Normy prawne, regulujące handel elektroniczny.

Regulacja prawna handlu elektronicznego w Ukrainie znajduje się na początkowym stadium rozwoju.

Do obecnych ustaw, które regulują działalność gospodarczą w Internecie w Ukrainie odnoszą się:

1. Ustawa od 2 października 1992r. „O informacji", która opisuje ogólne zasady otrzymania, stosowania, przesyłania i przechowywania informacji, określa status uczestników relacji informacyjnych, reguluje dostęp do informacji i jej ochronę.
2. Ustawa „O związku sieci teleinformatycznych" określa prawne, ekonomiczne, organizacyjne zasady działalności w dziedzinie związku w Ukrainie.
3. Ustawa „O systemach płatniczych i podpis elektroniczny" od 5 kwietnia 2001 r. określa ogólne zasady funkcjonowania systemów płatniczych w Ukrainie. W art.2. podano

definicje dokumentu elektronicznego i podpisu elektronicznego. Jest określone, iż dokument elektroniczny ma taką samą siłę, co i dokument papierowy, a podpis elektroniczny jest równoznaczny podpisowi zwykłemu. Artykuł 19 tej ustawy określa reguły i terminy przechowywania, usunięcia dokumentów elektronicznych. Ta ustawa jest pierwszym i jedynym dokumentem w Ukrainie, który określił dokładną prawną definicję dokumentu elektronicznego i podpisu elektronicznego.

4. Ustawa od 22 maja 2003 r. „O podpisie elektronicznym" reguluje oddzielny obszar relacji, dotyczących handlu elektronicznego, a szczególnie użycia podpisu elektronicznego. W tej ustawie jest dokładnie określony algorytm otrzymania podpisu elektronicznego, lista niezbędnych dokumentów, prawach i obowiązkach centrów autoryzacyjnych itd.

5. Postanowienie „ Procedura kryptograficznego bezpieczeństwa informacji w Ukrainie", podpisane przez prezydenta Ukrainy 22 maja 1998 r., które reguluje kryptograficzne bezpieczeństwo, jak i sposób bezpieczeństwa, który jest realizowany za pomocą przetwarzania informacji przy użyciu specjalnych kluczy. Państwową politykę, co do bezpieczeństwa kryptograficznego kontroluje Dział ochrony komunikacji specjalnej przy Państwowym Urzędzie Bezpieczeństwa Wewnętrznego.

6. Postanowienie „O dziale ochrony komunikacji specjalnej i bezpieczeństwa informacji" z 6 października 2000 r. W tym postanowieniu zaznaczono, że Dział ochrony komunikacji specjalnej i bezpieczeństwa informacji jest organem administracji państwowej, który działa w ramach Państwowego Urzędu Bezpieczeństwa Wewnętrznego.

7. Rozporządzenie Prezydenta Ukrainy z dnia 31 lipca 2000 r. "O rozwoju państwowej globalnej sieci informacyjnej Internet", postanawia zabezpieczyć wolny i szeroki dostęp do Internetu obywatelom Ukrainy i przedsiębiorstwom.

8. Ustawa od dnia 6 czerwca 2012 roku „O ochronie danych osobowych", która określa zasady zbierania, przetwarzania i przechowywania danych osobowych. W art. 6 również jest wspomnienie o niezbędności ochrony danych osobowych w Internecie i stworzenia polityki prywatności dla każdego podmiotu gospodarczego[100].

Jak wynika z powyżej zaznaczonych dokumentów, na dzień obecny w Ukrainie nie ma ustawy, która określałaby regulacje handlowe w Internecie. O potrzebie stworzenia takiego dokumentu mówi się już od kilku lat, nawet były podane projekty do Sejmu, ale żaden dokument nie był zaakceptowany.

[100] A.V.Chuchkovska, *Regulacja prawna handlu elektronicznego w Ukrainie,* Kyivski Uniwersytet Narodowy, Kyiv, 2007, s.27-42

W nowym dodatku ustawy „O informacji" z 13 grudnia 2012 r. są zamieszczone rekomendacje o dostępie użytkowników do informacji w Internecie, szczególnie na stronach internetowych, sklepach internetowych itd. Dodatek określa, że każdy podmiot gospodarczy w Internecie musi zabezpieczyć wolny dostęp do informacji o serwisie internetowym, firmie go prowadzącej, zasadach korzystania. Wynika z tego niezbędność umieszczenia tzw. zasad korzystania z serwisu (innymi słowami – regulamin). Dodatek nie określa elementów, które powinni być napisane w tym regulaminie, ale eksperci strony law.ua określają takie podstawowe części regulaminu zgodnie z ukraińskim prawem:

1. Informacja o stronie, podmiocie gospodarczym.
2. Rodzaje użytkowników, którzy mają prawo do korzystania z serwisu/sklepu.
3. Opis przedstawionych usług, towarów.
4. Metody płatności i dostawy.
5. Ochrona danych osobowych.
6. Określenia prawa autorskiego i reguł używania materiałów ze strony.
7. Zakres odpowiedzialności, prawo do reklamacji, zasady gwarancji.
8. Postanowienia końcowe.

W ukraińskim prawie nie ma obowiązku umieszczenia na stronie polityki prywatności sklepu internetowego, chociaż ustawa „O ochronie danych osobowych" poleca stworzenie takiej polityki. Dlatego, w naszym badaniu postanowiliśmy wszystkie pojedyncze hasła o ochronie danych osobowych na stronie internetowej uważać za tak zwaną politykę prywatności[101].

2. Wyniki badania

Według metodologii badania z rozdziału 4.3.1 przeanalizowaliśmy 50 największych ukraińskich sklepów internetowych w celu oceny posiadania reguł korzystania sklepu (Regulamin) i polityki prywatności. Ogólne wyniki oceny regulaminów ukraińskich sklepów internetowych są przedstawione w tabeli 4.13.

[101] A.V.Chuchkovska, *Regulacja prawna handlu elektronicznego w Ukrainie,* Kyivski Uniwersytet Narodowy, Kyiv, 2007, s.43-56

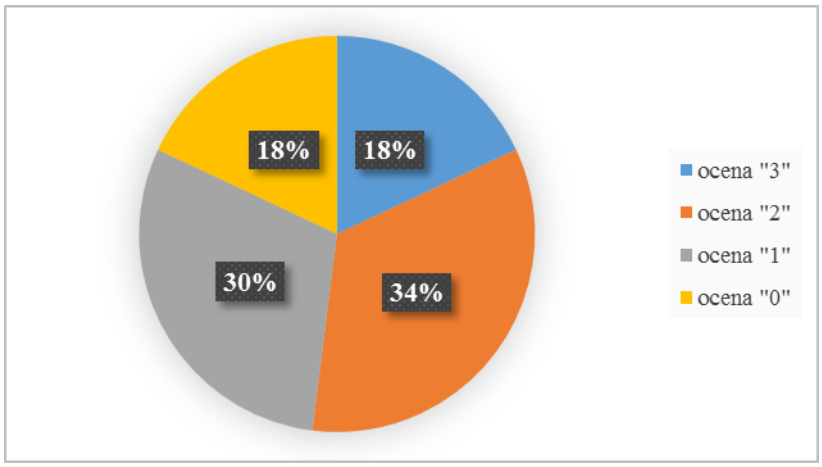
Tabela 4.13. Wyniki analizy regulaminów ukraińskich sklepów internetowych

Kategoria	Elektronika i AGD				
Sklep	rozetka.com.ua	allo.ua	fotos.ua	foxtrot.com.ua	mobilluck.ua
Ocena regulaminu	2	2	0	1	1
Sklep	comfy.ua	citrus.ua	eldorado.com.ua	fotomag.com.ua	sokol.ua
Ocena regulaminu	2	2	0	1	1
Kategoria	Zdrowie i uroda				
Sklep	beauty-life.com.ua	avon.com.ua	parfumeria.ua	eva.dp.ua	enjee.ua
Ocena regulaminu	3	3	2	2	0
Sklep	watsons.com.ua	ua.oriflame.com	makeup.com.ua	cosmetic.com.ua	beautystore.com.ua
Ocena regulaminu	2	3	2	1	2
Kategoria	Kultura i rozrywka				
Sklep	bukva.ua	yakaboo.ua	nashformat.ua	bookclub.ua	librabook.com.ua
Ocena regulaminu	1	2	1	2	1
Sklep	bookzone.com.ua	petrovka.ua	knigoland.com.ua	knigka.ua	book-mania.com.ua
Ocena regulaminu	0	1	0	1	0
Kategoria	Moda				
Sklep	bonprix.ua	leboutique.com.ua	modnakasta.ua	lamoda.ua	shopnow.com.ua
Ocena regulaminu	3	3	1	3	2
Sklep	shopart.ua	helen-marlen.ua	stylepit.ua	www.witt-international.ua	fame.ua
Ocena regulaminu	2	2	1	0	0
Kategoria	Sklepy specjalistyczne				
Sklep	e-esco.com.ua	winauto.ua	aqua-club.com.ua	autobazar.ua	rst.ua
Ocena regulaminu	2	2	3	0	1
Sklep	auto.ria.ua	infocar.ua	olx.ua	agromat.ua	prom.ua
Ocena regulaminu	1	2	3	1	3

Zródło: Opracowanie własne

Z tabeli wynika, że pełne i szczególne regulaminy mają tylko 9 sklepów z 50 analizowanych, regulaminy nieszczególne, ale odpowiadające normom kraińskiego prawa mają 17 sklepów, i 15 sklepów mają regulaminy niekompletne. Również 9 sklepów w ogóle nie mają na swojej stronie żadnych linków, dokumentów, dotyczących reguł korzystania ze sklepu. Procentowy podział wyników przedstawimy na rysunku 4.32.

Rysunek 4.32. Procentowy podział wyników analizy regulaminów ukraińskich sklepów internetowych



Zródło: Opracowanie własne

Z wykresu wynika, że połowa ukraińskich sklepów internetowych (52% sklepów z ocenami 3 i 2) mają regulaminy, które odpowiadają istniejącym normom ukraińskiego prawa. Ale to znaczy, że mniej niż polowa niestety nie ma żadnych reguł korzystania ze sklepu lub regulaminy są niekompletne.

Również przeanalizowaliśmy ukraińskie sklepy internetowe na posiadanie polityki prywatności, lub innego dokumentu o ochronie danych osobowych. Poszczególne wyniki badania przedstawimy w tabeli 4.14.

Tabela 4.14. Wyniki badania posiadania polityki prywatności przez ukraińskie sklepy internetowe

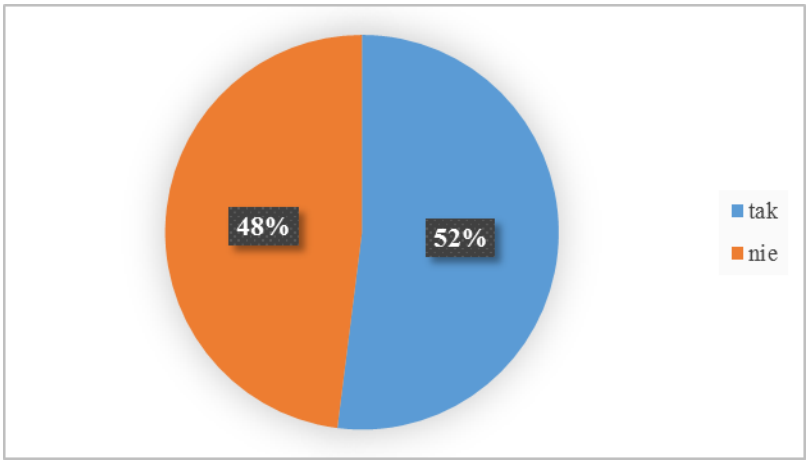
Kategoria	Elektronika i AGD				
Sklep	rozetka.com.ua	allo.ua	fotos.ua	foxtrot.com.ua	mobilluck.ua
Polityka prywatności	tak	nie	nie	nie	nie
Sklep	comfy.ua	citrus.ua	eldorado.com.ua	fotomag.com.ua	sokol.ua
Polityka prywatności	tak	tak	nie	nie	nie

Kategoria	Zdrowie i uroda				
Sklep	beauty-life.com.ua	avon.com.ua	parfumeria.ua	eva.dp.ua	enjee.ua
Polityka prywatności	tak	tak	tak	tak	nie
Sklep	watsons.com.ua	ua.oriflame.com	makeup.com.ua	cosmetic.com.ua	beautystore.com.ua
Polityka prywatności	tak	tak	tak	tak	tak
Kategoria	Kultura i rozrywka				
Sklep	bukva.ua	yakaboo.ua	nashformat.ua	bookclub.ua	librabook.com.ua
Polityka prywatności	tak	tak	nie	nie	nie
Sklep	bookzone.com.ua	petrovka.ua	knigoland.com.ua	knigka.ua	book-mania.com.ua
Polityka prywatności	nie	tak	nie	nie	nie
Kategoria	Moda				
Sklep	bonprix.ua	leboutique.com.ua	modnakasta.ua	lamoda.ua	shopnow.com.ua
Polityka prywatności	tak	tak	nie	tak	tak
Sklep	shopart.ua	helen-marlen.ua	stylepit.ua	www.witt-international.ua	fame.ua
Ocena regulaminu	tak	tak	nie	nie	nie
Kategoria	Sklepy specjalistyczne				
Sklep	e-esco.com.ua	winauto.ua	aqua-club.com.ua	autobazar.ua	rst.ua
Polityka prywatności	tak	nie	tak	nie	nie
Sklep	auto.ria.ua	infocar.ua	olx.ua	agromat.ua	prom.ua
Polityka prywatności	nie	tak	tak	nie	tak

Zródło: Opracowanie własne

Podane dane oczywiście nie określają całej sytuacji na rynku, ale 26 sklepów internetowych z 50 badanych ma tzw. politykę prywatności umieszczoną na stronie. Z innej strony 24 sklepy nie mają lub nie dodały na stronę politykę prywatności. Procentowy podział wyników jest pokazany na rysunku 4.33.

Rysunek 4.33. Procentowy podział analizy posiadania polityki prywatności na stronie internetowej sklepu w Ukrainie.



Zródło: Opracowanie własne

W podsumowaniu należy zaznaczyć, że dla początkowego etapu rozwoju e-commerce w Ukrainie, sytuacja bezpieczeństwa prawnego na ukraińskim rynku handlu elektronicznego jest na dość dobrym poziomie. Bez względu na brak ustaw i rozporządzeń, dotyczących handlu elektronicznego, sklepy samodzielnie regulują swoją działalność prawną, określając reguły korzystania z serwisu na stronie internetowej. Nie zapominają również o ochronie danych osobowych, tworząc własną politykę prywatności, bazując na ustawie „O ochronie danych osobowych". Chociaż tylko połowa badanych sklepów ma politykę prywatności, pojawia się tendencja do rozumienia przez właścicieli sklepów ważności posiadania dokumentów prawnych, regulujących relację pomiędzy konsumentem i sklepem internetowym. Dla początkowego etapu rozwoju e-commerce w Ukrainie, sytuacja bezpieczeństwa prawnego na rynku ukraińskiego handlu elektronicznego jest na dość dobrym poziomie.

Podsumowanie

Handel elektroniczny charakteryzuje się wysoką dynamiką zmian. Wynika to po-pierwsze z rozwoju nowych technologii informacyjnych, wzrostu natężenia konkurencji, powstawania nowych modeli biznesowych, a po drugie z rozwoju społeczeństwa informacyjnego i coraz większej dostępności do Internetu. W tych warunkach każdy podmiot gospodarczy prowadzący działalność w sferze e-handlu staje przed wyzwaniem - w jaki sposób zaspokoić oczekiwania i preferencje rynku docelowego.

Przedmiotem pracy magisterskiej była analiza bezpieczeństwa handlu elektronicznego ze strony technologicznej i prawnej w Polsce i Ukrainie. Jak już wspomniano, te kraje zostały wybrane ze względu na różny poziom rozwoju ekonomicznego i technologicznego, w celu analizy sytuacji obecnej i wykrycia lepszych praktyk.

W rozdziale pierwszym określiliśmy, że handel elektroniczny to szerokie pojęcie, które obejmuje procesy kupna i sprzedaży pośrednictwem Internetu. Popularność e-handlu wynika z wielu zalet tak dla firm, jak i dla konsumentów. Istnieją różne modele biznesowe handlu elektronicznego, dlatego firmy mają wybór, w jaki sposób prowadzić biznes w Internecie. Chociaż handel elektroniczny rozwija się bardzo szybko, są różne bariery dla jego dalszego rozwoju, to między innym niskie kompetencje komputerowe użytkowników, brak lub niedoskonałość norm prawnych, regulujących działalność w Internecie. Ale za wynikami licznych badań globalny rynek e-commerce będzie dalej dynamicznie rozwijał się.

W rozdziale drugim przeanalizowaliśmy globalną sytuację bezpieczeństwa w Internecie, określiliśmy główne rodzaje zagrożeń. Nie jest możliwe uniknięcie wszystkich zagrożeń, dlatego w firmie należy przeanalizować ryzyko i wyznaczyć priorytety bezpieczeństwa. Klasycznymi podejściami bezpieczeństwa internetowego są szyfrowanie i podpis elektroniczny. Ale handel elektroniczny ma swoją specyfikę i należy również stosować specjalne metody bezpieczeństwa, takie jak ochrona domeny internetowej, ochrona bazy danych, wybór bezpiecznego hostingu, ochrona serwera www itd. Stosowanie takich technik bezpieczeństwa pozwoli zwiększyć odporność systemu handlu elektronicznego przed głównymi zagrożeniami.

Rozdział trzeci dotyczył bezpieczeństwa prawnego. Międzynarodowe normy prawne, dotyczące regulacji handlu elektronicznego nadal formułują się. Jest powiązane po pierwsze z szybkim rozwojem e-handlu, a po drugie z odmiennymi normami prawnymi w poszczególnych krajach. Znajomość krajowych norm prawnych, dotyczących działalności

prowadzonej w Internecie, posiadanie regulaminu sklepu, polityki prywatności, prawidłowo napisanej umowy pozwoli przedsiębiorcy zabezpieczyć swój biznes.

W rozdziale czwartym zrobiono szczegółowe badanie stanu bezpieczeństwa w handlu elektronicznym dla Polski i Ukrainy. W Polsce sytuacja wygląda znaczniej lepiej niż w Ukrainie.

Prowadzone badanie polskich sklepów internetowych pokazało, że znaczna część sklepów (90%) chroni swoich użytkowników przez posiadanie certyfikatu SSL. Problemem nadal są niskie oceny certyfikatów lub ich nieważność na niektórych stronach, chociaż było wybranych 50 najpopularnejszych sklepów, z których korzysta większość Polaków. Jedynie 58% procent sklepów ma automatycznie przekierowanie stron poufnych na tryb bezpieczny https://, co znaczy, że 42% sklepy internetowe nie mają zabezpieczenia danych osobowych użytkowników. Polskie sklepy internetowe są również zabezpieczone prawnie, ponieważ więcej niż 90% sklepów ma umieszczane na swojej stronie regulamin sklepu i politykę prywatności.

Badanie ukraińskich sklepów wykazało, że z pięćdziesięciu sklepów tylko 31 ma ważne certyfikaty bezpieczeństwa, i tylko 23 z nich posiadają sprawne certyfikaty, co stanowi mniej niż połowę wszystkich badanych sklepów. 80% ukraińskich sklepów internetowych nie ma przekierowania na tryb bezpieczny na stronach, gdzie użytkownik wpisuje poufne informacje. Niestety sytuacja wygląda w nienajlepszy sposób, ponieważ takie złe zabezpieczenie rozwiązuje ręce cyberprzestępcom. Bezpieczeństwo prawne w Ukrainie jest na niskim poziomie, ponieważ nie są przyjęte ustawy prawne, regulujące działalność handlu elektronicznego. Ze względu na sytuację obecną wyniki badania na posiadanie regulaminu i polityki bezpieczeństwa są dobre – prawie polowa sklepów ma regulamin na swojej stronie.

Właściciele jak ukraińskich tak i polskich sklepów internetowych powinni rozumieć, że nieposiadanie żadnych zabezpieczeń stanowi zagrożenie nie tylko dla użytkowników, ale i dla biznesu. Certyfikaty SSL mają niewielkie koszty, ale pozwalają chronić przed większymi wydatkami w razie utraty danych przez atak na przykład. Jak i w polskim, tak i w ukraińskim Internecie są wielu przykładów regulaminu sklepu, polityki prywatności i nie zajmie dużo czasu napisanie własnego regulaminu i określenie polityki prywatności, ale takie rzeczy mogą zabezpieczyć przed rozprawy sądowe z-za braku regulaminu na przykład. Ale bezpieczeństwo sklepu internetowego, to nie tylko SSL, to również ochrona domeny internetowej, bazy danych, serwerów WWW i samego systemu informatycznego.

Propozycje, co do polepszenia bezpieczeństwa sklepów internetowych dla Polski i Ukrainy są następujące:

1. Regularnie sprawdzać datę ważności certyfikatu SSL, pry bliskim terminie ważności zaplanować przedłużenie certyfikatu.
2. Wybierać tylko zaufanych dostawców kluczy, samodzielnie podpisywanie certyfikatu nie jest bezpieczne. Pry możliwości wyboru długości kluczu, wybierać ten, która ma największą długość (na przykład 4096 bit).
3. Przez szeroko dostępne narzędzia (na przykład, SSL Labs i inne) sprawdzać siłę i ocenę certyfikatu i zwracać szczególną uwagę na wyniki badania i na czas podejmować odpowiednie działania.
4. Wybierać tylko zaufanych dostawców kluczy, samodzielnie podpisywanie certyfikatu nie jest bezpieczne.
5. Szczególnie zabezpieczać strony, gdzie klienci wprowadzają informacje poufne (logowanie, rejestracja, wysyłanie zamówienia). Wdrożenie na tych stronach trybu bezpiecznego https:// obniża ryzyko utraty danych osobowych, co z innej strony podnosi poziom zaufania konsumenta do danego sklepu internetowego.
6. Nie oszczędzać koszty na inwestycję w bezpieczeństwo systemu i transakcji. Trzeba pamiętać, że ekonomia na bezpieczeństwie może przynieść dużo większe straty dla firmy, jak i finansów, tak i klientów.
7. Nie jest możliwym zabezpieczyć e-sklep przed wszystkimi zagrożeniami, dlatego należy oceniać ryzyko zagrożeń i prawidłowo wyznaczać priorytety bezpieczeństwa.
1. Dbać o bezpieczeństwo innych istotnych częściach systemu informatycznego e-sklepu, między innym o bezpieczeństwo domeny internetowej, serwerów www, bazie danych i regularnie robić zapasowe kopie danych systemu. Regularna instalacja poprawek systemowych oraz najnowszych wersji programów może skutecznie zabezpieczyć system.
8. Sprawdzać wiadomości prawne na temat zmian w przepisach, ustawach, regulujących działalność handlową w Internecie i zgodnie im robić odpowiednie zmiany w regulaminie sklepu i umowach z klientami.
9. W odpowiedny sposób ochraniać dane osobowe użytkowników. Stworzenie i umieszczenie polityki prywatności – warunek konieczny.

W powyższym opracowaniu, doszliśmy do wniosku, że bezpieczeństwo to główna bariera w rozwoju handlu elektronicznego w kraju. Silnikiem handlu są konsumenci i od tego, jak bezpiecznie oni siebie przy zakupach internetowych zależy wzrost e-handlu i liczby konsumentów. Dlatego i sprzedawcy i urzędy państwowe muszą rozumieć potrzebę bezpieczeństwa handlu w Internecie dla rozwoju biznesu i gospodarki krajowej.

Bibliografia

Pozycje zwarte:

1. **Ambrozik M.,** Wojciechowski A. *E-Commerce - koncepcja biznesu.* Warszawa, 2007.
2. ***Bezpieczeństwo Serwery System*** *i bezpieczeństwo internetowe.* Wersja 6 wydanie 1. Wydawnictwo IBM.
3. **Chmielarz W.** *Systemy biznesu elektronicznego.* Wydawnictwo Difin, Warszawa 2007.
4. **Chuchkovska A.V.** *Regulacja prawna handlu elektronicznego w Ukrainie,* Kyivski Uniwersytet Narodowy, Kyiv, 2007.
5. ***Inspired by Internet.*** Praca zbiorowa pod redakcją naukową mgr Piotra Drygasa, Poznań, 2004.
6. **Gregor B.,** Stawiszyński M., *E-commerce,* Bydgość 2002.
7. ***IT w biznesie.*** *Prowadzenie do handlu elektronicznego,* PJWSTK, Warszawa 2012.
8. **Kępa L.,** Tomasik P., Dobrzyński S. *Bezpieczeństwo systemu e-commerce,* Helion 2012.
9. **Kirov N.,** Kuśmierz A., Rządca R., *Jak się kręci e-biznes*. PC Kurier 2003, nr 8.
10. **Lewicki M.** *Instrumenty dla tworzenia wartości dla klienta w handlu elektronicznym.* Rozprawa doktorska. Poznań 2012.
11. **Lubasz D.** *Handel elektroniczny. Bariery prawne.* Lexis Nexis, Warszawa 2013.
12. **Niedźwiedziński M.** *Globalny handel elektroniczny.* Warzawa, 2004
13. **Nojszewski D.** *Biznes elektroniczny – czyli jaki?* E-mentor №1(3), 2004.
14. **Pavlova V.** *O problemie rozwoju handlu elektronicznego w Ukrainie.,* Dziennik ekonomiczny, №1 (2014).
15. ***PC World Komputer Pro*** *– Bezpieczeństwo systemów,* SecurITy, nr 2/2003
16. **Pfitzmann B.** *A General Framework for Formal Notions of Secure" Systems,* Hildesheimer Informatik-Berichte 2012.
17. **PN-ISO/IES 27001:2007.** *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*
18. **Samołyk J.** *E-business - globalna rewolucja*. Infoman 1999, nr 7/8.
19. **Schneier B.** *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C,* Warszawa, Wydawnictwa Naukowo-Techniczne, 2002.
20. ***Systemy e-commerce.*** *Technologie internetowe w biznesie,* Praca zbiorowa pod redakcją Celiny M.Olszak, Katowice, 2004.
21. **Tanas R.** *Kryptografia*, Poznań 2009, s.44.
22. **Timmers P.** *Business models for electronic markets.* "Electronic Markets", 1998, Vol.8, no. 2.
23. **Wawszczyk A.** *E-gospodarka, Poradnik przedsiębiorcy,* Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2003.
24. ***Zagadnienia handlu elektronicznego***, PJWSTK, Warszawa 2012.

Raporty:

1. ***Atak i Obrona 2013*** *Raport: Ataki i metody obrony w Internecie w Polsce,* Warszawa 2014
2. ***Bezpieczeństwo i zaufanie.****Filary polskiego e-commerce*.Badania ceneo.pl, luty 2013.
3. ***Bezpieczeństwo zakupów w polskich sklepach internetowych****,* Raport certyfikatyssl.pl, marzec 2013.
4. ***Charakterystyka rynku handlu elektronicznego w Ukrainie 2013.***Raport badawczy dla ain.ua., 2014.
5. ***ECommerce*** *Poland Executive Summary Raport 2014*.
6. ***E-commerse*** *Polska 2014,* Gemius dla E-commerce Polska.
7. ***Internet Security Thred Report 2015****,* Symantek 2015.
8. ***Prognoza rozwoju*** *rynku e-commerce 2014-2017 rr.,* Prom.ua dla emarketing,ua, 2013.
9. ***Raport*** *E-handle Polska,* 2014.
10. ***Rynek elektroniczny w Polsce.*** Opracowane przez Agnieszkę Garbacz. Departament Informacji Gospodarczej Polska Agencja Informacji i Inwestycji Zagranicznych S.A., 2010
11. ***Rynek telekomunikacyjny***, Państwowy Urząd statystyczny Ukrainy, 2014.

Akty prawne:

1. ***Directive 2000/31/EC of the European Parliament*** *and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (Directive on electronic commerce), Official Journal L 178, 17/07/2000 p. 0001-0016.
2. ***Ustawa z dnia 4 lutego 2011 r. prawo prywatne międzynarodowe*** *oraz Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I).*

Zródła internetowe:

1. *Baza CVE,* www.cve.mitr.org [dostęp 15.07.2014]
2. *CISCO 2014. Annual security report.* http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf, [dostęp 15.11.2014]
3. *Debis Systemhaus GmbH Report 2012,* http://www.channelpartner.de/schwerpunkt/Debis%20Systemhaus [dostep 10.07.2014]
4. *E-handel (handel elektroniczny),* http://stat.gov.pl/metainformacje/slownik-pojec/definicje-pojec/1778,pojecie.html [dostęp: 12.04.2014]
5. *Forrester Research Online Retail Forecast 2017,* https://www.forrester.com/Forrester+Research+Online+Retail+Forecast+2013+To+2018+Western+Europe+Q4+2014+Update/fulltext/-/E-res120541 [dostęp 08.05.2014]
6. *Global Selling Report 2013,* http://www.channeladvisor.com/platform/global-selling/ [dostęp 08.05.2014]
7. *Ochrona prywatności konsumentów e-commerce.* http://www.een.org.pl/index.php/internet-i-handel-elektroniczny---

spis/page/4/articles/ochrona-prywatnosci-konsumentow-e-commerce.html [dostęp 18.04.2015]
8. *Oficjalny portal Unii Europejskiej*, http://www.europa.eu.int/information_society/eerope/index_en.htm [dostęp 10.10.2014]
9. *Ranking Sklepów internetowych 2014.* http://ranking.money.pl/ [dostęp 18.03.2015]
10. *Ranking ukraińskich sklepów internetowych*, www.shops.prom.ua [dostęp 22.04.2015]
11. Raport serwisu Sklepy24.pl, *E-handel Polska 2009*. http://dotcomriver.pl/files/raport-ehandel-polska-2012.pdf [dostęp: 12.04.2014]
12. *Security Issues in E-Commerce,* http://webscience.ie/blog/2010/security-issues-in-e-commerce/ [dostep 08.07.2014]
13. J.Winiarski, *Technologie internetowe –wprowadzenie.* http://www.slideshare.net/piniol/gospodarka-elektroniczna-1 [dostęp: 10.04.2014]
14. *Worldwide B2C Ecommerce: 2012 Complete Forecast.* http://www.emarketer.com/report/1259 [dostęp 12.04.2014]
15. *Zagadnienia handlu elektronicznego*, PJWSTK, Warszawa 2012.

Spis rysunków

Rysunek 1.1. Główne źródła trudności definicyjnych pojęcia handel elektroniczny 8
Rysunek 1.2. Miejsce handlu elektronicznego wśród pojęć pokrewnych 9
Rysunek 1.3. Topologia handlu elektronicznego.....14
Rysunek 1.4. Scenariusz wprowadzenia handlu elektronicznego 21
Rysunek 1.5. Architektura systemu informatycznego dla e-handlu 22
Rysunek 1.6. Prognoza sprzedaży e-commerce w świecie..... 24
Rysunek 1.7. Prognozy rozwoju handlu elektronicznego w świecie na 2017 rok.....29
Rysunek 1.8. TOP 10 krajów na europejskim rynku e-handlu.....30
Rysunek 2.1. Motywy hakowania serwisów e-commerce według serwisu Zone-H 32
Rysunek 2.2. Mapa najczęściej występujących krajów w zestawieniach źródeł ataków. 39
Rysunek 2.3. Najczęściej występujące ataki w Internecie.....39
Rysunek 2.4. Podział ataków hostingowych według rozmiaru firmy 42
Rysunek 2.5. Czas awarii a ryzyko upadłości przedsiębiorstwa 43
Rysunek 2.6. Wykres analizy wpływu na biznes (BIA).....43
Rysunek 2.7. Schemat szyfrowania symetrycznego.....45
Rysunek 2.8. Schemat szyfrowania niesymetrycznego.....47
Rysunek 4.1. Procentowy podział użytkowników Internetu w Polsce, %.....72
Rysunek 4.2. Częstotliwość robienia zakupów w sieci 73
Rysunek 4.3. Motywacja robienia zakupów w sieci..... 74
Rysunek 4.4. Wzrost liczby sklepów internetowych za 2008-2014 rr. 74
Rysunek 4.5. Podział sklepów internetowych za wiekiem 75
Rysunek 4.6. Polski rynek e-commerce za branżami 75
Rysunek 4.7. Rozmiar oferty polskich sklepów internetowych 76
Rysunek 4.8. Procentowy podział użytkowników Internetu w Ukrainie, % 78
Rysunek 4.9. Podział ukraińskich użytkowników Internetu za wiekiem. 79
Rysunek 4.10. Motywacja ukraińskich konsumentów do zakupów w Internecie 79
Rysunek 4.11. Obrót towarów w Internecie za kategoriami, mln. UAH.....80
Rysunek 4.12. Podział towarów, które najczęsciej kupują ukraińcy.....81
Rysunek 4.13. Dochody największych sklepów internetowych w Ukrainie w 2014 roku, mln. UAH 82
Rysunek 4.14. Wynik badania SSL Labs dla strony amazon.com 84
Rysunek 4.15. Okno logowania na srtonie amazon.com w trybie „security” 86
Rysunek 4.16. Statystyka konsumentów o oszuctwach w sieci 87

Rysunek 4.17. Statystyka opinii konsumentów według bezpieczeństwa zakupów w Internecie.... 88
Rysunek 4.18. Procentowy podział ocen bezpieczeństwa certyfikatów SSL polskich sklepów.... 91
Rysunek 4.19. Procent posiadania sprawnych i niesprawnych certyfikatów SSL 92
Rysunek 4.20. Podział polskich sklepów internetowych za długością kluczy... 92
Rysunek 4.21. Procentowy podział posiadania certyfikatu SSL na stronach poufnych... 93
Rysunek 4.22. Procentowy udział wybieranych centrum certyfikacyjnych przez polskie sklepy... 94
Rysunek 4.23. Statystyka najczęściej występujących problemów przy zakupach 95
Rysunek 4.24. Statystyka opinii konsumentów według bezpieczeństwa zakupów w Internecie... 96
Rysunek 4.25. Procentowy podział ocen bezpieczeństwa certyfikatów SSL ukraińskich sklepów 101
Rysunek 4.26. Procent posiadania sprawnych i niesprawnych certyfikatów SSL 101
Rysunek 4.27. Podział polskich sklepów internetowych za długością kluczy 101
Rysunek 4.28. Procentowy podział posiadania certyfikatu SSL na stronach poufnych.....102
Rysunek 4.29. Procentowy udział wybieranych centrum certyfikacyjnych przez polskie sklepy 103
Rysunek 4.31. Procentowy podział wyników analizy regulaminów polskich sklepów internetowych.....109
Rysunek 4.32. Procentowy podział analizy posiadania polityki prywatności na stronie internetowej sklepu w Polsce. 111
Rysunek 4.33. Procentowy podział wyników analizy regulaminów ukraińskich sklepów internetowych.....115
Rysunek 4.34. Procentowy podział analizy posiadania polityki prywatności na stronie internetowej sklepu w Ukrainie. 117

Spis tabeli

Tabela 1.1. Różne definicje pojęcia „handel elektroniczny” 8
Tabela 1.2. Nieścisłości w zakresie definiowania pojęcia e-handel 11
Tabela 1.3. Różnice pomiędzy handlem elektronicznym a tradycyjnym 16
Tabela 1.4. Główne modele biznesowe w sektorze B2C 19
Tabela 1.5. Główne modele biznesowe w sektorze B2B 19
Tabela 1.6. Potrzeby i korzyści wynikające z zastosowania handlu elektronicznego 26
Tabela 4.1. Top-50 polskich sklepów internetów według kategorii 78
Tabela 4.2. Statystyki i prognoza rozwoju e-commerce w Ukrainie 79
Tabela 4.3. Top-50 ukraińskich sklepów internetów według branży 83
Tabela 4.4. Oceny certyfikatów według SSL 84
Tabela 4.5. Oceny protokolów wedlug SSL Labs 85
Tabela 4.6. Oceny procentowe kluczy 86
Tabela 4.7. Procentowe oceny szyfrowania według SSL Labs 86
Tabela 4.8. Wyniki badania bezpieczeństwa 50 sklepów elektronicznych w Polsce 89
Tabela 4.9. Wyniki badania bezpieczeństwa 50 sklepów elektronicznych w Ukrainie 97
Tabela 4.10. Ocena jakości regulaminu sklepu internetowego 105
Tabela 4.11. Wyniki oceny regulaminów polskich sklepów internetowych 109
Tabela 4.12. Wyniki badania posiadania polityki prywatności przez polskie sklepy internetowe 110
Tabela 4.13. Wyniki analizy regulaminów ukraińskich sklepów internetowych 114
Tabela 4.14. Wyniki badania posiadania polityki prywatności przez ukraińskie sklepy internetowe 116