Katarzyna Kurkiewicz[1]
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego

Wielowymiarowy aspekt gospodarki elektronicznej z uwzględnieniem kwestii bezpieczeństwa

Streszczenie

E-gospodarka, znana również jako gospodarka elektroniczna, to dynamiczny obszar działalności gospodarczej oparty na rozwiązaniach technologicznych. W artykule przedstawiono zależność między tradycyjną gospodarką a jej elektronicznym wymiarem. Autorka omówiła problemy związane z zagrożeniami, jakie niesie za sobą gospodarka elektroniczna, wyróżniając zagrożenia celowe i przypadkowe. Poruszono również kwestie bezpieczeństwa, w tym bezpieczeństwa sprzętu, kontroli dostępu oraz zakupu oprogramowania komercyjnego. Na koniec omówiono problematykę przepisów prawnych regulujących e-gospodarkę w świetle prawa Unii Europejskiej i Polski. Celem artykułu jest odpowiedź na pytanie, w jakim kierunku zmierza e-gospodarka, z uwzględnieniem kwestii bezpieczeństwa, oraz potwierdzenie bądź sfalsyfikowanie postawionej hipotezy badawczej. Autorka odniosła się do zastosowania takich metod badawczych jak: uogólnienie, analiza, synteza i wnioskowanie. Niniejszy artykuł nie wyczerpuje pełnego problemu, ale jedynie wskazuje kierunki analizy.

Słowa kluczowe: e-gospodarka, gospodarka, e-handel, e-biznes, cyfryzacja, rozwój technologiczny, informacja, zagrożenia, przedsiębiorstwa, konsument

Abstract

E-economy, also known as electronic economy, is a dynamic area of economic activity based on technological solutions. The article indicates the relationship between the traditional economy and its electronic dimension. The author understood the problem-specific issues related to the threats posed by the electronic economy, distinguishing intentional threats and accidental threats. Security issues were presented, including hardware security and access controls, as well as the purchase of commercial software. Finally, the issue of legal provisions regulating the e-economy in the light of European Union and Polish law was raised. The aim of the article is to answer the question in what direction the e-economy is heading, taking into account security issues, and to confirm or falsify the research hypothesis. The author referred to the use of such research methods in the article as: generalization, analysis, synthesis, and inference. This article does not constitute a full exhaustion of the problem but only indicates the directions of analysis.

Keywords: e-economy, economy, ecommerce, e-business, digitalization, technological development, information, threat, enterprise, consumer

[1] e-mail: kasia56340@gmail.com

Wstęp

Dynamiczny rozwój technologii i zachodzące wraz z nim zmiany zauważalne są niemal w każdym wymiarze życia całego społeczeństwa jak i poszczególnych jednostek. Całokształt tego przekłada się w dużej mierze na wygodę życia. Przemawiają za tym udogodnienia takie jak chociażby: możliwość płatności mobilnych – tutaj dotyczy to przede wszystkim możliwości płatności kartą czy blikiem, coraz częściej używane do płatności są zegarki bądź nawet pierścionki NFC; robienie zakupów na odległość; komputerowe wspomaganie procesów produkcyjnych. Cyfryzacja odmieniła zupełnie sposób życia oraz przekształciła działanie przedsiębiorstw i konsumentów. W obecnym cyfrowym świecie, gospodarka elektroniczna nie tylko jest popularnym światopoglądem, ale koniecznością. Obok znaczących korzyści jakie niesie informatyzacja nie można pominąć kwestii związanych z bezpieczeństwem oraz zagrożeniami. Należy zaznaczyć, iż są to dwa powszechnie znane terminy, oznaczające dwa całkowicie przeciwstawne, ale również współzależne stwierdzenia. Pojęcie bezpieczeństwa ma charakter zmienny i dynamiczny a definiowane jest w różnorodny sposób ze względu na dotyczący go wieloaspektowy fenomen. Najczęściej określane jest jako stan wolny od niepokoju, tworzący poczucie pewności, stan bez troski od łacińskiego ,,sine cura – securitas'' (Zięba, 2005, s. 33). Bez wątpienia antonimem bezpieczeństwa są zagrożenia. „Współcześnie poczucie zagrożenia u człowieka nieobarczonego chorobliwymi lękami powstaje w atypowych, ekstremalnych sytuacjach, znajdujących bezpośrednie odniesienie do siebie lub innych osób. Pojawia się zazwyczaj sporadycznie, niespodziewanie i spontanicznie, nierzadko także w obliczu spektakularnych doniesień prasowych o przypadkach poruszających wyobraźnię i pozostających w opozycji do powszechnie akceptowanych norm etycznych i prawnych. Na ogół dopiero wówczas występuje potrzeba myślenia czy dyskutowania na temat bezpieczeństwa" (Piwowarski, Zachuta, 2013, s. 6). Bowiem właśnie dzięki zagrożeniom można stwierdzić jaki jest poziom odczuwania bezpieczeństwa w danym miejscu i czasie. Zagrożenia wraz z rozwojem cywilizacyjnym cały czas ewoluują. W artykule formułuje się następującą hipotezę badawczą, iż e-gospodarka stanowi potęgę dzisiejszego świata, przy czym zważając na zagrożenia zmierza ona do wykluczenia tradycyjnej gospodarki. Do tak szerokiego tematu wykorzystano wiele materiałów, w tym publikacje papierowe jak i internetowe, wydawnictwa ciągłe oraz dokumenty normatywne związane z omawianymi problemami.

Gospodarka i e-gospodarka – ujęcie definicyjne

Rozwój gospodarki elektronicznej niesie ze sobą zarówno obietnice jak i wyzwania. W miarę jak technologie cyfrowe penetrują coraz szersze obszary życia społecznego i gospodarczego, kluczowe staje się zapewnienie bezpieczeństwa w tym nowym ekosystemie. Definiowanie terminów takich jak „gospodarka" czy „e-gospodarka" staje się zatem kluczowe, ponieważ to od nich zależy zrozumienie oraz kształtowanie odpowiednich strategii i polityk. Tak więc, odpowiedź na py-

tanie dokąd wielowymiarowy aspekt gospodarki elektronicznej zmierza zważając na kwestie bezpieczeństwa wymaga na początek uporządkowania kwestii definicji dlatego, że należy określić co rozumiemy pod kluczowymi pojęciami. Głównym tego powodem jest używanie zamiennie pojęć odnoszących się i stricte związanych z samą e-gospodarką. Kluczowym również jest aktualizowanie definicji, aby odzwierciedlić zmieniającą się rzeczywistość i trendy. Każde zmiany w w wielowymiarowym aspekcie gospodarki elektronicznej muszą więc uwzględniać te podstawowe definicje, aby skutecznie odpowiadać na wyzwania związane z bezpieczeństwem danych i infrastruktury cyfrowej.

Gospodarka jest szeroko pojętym systemem, który obejmuje wszystkie procesy związane z produkcją, dystrybucją oraz konsumpcją dóbr i usług. Odnosi się do działalności gospodarczej prowadzonej w danej przestrzeni geograficznej – region, kraj, świat. Encyklopedia PWN definiuje gospodarkę jako: „całość mechanizmów i warunków działania podmiotów gospodarczych związana z wytwarzaniem i podziałem dóbr i usług" (Encyklopedia PWN, https://encyklopedia.pwn.pl/, dostęp: 05.07.2024). W ramach gospodarki zachodzą różnorodne interakcje między podmiotami gospodarczymi, takimi jak firmy, konsumenci czy nawet instytucje rządowe. Gospodarka jest nierozerwalnie związana z pojęciem zasobów, zarządzaniem nimi oraz ich alokacją w celu zaspokojenia potrzeb społeczeństwa. Bez wątpienia, kluczowym czynnikiem kształtującym gospodarkę każdego kraju jest międzynarodowa współpraca gospodarcza oraz procesy globalizacyjne (Nerć-Pełka, Wysocka, 2012).

W ewolucji gospodarki kluczowe znaczenie miało wprowadzenie podziału na trzy podstawowe sektory (tzw. teoria trzech sektorów), który zaczął się kształtować w latach trzydziestych XX wieku (Noga, 2000). Teoria ta jest istotnym narzędziem analizy ekonomicznej, pozwalającym na zrozumienie ewolucji gospodarczej oraz struktury gospodarek narodowych. Podział ten obejmuje trzy kluczowe obszary działalności gospodarczej, które historycznie kształtowały rozwój cywilizacji:

1) sektor rolniczy – obejmujący rolnictwo, leśnictwo, myślistwo, rybołówstwo i przemysł wydobywczy;
2) sektor przemysłowy – obejmujący przemysł przetwórczy, górnictwo i budownictwo;
3) sektor usługowy – obejmujący szeroko rozumiane usługi, gdzie usługi materialne (związane z produktami, naprawami przedmiotów) i niematerialne (to usługi świadczone przez jedną osobę drugiej osobie, np. lekarz, prawnik, audytor) (Runge, 2008).

Rzadziej możemy również wyróżnić czwarty sektor, który skupia się na zdobywaniu, przetwarzaniu i dostarczaniu informacji w rozumieniu usług zaawansowanych – branża IT, szkolnictwo, bankowość. Sektory gospodarki są istotne, ponieważ pomagają w analizie różnych dziedzin działalności ekonomicznej. Ukazane segmenty służą także do wskazania osiągniętego stopnia rozwoju gospodarczego oraz o wysokości urbanizacji o której informuje nas malejący udział zatrudnienia w sektorze pierwszym oraz drugim a wzrastający w sektorze trzecim (Runge,

2008). Ten podział został ukazany, aby lepiej zrozumieć historyczne kierunki rozwoju gospodarczego i strukturalne zmiany w ekonomiach narodowych. Umożliwia on analizę przejścia od społeczeństwa rolniczego, przez przemysłowe, aż do współczesnej gospodarki opartej na usługach i technologiach zaawansowanych. Dzięki temu, można lepiej identyfikować i prognozować zmiany w strukturze gospodarki, co jest kluczowe dla planowania polityki ekonomicznej i rozwoju społecznego.

Obecnie wiele krajów funkcjonuje w systemie gospodarczym, który można określić jako gospodarka rynkowa, choć niektórzy używają terminu gospodarka mieszana. Gospodarka rynkowa charakteryzuje się przewagą mechanizmów rynkowych w regulowaniu produkcji, dystrybucji i konsumpcji dóbr oraz usług. W takim systemie ceny są ustalane na podstawie popytu i podaży, a przedsiębiorstwa konkurują ze sobą na wolnym rynku. Rola państwa jest ograniczona do regulacji, ochrony praw własności, zapewnienia porządku publicznego oraz dostarczania publicznych dóbr i usług, które nie są dostarczane w wystarczającym stopniu przez sektor prywatny. Praktyczne zastosowanie tej idei przejawia się w traktatowych regulacjach funkcjonowania Unii Europejskiej, a także w konstytucyjnym uznaniu społecznej gospodarki rynkowej, na przykład w Polsce. W traktacie ustanawiającym Konstytucję dla Europy uznano, że podstawą trwałego rozwoju Unii Europejskiej będzie społeczna gospodarka rynkowa (Traktat ustanawiający Konstytucję dla Europy, Dz. Urz. UE C 310, t. 47, 16.12.2004). Jeżeli chodzi o konstytucyjne uznanie to zgodnie bowiem z art. 20 Konstytucji Rzeczypospolitej Polskiej „społeczna gospodarka rynkowa oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej" (Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. nr 78, poz. 483). Gospodarka rynkowa wyróżnia się zdolnością do stymulowania innowacji, co wynika z konkurencji, która motywuje przedsiębiorstwa do ciągłego wprowadzania nowych produktów i usług. Taki system sprzyja również tworzeniu dobrobytu, ponieważ firmy, dążąc do zysku, inwestują w rozwój technologii i infrastruktury, co przekłada się na wzrost jakości życia obywateli. W efekcie, dynamiczna gospodarka rynkowa przyczynia się do lepszego dostosowania do zmieniających się potrzeb społeczeństwa, zwiększając ogólne zadowolenie i dobrobyt.

Większość gospodarek świata można również określić mianem gospodarek mieszanych, które łączą elementy gospodarki rynkowej z interwencją państwa w pewne kluczowe obszary. Główną rolę odgrywa w nich własność prywatna i rynek, jednak ograniczoną, choć istotną funkcję pełnią również własność publiczna oraz ingerencja państwa (Musiałkiewicz, Kwiatkowski, 2021). Choć rynek odgrywa dominującą role w alokacji zasobów, państwo interweniuje w celu korygowania nierówności, ochrony środowiska, zapewnienia opieki zdrowotnej, edukacji oraz innych usług społecznych. W gospodarkach mieszanych, rządy często posiadają lub kontrolują niektóre sektory strategiczne, takie jak energetyka, transport czy obrona narodowa. Pandemia COVID-19 również uwydatniła znaczenie gospodarki mieszanej. W wielu krajach rządy interweniowały na dużą skalę,

aby wesprzeć przedsiębiorstwa i obywateli poprzez programy pomocowe, zasiłki i różne formy wsparcia finansowego. Tego rodzaju działania podkreślają, że nawet w najbardziej rynkowo zorientowanych gospodarkach, interwencja państwa jest niekiedy niezbędna do utrzymania stabilności i dobrobytu społecznego. Pojęcie gospodarki mieszanej wynika z przekonania, że ani czysta gospodarka rynkowa, ani całkowicie planowana gospodarka nie są w stanie w pełni sprostać wyzwaniom współczesnych społeczeństw. Gospodarka rynkowa jest efektywna w alokacji zasobów i stymulowaniu innowacji, ale może prowadzić do znaczących nierówności społecznych i problemów związanych z monopolem. Natomiast gospodarka planowana, mimo że może skutecznie realizować cele społeczne, często cierpi na brak elastyczności i innowacyjności. Tak więc, obecny system gospodarczy, często określany jako gospodarka rynkowa lub mieszana, jest wynikiem prób znalezienia równowagi między efektywnością rynkową a interwencją państwową. Ta równowaga pozwala na skuteczne reagowanie na wyzwania gospodarcze i społeczne, zapewniając zarówno rozwój gospodarczy, jak i ochronę interesów społecznych.

Istnieje jeszcze wiele klasyfikacji gospodarki, które pozwalają nam lepiej zrozumieć jej różnorodność oraz dynamikę funkcjonowania. Klasyfikacja bez wątpienia umożliwia analizę i porównanie różnych modeli gospodarczych, co jest istotne zarówno dla badaczy, jak i dla procesów decyzyjnych na różnych szczeblach. Wskazując na różne aspekty możemy wyróżnić klasyfikacje gospodarki:

1) ze względu na sposób pozyskiwania dóbr i usług:
   - gospodarka naturalna,
   - gospodarka towarowo-pieniężna;
2) ze względu na mechanizmy regulacyjne:
   - gospodarka rynkowa,
   - gospodarka nakazowa,
   - gospodarka mieszana;
3) ze względu na siłę powiązań z podmiotami zewnętrznymi:
   - gospodarka otwarta,
   - gospodarka zamknięta,
   - gospodarka częściowo otwarta;
4) ze względu na poziom rozwoju społecznego:
   - gospodarka tradycyjna,
   - gospodarka przemysłowa,
   - gospodarka postindustrialna;
5) inne podziały:
   - gospodarka oparta na usługach,
   - gospodarka oparta na wiedzy,
   - gospodarka oparta na zasobach,
   - gospodarka energooszczędna (gospodarka niskoenergetyczna, gospodarka niskoemisyjna),
   - gospodarka ekstensywna,
   - gospodarka komunalna,

- gospodarka niedoboru,
- gospodarka samowystarczalna (https://plwiki.pl, dostęp: 05.07.2024).

Klasyfikacja gospodarki ze względu na wyżej wymienione aspekty pozwala zrozumieć charakter danej gospodarki oraz daje możliwość badaczom, ekonomistom analizować i porównywać gospodarki na różnych poziomach, co jest kluczowe w procesach decyzyjnych w przypadku, gdzie są wymagane działania naprawcze lub wsparcia. Ma to również znaczenie i wpływ na rozwijanie e-gospodarki w danym kraju lub regionie – oddziałuje na dostępność, charakter, rozwój. Reasumując, temat dotyczący gospodarki stanowi fundament funkcjonowania społeczeństwa wpływając na jakość życia. Ukazane zostały tylko kluczowe aspekty w celu zrozumienia dalszych rozważań. Zrozumienie różnych typów gospodarek jest kluczowe również w kontekście globalnej współpracy i handlu, ponieważ pozwala na lepsze dopasowanie strategii ekonomicznych między krajami. Ponadto, świadomość tych podziałów umożliwia także lepsze przewidywanie ewentualnych skutków działań gospodarczych na skalę lokalną i globalną.

Wraz z rozszerzającym się zjawiskiem nowych technologii, globalizacja wpłynęła w głównej mierze na handel, usługi oraz produkcję. Zatem e-gospodarka stanowi nowy model gospodarki z wykorzystaniem technologicznej rzeczywistości tworząc taką wirtualną arenę. Jak zaznacza Kisielnicki „Gospodarka elektroniczna to wymiana: towarów, usług i własności intelektualnej wszelakiego rodzaju przez media elektroniczne. Jest to też sposób prowadzenia działalności gospodarczej przez uniwersalne i powszechne sieci komputerowe. Gospodarka elektroniczna jest konsekwencją rozwoju technologicznego i konwergencji, czyli połączenia się i przenikania: technik przetwarzania danych, telekomunikacji, wiedzy" (Kisielnicki, 2008, s. 331). Zmieniające się uwarunkowania gospodarcze wymuszają wykorzystanie nowych technologii ze względów na m.in.: konkurencję (pozwalają na efektywniejszą produkcję i dostarczanie usług), łatwiejszy dostęp do rynków (globalny zasięg), innowację (udoskonalenie usług oraz idące za tym większe zyski). Jeżeli mowa o konkurencji to należy zauważyć, że fundamentalną cechą gospodarki elektronicznej jest koncentracja na zasobach niematerialnych, a zwłaszcza na kapitale intelektualnym (Dudek, 2011). Według D. Tapscott'a gospodarka elektroniczna to gospodarka wiedzy – zdolność wykorzystania wiedzy i umiejętności do tworzenia wartości, przychodów i zysków (Tapscott, 1998). E-gospodarka przenika także do każdego sektora gospodarczego niezależnie od produkcji towarów materialnych czy usług niematerialnych. Biorąc pod uwagę względy ekonomiczne można spodziewać się w przyszłości eliminacji z rynku gospodarki wykorzystującej tradycyjne papierowe dokumenty. Jest to skutkiem oddziaływania dwóch procesów odpowiedzialnych za rozwój technologii oraz za większe znaczenie informacji, która stała się w dzisiejszych czasach produktem. W ramach elektronicznej gospodarki prowadzona jest: m.in.:

- elektroniczna wymiana dokumentów,
- elektroniczna bankowość,
- elektroniczne zakupy,

- elektroniczny transfer środków pieniężnych,
- interaktywne systemy informacji głosowej,
- systemy rezerwacji (Borowiecki, Kwieciński, 2003).

Wszystko to przekłada się na zwiększenie produktywności, która powoduje wzrost standardów życia.

Rozwój gospodarki elektronicznej

Gospodarka elektroniczna zaczęła się kształtować w latach 90. XX wieku wraz z upowszechnieniem się Internetu oraz technologii cyfrowych. Nie można wskazać jednoznacznej daty, ponieważ jest to ciągły proces wdrażania technologii cyfrowych do aspektów gospodarki. W ramach e-gospodarki funkcjonuje wiele terminów z nią związanych. Najczęściej e-biznes nazywany jest e-handlem. Należy zauważyć pewną zależność, mianowicie tak jak tradycyjny handel jest częścią biznesu, tak handel elektroniczny jest częścią biznesu elektronicznego, a więc: e-handel (ang. *e-commerce*) < e-biznes (ang. *e-business*) < e-gospodarka (ang. *e-economy*) (Gregor, Stawiszyński, 2002). Oznacza to, że znaczenie e-gospodarki dla jednych przedsiębiorców może być tylko rozwinięciem rynku tradycyjnego, a dla innych może stanowić tą wirtualną arenę. W kontekście e-gospodarki, bardziej precyzyjnym terminem jest biznes elektroniczny (e-biznes), który stanowi jej bardziej szczegółowy obszar. Według A. Hartmana biznes elektroniczny stanowi wykorzystanie nowoczesnych technologii informacyjnych dla praktyki gospodarczej, której przedmiotem są procesy gospodarcze (Hartman, Sifonis, Kador, 2001). W tym kontekście jednym z tych procesów jest e-handel, który odbywa się za pomocą technologii informacyjnych.

Należy wskazać, że rozwój gospodarki elektronicznej jest zjawiskiem ciągle zmieniającym się, ewaluującym. W ostatnich dekadach dynamiczny rozwój technologii informacyjnych i komunikacyjnych zrewolucjonizował sposób, w jaki prowadzimy biznes. Transformacja cyfrowa, która trwa nieprzerwanie od kilkunastu lat, zmieniła i wciąż zmienia rzeczywistość, przynosząc społeczeństwu wiele korzyści (*Społeczeństwo informacyjne w Polsce w 2023 r.,* 2023). Automatyzacja procesów biznesowych, wykorzystanie sztucznej inteligencji oraz analizy danych to tylko niektóre z narzędzi, które wspierają rozwój gospodarki elektronicznej. Największy wzrost inwestycji w ten sektor notuje się w latach 2005-2015, po czym tempo wzrostu nieco spowolniło, jednak nie zatrzymało się całkowicie (Czas na cyfrową gospodarkę!, 2024). Spowolnienie procesów gospodarki elektronicznej wynika głównie z trzech głównych czynników: nasycenia rynku, wzrostu kosztów operacyjnych oraz trudności w znalezieniu odpowiednio wykwalifikowanych pracowników. Te czynniki powodują spowolnienie tempa innowacji i rozwoju w branży, utrudniając dynamiczny rozwój firm działających w tym sektorze. W 2017 roku Polska zajęła 23. miejsce w Indeksie Cyfrowej Gospodarki i Społeczeństwa (DESI), odnotowując postępy w korzystaniu z Internetu, infrastrukturze komunikacyjnej i dostępie do szerokopasmowej łączności mobilnej (Polska w indeksie gospodarki cyfrowej i społeczeństwa cyfrowego, 2024).

Po wyhamowaniu rozwoju gospodarki cyfrowej, kolejnym punktem zwrotnym stała się pandemia COVID-19, która skłoniła wiele firm do szybkiego przyjęcia i wdrożenia rozwiązań cyfrowych oraz pracy zdalnej. Te zmiany, chociaż początkowo były wynikiem kryzysu, mają teraz trwały wpływ na strategie biznesowe i długoterminowy rozwój przedsiębiorstw. Pandemia COVID-19 przyspieszyła proces digitalizacji i adaptacji technologicznej, nie tylko w zarządzaniu biznesowym, ale także w społeczeństwie jako całości. Organizacje z różnych sektorów, zmuszone do działań w warunkach związanych z pandemią, muszą stosować innowacyjne rozwiązania cyfrowe, aby kontynuować działalność. W obliczu konieczności ograniczenia kontaktów fizycznych i zamknięcia wielu tradycyjnych miejsc pracy, przedsiębiorstwa i konsumenci masowo zaczęli korzystać z rozwiązań cyfrowych. Od tego czasu rozwój gospodarki elektronicznej jest kontynuowany, napędzany rosnącym zapotrzebowaniem na usługi online, zdalną pracę oraz e-commerce. Technologie cyfrowe stały się nieodłącznym elementem codziennego życia, a ich dalsza ekspansja wydaje się nieunikniona.

Z kolei rok 2022 był przełomowy i istotny z perspektywy rozwoju elektronicznej gospodarki, odzwierciedlając dynamiczny postęp technologiczny oraz rosnące znaczenie handlu elektronicznego, które zostało przyspieszone przez pandemię COVID-19. Inflacja i widmo kryzysu gospodarczego skłoniły 76% polskich konsumentów do większych zakupów w Internecie (Raport e-Izby, 2023). Klienci zaczęli preferować wygodę i bezpieczeństwo zakupów online, co wpłynęło na dalszy rozwój e-comerce w Polsce. Przyspieszenie cyfryzacji w 2022 roku wymusiło na firmach inwestycje w technologie IT, logistykę oraz marketing cyfrowy, aby sprostać rosnącym oczekiwaniom klientów. Widoczne zmiany w zachowaniach konsumenckich wskazują na trwałą transformację sektora handlu, gdzie “sieć” staje się głównym kanałem sprzedaży.

Konkludując, nie jest prawdziwym twierdzeniem, że każde pojęcie kojarzone z biznesem elektronicznym znaczy to samo. Taką główną różnicą między tymi dwoma pojęciami jest to, że e-biznes to szersze pojęcie obejmujące prowadzenie działań biznesowych, w tym handlu za pomocą cyfryzacji, ale także obejmuje zarządzanie oraz marketing. Sam e-handel koncentruje się wyłącznie na sprzedaży i zakupie w sieci. Rozwój elektronicznej gospodarki na przestrzeni był charakteryzowany przez kolejne wzrosty i spadki, ale także ciągłą ewolucję. początkowo koncentrował się na głównym e-handlu, czyli sprzedaży i zakupach online. Dziś e-biznes to znacznie więcej niż tylko e-handel. Obejmuje on całościowe podejście do prowadzenia działalności gospodarczej w środowisku cyfrowym. Oprócz sprzedaży i zakupów online, e-biznes obejmuje również zarządzanie firmą przy użyciu technologii cyfrowych, marketing internetowy, obsługę klienta online, analizę danych, logistykę elektroniczną, oraz wiele innych aspektów związanych z prowadzeniem biznesu w erze cyfrowej. Rozwój oprogramowania jest produktem elektrycznym, który jest dostępny pod nową technologią, trendami społecznymi i zmieniającymi się potrzebami biznesowymi. Coraz większa penetracja Internetu, rozwój sztucznej inteligencji, Internetu rzeczy oraz blockchain zawierają tylko niektóre z czynników wywołujących tę ewolucję.

Zagrożenia e-gospodarki

W globalnym krajobrazie gospodarczym, elektroniczna gospodarka stanowi centralny filar rozwoju i innowacji. Wraz z jej pojawieniem się, pojawiły się zagrożenia, które muszą zostać uwzględnione. Zagrożenia związane z elektroniczną gospodarką obejmują przeróżne aspekty cyberbezpieczeństwa, ochrony danych osobowych, rozprzestrzeniania się zagrożeń z infrastruktury przemysłowej oraz ryzyko ataku związane z przestępczością internetową. W obecnych czasach cyfryzacji posiadając strukturę informacyjną związani jesteśmy ze szczególną podatnością na zagrożenia czyhające w sieci elektronicznej. Niewątpliwie jednym z najbardziej powszechnych niebezpieczeństw jest utrata informacji mogąca być skutkiem nieuprawnionego dostępu do danych jak również kwestią przypadku, błędu czy awarii.

Wśród zagrożeń związanych z elektroniczną gospodarką istnieje szereg działań, których celem jest nieuprawniony dostęp do danych oraz infrastruktury. Złośliwe oprogramowanie typu malware stanowi istotne zagrożenie, przenikając przez pocztę elektroniczną lub odwiedzane strony internetowe. Jego głównym celem jest wyłudzenie pieniędzy poprzez kradzież, zaszyfrowanie lub usunięcie danych, a także umożliwienie hakerom zdalnego dostępu. Rodzaje malware'u, takie jak robaki czy konie trojańskie, posiadają różnorodne funkcje zaprogramowane przez hakerów. Robak oraz koń trojański to dwa różne rodzaje złośliwego oprogramowania, które stanowią zagrożenie dla bezpieczeństwa systemów informatycznych. Robak jest programem komputerowym, który ma zdolność do samodzielnego replikowania się i rozprzestrzeniania przez sieć, infekując kolejne komputery. Można rzec, że przedostaje się „pełzając" z komputera na komputer za pomocą sieci oraz zaprogramowane przez hakera działania. Posiada zwykle wbudowane instrukcje, które pozwalają mu na automatyczne rozprzestrzenianie się oraz wykonywanie określonych działań na zainfekowanych systemach, na przykład kradzież danych czy wysyłanie spamu. Z kolei koń trojański jest rodzajem złośliwego oprogramowania, które podszywa się pod legalne lub pożądane aplikacje lub pliki, aby uzyskać nieuprawniony dostęp do systemu. Nazwa „koń trojański" nawiązuje do mitu o Troi, gdzie wierzono, że zrobiona z drewna figura konia była darem, podczas gdy wewnątrz znajdowały się ukryte siły wroga. Podobnie, koń trojański wydaje się być niewinnym plikiem lub programem, ale po uruchomieniu wykonuje szkodliwe działania, takie jak kradzież danych, uszkodzenie plików czy umożliwienie hakerom zdalnego dostępu do systemu. Coraz bardziej zaawansowane i zróżnicowane formy koni trojańskich oraz ich rosnąca funkcjonalność sprawiają, że przestarzałe zabezpieczenia stają się główną przyczyną ich występowania (Protasowicki, 2017).

Phishing, będący kolejnym zagrożeniem, polega na próbie wyłudzenia danych poprzez podszywanie się pod wiarygodne źródło, często za pomocą fałszywych e-maili lub komunikatów SMS. Szczególną odmianą jest spear phishing, który wykorzystuje personalizowane dane w celu osiągnięcia większej skuteczności. Oprócz tego, szpiegostwo korporacyjne stanowi zagrożenie ze strony pracowni-

ków lub osób mających dostęp do poufnych informacji, które mogą zostać przekazane niepowołanym osobom. Phishing został po raz pierwszy publicznie wykorzystany i zarejestrowany 2 stycznia 1996 roku (Malwarebytes, 2023). Sytuacja miała miejsce w połowie lat 90., gdzie hakerzy podszywali się pod pracownika AOL (jeden z dostawców usług internetowych powstały w 1983 r.) i wysyłali wiadomości z prośbą o ujawnienie hasła – zweryfikowanie konta. Pokazuje to, że ofiarą phishingu może być każdy z nas, dlatego powinniśmy nauczyć się skutecznie rozpoznawać próby oszustwa. Istnieje wiele rodzajów tego przestępstwa:

- Phishing e-mail – najczęściej w formie wiadomości e-mail, celem kliknięcie złośliwych łączy lub pobranie szkodliwego oprogramowania;
- Vishing – wiąże się z rzeczywistą osobą mówiącą po drugiej stronie telefonu;
- Smishing – przypomina phishing e-mail z tą różnicą, że odbywa się za pośrednictwem wiadomości SMS;
- Pharming – cyberatak, który przekierowuje cały ruch witryny do innej złośliwej witryny;
- Spear phishing – wykorzystanie danych osobowych w celu wyrządzenia maksymalnych szkód;
- Whaling – podobny do ataku typu spear phishing, z tą różnicą, że celem jest „wieloryb", czyli wysoko postawiony cel, a nie zwykła osoba lub sieć małej firmy (Kurkiewicz, 2023).

Wśród celowych działań możemy wyróżnić jeszcze szpiegostwo korporacyjne, które jest celowym działaniem pracowników lub osób z dostępem do kluczowych informacji, którzy przekazują je osobom nieupoważnionym lub celowo sabotują działanie systemu organizacji. Jest to forma działania, która może prowadzić do poważnych konsekwencji dla firmy, w tym utraty poufnych danych, obniżenia reputacji oraz strat finansowych. Praktyki szpiegowskie mogą obejmować kradzież informacji handlowych, przekazywanie tajemnic handlowych konkurencji lub działania zmierzające do zakłócenia pracy systemów komputerowych. Firmy muszą stosować skuteczne środki bezpieczeństwa, takie jak monitorowanie aktywności pracowników i ścisłe zarządzanie dostępem, aby minimalizować ryzyko szpiegostwa korporacyjnego. Ponadto, edukacja pracowników w zakresie bezpieczeństwa informacji oraz świadomość zagrożeń są kluczowe dla zapobiegania tego typu działaniom. W dzisiejszym świecie, gdzie dane są jednym z najcenniejszych aktywów, walka ze szpiegostwem korporacyjnym jest niezwykle istotna dla zachowania konkurencyjności i integralności firm.

W przeciwieństwie do celowych działań, zagrożenia niecelowe wynikają z ludzkich błędów lub czynników losowych. Błędy ludzkie mogą obejmować nieuwagę w zabezpieczeniach systemowych, niezmienianie haseł, czy brak odpowiedniej wiedzy w zakresie cyberbezpieczeństwa. Z kolei czynniki losowe, takie jak zalanie wodą, pożary czy uszkodzenia sprzętu, mogą spowodować poważne szkody dla infrastruktury elektronicznej. Wszystkie te zagrożenia wymagają systematycznego monitorowania oraz zastosowania skutecznych środków ochrony, aby minimalizować ryzyko dla gospodarki elektronicznej.

Bezpieczeństwo e-gospodarki

W erze cyfrowej, gdzie dane odgrywają kluczową rolę w niemal każdym aspekcie życia, bezpieczeństwo informacji staje się priorytetem. Technologie telekomunikacyjne i informacyjne kształtują współczesny rozwój społeczeństwa nie tylko w skali państw, ale również w skali globalnej (Monarcha-Matlak, 2011). Przedsiębiorstwa, instytucje rządowe i indywidualni użytkownicy muszą sprostać coraz większym wyzwaniom związanym z ochroną danych. Cyberprzestępczość i zagrożenia takie jak malware, ransomware czy phishing są na porządku dziennym. Dlatego niezbędne jest wdrożenie skutecznych mechanizmów ochrony, aby zapobiegać utracie, kradzieży i nieautoryzowanemu dostępowi do danych. Informacja w dzisiejszym świecie stała się produktem wymagającym szczególnej ochrony. Biorąc ten fakt pod uwagę ważnym stanowiskiem są dostosowane mechanizmy zabezpieczeń na każdym poziomie jej przechowywania i przetwarzania. Możemy spotkać wiele różnych metod i sposobów produktywnego zabezpieczenia systemów przed zagrożeniami.

Bez wątpienia użytkowany sprzęt odgrywa kluczową rolę w ochronie przed zagrożeniami. W dzisiejszym świecie, gdzie wiele działań przeniosło się do sfery wirtualnej, a większość firm działa online, zabezpieczenie urządzeń przed nieuprawnionym dostępem staje się priorytetem. Technologia stała się nieodłącznym elementem codziennego życia i pracy, co oznacza, że odpowiednie zabezpieczenia są niezbędne do ochrony wrażliwych danych. Cyberprzestępcy stale poszukują luk w systemach, aby przejąć dane lub zakłócić działanie przedsiębiorstw. Dlatego stosowanie aktualnych i skutecznych środków ochrony jest absolutnie konieczne. Nie chodzi tylko o fizyczne zabezpieczenia, ale również o zabezpieczenie sieci czy też rozwaga przy podłączaniu się pod sieć w miejscach publicznych. Obejmuje to zarówno oprogramowanie antywirusowe, jak i firewalle, szyfrowanie danych oraz regularne aktualizacje systemów operacyjnych. Z badań dotyczących zabezpieczeń systemów informatycznych w urzędach gmin wynika, że najczęściej wdrażanymi rozwiązaniami są programy antywirusowe i firewalle korporacyjne (Lisiak-Felicak, Szmit, 2016). Ponadto, edukacja użytkowników na temat bezpiecznego korzystania z technologii jest równie ważna. Tylko w ten sposób można zapewnić kompleksową ochronę przed różnorodnymi zagrożeniami cyfrowymi. Należy również zwracać uwagę, aby nie zostawiać urządzeń w miejscach bez nadzoru osoby uprawnionej. Ważne jeszcze jest to, aby kontrolować dostęp do systemów przechowujących dane. Ma to odniesienie do takich zabezpieczeń jak: czytnik odcisków palców, konta użytkowników oraz ograniczenia dostępu do danych wyszczególnionych odbiorców.

Kolejnym istotnym elementem, który przyczynia się do bezpieczeństwa gospodarki elektronicznej, jest komercyjne oprogramowanie. Jest ono projektowane z myślą o zabezpieczeniu danych oraz procesów biznesowych przed cyberzagrożeniami. Proces rozwoju oprogramowania jest ciągły i nieustanny, ponieważ zawsze pojawiają się nowe potrzeby i wymagania, które wymagają zmian i ulepszeń (Karwatka, 2013). Najistotniejszym elementem jest to, iż firmy zajmujące się ko-

mercyjnym oprogramowaniem inwestują ogromne środki w rozwój i aktualizację swoich produktów, aby sprostać rosnącym wyzwaniom bezpieczeństwa. Bowiem regularne aktualizacje i łatki zabezpieczające są niezbędne, aby chronić przed nowymi typami ataków oraz reagować na potencjalne zagrożenia. Wysokiej jakości oprogramowanie komercyjne oferuje zaawansowane funkcje, takie jak szyfrowanie danych czy systemy wykrywania włamań. Dodatkowo, dostawcy takiego oprogramowania często oferują wsparcie techniczne i szkolenia dla użytkowników. Dzięki temu przedsiębiorstwa mogą skupić się na swojej działalności, mając pewność, że ich cyfrowe zasoby są chronione. W efekcie, komercyjne oprogramowanie stanowi podstawę stabilnego i bezpiecznego funkcjonowania e-gospodarki. Naturalnym faktem jest, że komercyjne oprogramowania mają swoich zwolenników jak i przeciwników. Przeciwnicy będą za tym, iż nie zawsze komercyjne oprogramowania jest jedynym słusznym wyborem ponieważ własne rozwiązania mogą być równie skuteczne przy zachowaniu dbałości o bezpieczeństwo. Tak więc wybór powinien być dostosowany do indywidualnych potrzeb. Wspomniane komercyjne oprogramowania na pewno sprawdzą się w przypadku większych sektorów, gdzie nie jest się w stanie kontrolować wszystkiego odrębnie.

Przepisy prawne dotyczące elektronicznej gospodarki

Przepisy prawne dotyczące e-gospodarki w dzisiejszym cyfrowym świecie są istotne dla skutecznego zarządzania oraz regulowania szeroko pojętego bezpieczeństwa (ochrona danych osobowych, cybernetyczne), poufności i sprawiedliwości. Przepisy wynikające z prawa będą się różnić w zależności od kraju. Przepisy prawne dotyczące e-gospodarki zarówno na poziomie Unii Europejskiej, jak i w poszczególnych krajach, takich jak Polska, pełnią kluczową rolę w zapewnieniu skutecznego zarządzania oraz regulowania różnorodnych aspektów cyfrowego świata.

W Unii Europejskiej, Dyrektywa o handlu elektronicznym 2000/31/WE (https://eur-lex.europa.eu, dostęp: 05.07.2024) stanowi istotny akt, który reguluje kwestie związane z handlem elektronicznym I świadczeniami usług w środowisku cyfrowym. Zawarte są w niej m.in:

- Zasady kraju pochodzenia: dostawca usług online podlega przepisom prawnym swojego kraju, a nie każdego kraju, do którego kierowane są usługi;
- Obowiązek informacyjny: dostawcy mają obowiązek poinformowania o cenach, firmie, opisie usług;
- Zasada poufności: zabezpieczenie danych osobowych oraz informacja w sprawie prywatności.

Dyrektywa ta stanowi pewnego rodzaju piętno e-handlu i stanowi podstawę dla wielu późniejszych przepisów i regulacji obejmujących świadczenie usługi online. Dodatkowo, dyrektywa określa obowiązek dostawców informowania o cenach, firmie oraz opisie usług, co zwiększa przejrzystość transakcji. Zasada poufności zawarta w Dyrektywie stanowi istotny element ochrony danych osobowych konsumentów, co przekłada się na ich większe zaufanie do e-handlu. Ustalenia Dyrektywy tworzą również podstawy dla późniejszych regulacji dotyczących han-

dlu elektronicznego w UE, co ułatwia harmonizację przepisów między państwami członkowskimi. Dzięki odpowiednim uregulowaniom, konsumentom zapewniona jest większa ochrona praw, a podmiotom działającym w e-gospodarce równoprawne warunki konkurencji, co sprzyja rozwojowi rynku i innowacjom.

Kolejnym aktem obowiązującym w Unii Europejskiej jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (https://eur-lex.europa.eu/, dostęp: 05.07.2024), która reguluje różnorodne aspekty płatnicze. Dyrektywa umożliwia firmom konkurowanie poprzez oferowanie różnorodnych rozwiązań płatniczych. Jednym z istotnych elementów tej Dyrektywy jest wzmocnienie zabezpieczenia transakcji poprzez wprowadzenie uwierzytelniania dwuskładnikowego, co zwiększa bezpieczeństwo operacji finansowych online dla konsumentów. Ponadto, Dyrektywa umożliwia otwarty dostęp do kont bankowych dla firm trzecich, co sprzyja innowacyjności i konkurencyjności na rynku usług płatniczych, dając konsumentom większy wybór rozwiązań płatniczych. Dzięki właściwie uregulowanym usługom płatniczym, konsumentom zapewniona jest większa ochrona ich danych finansowych oraz transakcji, co buduje zaufanie do korzystania z usług online. Dodatkowo, otwarty dostęp do kont bankowych dla firm trzecich sprzyja innowacjom, co może prowadzić do powstania nowych, bardziej wydajnych i kliento-zorientowanych rozwiązań płatniczych. Dzięki harmonizacji przepisów w ramach UE, podmioty działające w e-gospodarce mają równoprawne szanse na konkurowanie na rynku usług płatniczych, co przyczynia się do dynamicznego rozwoju sektora finansowego. W rezultacie, kwestie legislacyjne w obszarze usług płatniczych sprzyjają zarówno ochronie konsumentów, jak i rozwojowi innowacyjności oraz konkurencyjności na rynku.

Dyrektywa o prawach konsumentów (Dyrektywa 2011/83/UE) to akt regulujący prawa osób nabywających produkty lub usługi w sytuacji, gdy umowa zawierana jest na odległość. Określa ona prawa, obowiązki oraz zasady odstąpienia od umowy dla konsumentów, którzy są końcowymi odbiorcami w łańcuchu ekonomicznym. Korzyści kwestii legislacyjnych dla konsumentów są liczne. Przede wszystkim, zapewniają one większe bezpieczeństwo i pewność prawna podczas dokonywania transakcji na odległość, co buduje zaufanie do rynku e-commerce. Ponadto, określenie jasnych zasad odstąpienia od umowy daje konsumentom poczucie kontroli nad swoimi decyzjami zakupowymi oraz umożliwia uniknięcie niepotrzebnego ryzyka. Dla sprzedawców i firm również istnieją korzyści wynikające z kwestii legislacyjnych. Stosowanie klarownych przepisów ułatwia zrozumienie i przestrzeganie regulacji, co może przyczynić się do poprawy relacji z klientami oraz zwiększenia zaufania do marki. Dodatkowo, regulacje te promują uczciwą konkurencję na rynku, eliminując nieuczciwe praktyki handlowe i poprawiając jakość usług świadczonych przez różnych dostawców. W rezultacie, kwestie legislacyjne dotyczące praw konsumentów przyczyniają się do równowagi i sprawiedliwości na rynku, zapewniając korzyści zarówno dla konsumentów, jak i dla przedsiębiorców.

W Polsce, przepisy prawne stanowią kompleksowy zbiór regulacji dotyczących różnorodnych aspektów e-gospodarki. Obejmują one kluczowe obszary, takie jak handel elektroniczny, ochrona danych osobowych oraz zastosowanie podpisu elektronicznego. Te uregulowania mają na celu zapewnienie bezpieczeństwa, integralności oraz skuteczności transakcji online w Polsce.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (SUDE) (Dz.U. 2020 poz. 344, tj.) jest fundamentem regulującym świadczenie usług online w Polsce, określając prawa i obowiązki dostawców oraz użytkowników, co przyczynia się do zapewnienia przejrzystości i bezpieczeństwa transakcji internetowych. Dodatkowo, ustawa stanowi istotną podstawę prawna ochrony danych osobowych, chroniąc prywatność użytkowników w środowisku online. Przepisy, które wynikają z ustawy zawierają szereg zasad, które służą zapewnieniu uczciwemu i bezpiecznemu świadczeniu usług na odległość. Korzyści płynące z kwestii legislacyjnych, takich jak SUDE, są znaczące dla konsumentów oraz innych podmiotów. Uregulowanie świadczenia usług drogą elektroniczną zapewnia konsumentom klarowność i pewność co do warunków korzystania z usług online. Dzięki temu mogą oni świadomie podejmować decyzje dotyczące zakupów czy korzystania z różnorodnych platform internetowych. Ponadto, SUDE stawia wysokie wymagania dotyczące ochrony danych osobowych, co sprzyja zachowaniu prywatności użytkowników i buduje zaufanie do firm działających online. Legislacja ta również chroni konsumentów przed nieuczciwymi praktykami, wymuszając na dostawcach usług przestrzeganie określonych standardów etycznych i uczciwej konkurencji. Dzięki temu klienci mogą mieć pewność, że są traktowani zgodnie z przepisami prawa i że ich prawa są respektowane. SUDE przyczynia się także do poprawy bezpieczeństwa transakcji internetowych poprzez wymóg stosowania odpowiednich środków zabezpieczających, co zmniejsza ryzyko kradzieży danych czy oszustw online. To z kolei zachęca konsumentów do częstszego korzystania z usług online, co sprzyja rozwojowi gospodarki cyfrowej i innowacji. Ponadto SUDE promuje również zasadę swobody przepływu danych wewnątrz Unii Europejskiej, ułatwiając tym samym dostęp do różnorodnych usług online dla konsumentów na terenie całej UE. Dzięki temu mogą oni korzystać z ofert różnych firm z różnych krajów bez obaw o przeniesienie swoich danych poza granice Unii.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2024 poz. 30, tj.) jest kluczowym aktem prawnym w Polsce, regulującym różnorodne usługi finansowe, takie jak płatności kartami, przelewy czy inkaso (zbieranie płatności od dłużników przez firmę lub osobę trzecią obejmuje negocjacje, upomnienia, procedury prawne np. przy niezapłaconych fakturach i innych zobowiązaniach finansowych) oraz też działalność banków lub innych podmiotów tego typu wprowadzając zabezpieczenia transakcji, ochrony konsumentów. Ustawa ta precyzyjnie reguluje szeroki zakres usług finansowych. Dzięki tym regulacjom, klienci mogą korzystać z usług płatniczych w sposób bezpieczny i przejrzysty, bez obawy o nadużycia czy utratę środków. Ponadto, ustawa ta stawia konkretne wymagania przed instytucjami finansowymi, co sprzyja poprawie jakości świadczonych usług oraz

zwiększeniu zaufania klientów do sektora bankowego i podobnych podmiotów. Zapewnienie stabilności i transparentności transakcji przekłada się także na lepsze funkcjonowanie całego rynku finansowego, co może sprzyjać rozwojowi gospodarczemu kraju. Dodatkowo, uregulowanie procedur inkasa przyczynia się do skutecznego odzyskiwania należności, co może być istotne dla firm i osób trzecich zajmujących się windykacją. W rezultacie, kwestie legislacyjne w zakresie usług płatniczych mają istotne korzyści zarówno dla konsumentów, jak i dla instytucji finansowych oraz innych podmiotów związanych z sektorem finansowym, przyczyniając się do stabilności i zaufania na rynku.

Istotne znaczenie w kontekście e-gospodarki ma Ustawa o prawie autorskim i prawach pokrewnych, która kontekście e-gospodarki porządkuje prawa i obowiązki twórców i autorów szeroko rozumianych dzieł oraz osób wykorzystujących to poprzez kopiowanie bądź elektroniczny handel dziełami. Ta legislacja zapewnia ochronę intelektualną dla twórców, co jest kluczowe w erze cyfrowej, gdzie łatwość kopiowania i dystrybucji dzieł jest znacznie większa niż w tradycyjnych mediach. Dzięki tym regulacjom konsumenci mogą mieć pewność, że korzystają z legalnych źródeł i produktów, co z kolei może wpłynąć na rozwój uczciwej konkurencji na rynku. Ponadto, ustawa ta umożliwia twórcom uzyskanie zasłużonych wynagrodzeń za wykorzystanie ich dzieł, co jest istotne dla zachęcania do twórczości i innowacji. W kontekście e-gospodarki, gdzie treści cyfrowe stanowią kluczowy element działalności wielu firm i przedsiębiorstw, odpowiednie uregulowania prawne są niezbędne dla zapewnienia stabilności i rozwoju rynku. Dodatkowo, ustawa ta może być również korzystna dla konsumentów, ponieważ promuje rozwój różnorodnych treści i dziedzin kultury, co z kolei może wpływać na bogactwo oferty dostępnej dla odbiorców. W ten sposób, kwestie legislacyjne w zakresie prawa autorskiego i praw pokrewnych mają istotne znaczenie dla zapewnienia równowagi między ochroną praw twórców a korzyściami dla konsumentów i rozwojem e-gospodarki.

Podsumowanie

Elektroniczna gospodarka jest to złożony obszar gospodarki oparty na cyfrowych rozwiązaniach. W dzisiejszym świecie niemal każdy ma dostęp do cyfrowego świata. Właśnie ten technologiczny rozwój sprawił, że e-gospodarka stała się integralną częścią życia i zaczęła wypierać tradycyjną gospodarkę. Obok znaczących korzyści e-gospodarka nie jest pozbawiona wyzwań i zagrożeń, o których musimy pamiętać. Należy zdać sobie sprawę z tego, iż najcenniejszym produktem stała się informacja, którą często sami udostępniamy narażając się na zagrożenia, na co koniecznie należy uważać. Ciężko jednak jednoznacznie stwierdzić i odpowiedzieć na pytanie w którą stronę ten rozwój technologiczny gospodarki zmierza. Sfalsyfikowana zostaje zatem hipoteza badawcza pokazując, że w przypadku e-gospodarki nie jest możliwe jednoznaczne określenie przyszłego kierunku rozwoju. Mają na to wpływ głównie zmienność, niespodziewane czynniki, ciągły rozwój ale i również ciągle idące zagrożenia tym śladem. Podążanie za zmianami

stanowi centralny element sukcesu w dzisiejszym cyfrowym świecie. Dynamiczny charakter tej dziedziny pokazuje, że przewidywanie w tym przypadku jest niezwykle trudne, a badania pozostają otwarte na różnorodność scenariuszy. Kluczowym elementem sukcesu w tym środowisku jest więc zdolność do szybkiej adaptacji i reagowania na zmiany, aby utrzymać konkurencyjność i zapewnić bezpieczeństwo danych oraz transakcji online. W miarę jak e-gospodarka będzie się rozwijać, istotne będzie również monitorowanie i regulowanie jej funkcjonowania, aby maksymalnie wykorzystać jej potencjał przy minimalizacji ryzyka dla społeczeństwa i gospodarki.

Literatura

Artykuły i pozycje książkowe

1) Borowiecki, R., Kwieciński, M. (2003). *Monitorowanie otoczenia: przepływ i bezpieczeństwo informacji w stronę inteligencji przedsiębiorstwa*. Kraków: Zakamycze.
2) Fundacja Digital Poland. (2024). Raport "Czas na cyfrową gospodarkę! 4. edycja".
3) Główny Urząd Statystyczny. (2023). *Społeczeństwo informacyjne w Polsce w 2023 r.* Warszawa, Szczecin.
4) Gregor, B., Stawiszyński, M. (2002). *E-commerce*. Bydgoszcz: Branta.
5) Hartman, A., Sifonis, J., Kador, J. (2001). *E-biznes: strategie sukcesu w gospodarce internetowej: sprawdzone metody organizacji przedsięwzięć e-biznesowych*. Warszawa: K.E. Liber.
6) Karwatka, P. (2013). *Technologia w ecommerce. Teoria i praktyka. Poradnik menedżera*. Gliwice: Helion.
7) Kisielnicki, J. (2008). *MIS – systemy informatyczne zarządzania*. Warszawa: Placet.
8) Kurkiewicz, K. (2023). *System medialny jako determinanta bezpieczeństwa we współczesnym świecie*. W: J. Woźniak (red.), *Cyfryzacja i innowacje w organizacjach oraz ich uwarunkowania* (91-92).
9) Lisiak-Felicak, D., Szmit, M. (2016). *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*. Kraków: European Association for Security.
10) Monarcha-Matlak, A. (2011). *Obowiązki administracji w komunikacji elektronicznej*. Warszawa: Wolters Kluwer Polska.
11) Musiałkiewicz, J., Kwiatkowski, G. (2021). *Podstawy przedsiębiorczości 2.0*. Warszawa: Ekonomik.
12) Nerć-Pełka, A., Wysocka, A. (2012). *Gospodarka i społeczeństwo – współczesne wyzwania*. Szczecin: Zeszyty Naukowe 735.
13) Noga, M. (2000). *Makroekonomia*. Wrocław: Akademia Ekonomiczna im. Oskara Langego.
14) Piwowarski, J., Zachuta, A. (2013). *Pojęcie bezpieczeństwa w naukach społeczno-prawnych*. Kraków: Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego Apeiron w Krakowie.

15) Protasowicki, I. (2017). *RAT – Zagrożenie każdego użytkownika sieci globalnej.* Warszawa: Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji.
16) Runge, A., Runge, J. (2008). *Słownik pojęć z geografii społeczno-ekonomicznej*. Katowice: Videograf Edukacja.
17) Tapscott, D. (1998). *Gospodarka Cyfrowa*. Warszawa: Business Press.
18) Zięba, R. (2005). *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych.* Toruń: Grado.

Źródła internetowe

1) Encyklopedia PWN. Pobrane z: https://encyklopedia.pwn.pl/ (dostęp: 05.07.2024).
2) Grantthornton. (2020). *Phishing – największe zagrożenie dla cyberbezpieczeństwa.* Pobrane z: https://grantthornton.pl/publikacja/phishing-najwieksze-zagrozenie-dla-cyberbezpieczenstwa/ (dostęp: 05.07.2024).
3) Komisja Europejska. (2024). *Polska w indeksie gospodarki cyfrowej i społeczeństwa cyfrowego.* Pobrane z: https://digital-strategy.ec.europa.eu/pl/policies/desi-poland (dostęp: 11.07.2024).
4) Malwarebytes. (2023). *Phishing.* Pobrane z: https://pl.malwarebytes.com/phishing/ (dostęp: 05.07.2024).
5) PlWiki. (2023). *Gospodarka*. Pobrane z: https://plwiki.pl/Leksykon/Gospodarka (dostęp: 05.07.2024).
6) Raport e-Izby. (2023). *Dekada polskiego e-commerce 2013-2023*. Pobrane z: https://eizba.pl/wp-content/uploads/2023/02/Raport_e-Izby_Dekada_polskiego-e-commerce_2023.pdf (dostęp: 05.07.2024).
7) *Słownik języka polskiego PWN.* Pobrane z: https://sjp.pwn.pl/sjp/gospodarka;2462496.html (dostęp: 05.07.2024).

Akty prawne

1) Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym). Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32000L0031 (dostęp: 05.07.2024).
2) Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady. Tekst mający znaczenie dla EOG. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32011L0083 (dostęp: 05.07.2024).
3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego,

zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE. Tekst mający znaczenie dla EOG. Pobrane z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32015L2366 (dostęp: 05.07.2024).
4) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483).
5) Traktat ustanawiający Konstytucję dla Europy (Dz. Urz. UE C 310, t. 47, 16.12.2004).
6) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2020, poz. 344, tj.).
7) Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2024, poz. 30, tj.).