

Mateusz KUBIEŃ¹, Natalia BOCZAR², Damian KOLNY³,
Robert DROBINA⁴

Opiekun naukowy: Robert DROBINA

ROZWÓJ TECHNOLOGICZNY PRZEDSIĘBIORSTW PRODUKCYJNYCH W KONTEKŚCIE CYFROWEJ TRANSFORMACJI I CYBERBEZPIECZEŃSTWA

Streszczenie: Dynamiczny rozwój technologii informatycznych wywiera coraz większy wpływ na sposób funkcjonowania przedsiębiorstw produkcyjnych. Wykorzystanie najnowszych technologii informatycznych otwiera przed przedsiębiorstwami nowe, ciekawe możliwości. Celem niniejszego opracowania jest przedstawienie technologii informatycznych oraz sposobu ich wykorzystania w przedsiębiorstwach produkcyjnych wraz z potencjalnymi zagrożeniami w kontekście cyberbezpieczeństwa. Artykuł ma charakter przeglądowy w zakresie transformacji cyfrowej przedsiębiorstw produkcyjnych w dobie Przemysłu 4.0.

Słowa kluczowe: cyfryzacja, technologia, zarządzanie produkcją, Internet, chmura obliczeniowa

TECHNOLOGICAL DEVELOPMENT OF PRODUCTION ENTERPRISES IN THE CONTEXT OF DIGITAL TRANSFORMATION AND CYBERSECURITY

Summary: Dynamic development of information technologies has an increasing impact on the way production companies operate. The use of the latest information technologies opens up new and interesting opportunities for enterprises. The purpose of this paper is to present new information technologies and the way they are used by manufacturing companies, along with potential threats in the context of cybersecurity. The article is a review in the field of digital transformation of manufacturing enterprises in the age of Industry 4.0.

Keywords: digitization, technology, production management, Internet, cloud computing

¹ inż. Mateusz Kubień, Akademia Techniczno-Humanistyczna w Bielsku-Białej, Wydział Budowy Maszyn i Informatyki, Inżynieria Zarządzania Przedsiębiorstwem, mateusz.kubien01@gmail.com

² Natalia Boczar, Uniwersytet Jagielloński email: chempra111@wp.pl

³ mgr inż. Damian Kolny, Akademia Techniczno-Humanistyczna w Bielsku-Białej, email: dkolny@ath.bielsko.pl

⁴ dr hab. inż., prof. ATH Robert Drobina Akademia Techniczno-Humanistyczna w Bielsku-Białej, Wydział Budowy Maszyn i Informatyki, email: rdrobina@ath.bielsko.pl

1. Cyfrowa transformacja w aspekcie rozwoju technologicznego w przedsiębiorstwach produkcyjno-usługowo-handlowych

Jedną z najbardziej dynamicznych i wpływowych zmian obecnych czasów jest cyfryzacja gospodarki i społeczeństwa. Otwiera ona nowe możliwości nie tylko w życiu codziennym, ale również w tworzeniu współczesnych modeli biznesowych. Problemem jest natomiast niepewność, którą niesie za sobą cyfryzacja oraz inne zagrożenia wiążące się między innymi ze społecznymi skutkami automatyzacji procesów wytwórczych lub szeroko rozumianym bezpieczeństwem (w tym problemy związane bezpieczeństwem danych). Poprzez ciągłe przenikanie się świata rzeczywistego oraz wirtualnego cyfryzacja staje się jednym z głównych motorów innowacji i zmian.

Jako kluczowe czynniki napędzające rozwój gospodarki cyfrowej wymienia się obecnie:

- Internet Rzeczy (ang. Internet of Things – IoT; jest to termin określający jedną z najnowszych koncepcji informatycznych polegającą na połączeniu materialnych przedmiotów ze sobą z internetowymi zasobami za pomocą rozbudowanej i nowoczesnej sieci komputerowej [27]) oraz Internet Wszecznego (ang. Internet of Everything – IoE;) termin określający sieć łączącą ludzi, procesy, dane i przedmioty za pomocą sieci komputerowej,
- wszechobecna łączność,
- aplikacje i usługi oparte na chmurze obliczeniowej,
- analitykę dużych zbiorów danych,
- automatyzację i robotyzację procesów produkcyjnych,
- wielokanałowe oraz wszechkanałowe modele dystrybucji produktów i usług.

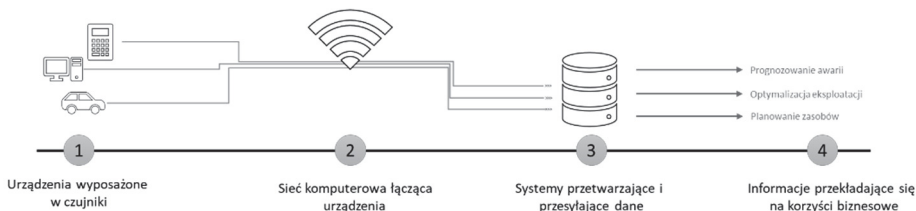
Aby sprostać zmianom, jakie niesie za sobą postępująca cyfryzacja, pojedyncze przedsiębiorstwa, jak i całe sektory gospodarcze, zmuszone są do dokonywania tzw. transformacji cyfrowej. W przypadku przedsiębiorstw transformacja cyfrowa jest procesem polegającym na transformacji modeli biznesowych oraz optymalizacji procesów wewnątrz organizacji. Proces ten skupia się na tworzeniu cyfrowego środowiska pracy i zaangażowaniu pracowników, a także klientów przy użyciu różnych kanałów komunikacji [29].

Adaptacja do funkcjonowania w warunkach gospodarki cyfrowej przejawia się między innymi przez powstawanie takich koncepcji jak np. Przemysł 4.0 (ang. *Industry 4.0*), oraz jej pochodnych jak Logistyka 4.0 (ang. *Logistics 4.0*) oraz Motoryzacja 4.0 (ang. *Automotive 4.0*).

Transformacja cyfrowa jest szczególnym rodzajem zmiany organizacyjnej w obrębie przedsiębiorstwa, sektora jak również administracji publicznej oraz całych gospodarek. Ma ona wpływ na trzy obszary organizacji [14]:

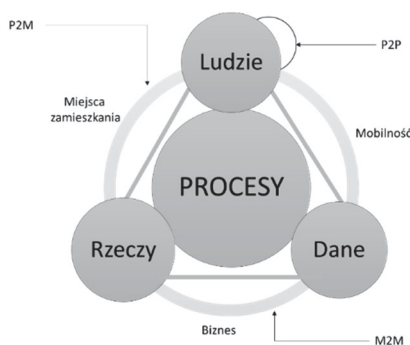
- doświadczenia klientów organizacji - wiąże się to ze zrozumieniem potrzeb klientów, wprowadzenie większej ilości kanałów komunikacji z klientami oraz elementów samoobsługi,
- procesy organizacyjne – zmiana dotyczy zarówno procesów wewnątrz organizacji, środowiska pracy, jak również mechanizmów monitorowania wydajności,
- model działania przedsiębiorstwa – dotyczy produktów lub usług, jakie przedsiębiorstwo dostarcza na rynek bądź rynki.

People-to-Machine) oraz M2M (ang. *Machine-to-Machine*). Istotę funkcjonowania takiego rozwiązania przedstawiono na Rysunku 2.



Rysunek 2. Istota funkcjonowania rozwiązań opartych na Internecie Rzeczy [2, 14, 30]

Obecnie rozwój Internetu Rzeczy jest napędzany dzięki ogromnemu postępowi jaki następuje w zakresie technologii mobilnych. Dowodem na rozwój w tym zakresie jest tzw. mobilna rewolucja – w 2014 roku, po raz pierwszy liczba użytkowników korzystających z Internetu za pomocą mobilnych urządzeń przekroczyła liczbę podłączonych do sieci komputerów stacjonarnych. Coraz częściej mówi się również o Internecie Wszeczhaczy, czyli sieci przedmiotów, danych, procesów, smartfonów oraz specjalnego oprogramowania umożliwiającego stałą łączność. Podłączenie do sieci jest również możliwe za pomocą specjalnych czujników lub sensorów, zarówno w przypadku przemysłu, jak również gospodarstw domowych. Internet Wszeczhaczy został przedstawiony na Rysunku 3 [25].



Rysunek 3. Istota Internetu Wszeczhaczy [2, 14, 30]

Jedną z kluczowych rzeczy, której zadaniem jest ułatwienie przetwarzania danych, jest tzw. chmura obliczeniowa (ang. *cloud computing*). Jest to model rozproszonego przetwarzania danych, który jest oparty na korzystaniu z usługi dostarczanej przez podmioty zewnętrzne, dostępnej dla użytkownika w dowolnym momencie oraz zmieniającej swoje rozmiary w zależności od jego potrzeb. Jest to technologia, która nie wymaga od przedsiębiorstwa ponoszenia dodatkowych kosztów związanych z zakupem i zbudowaniem odpowiedniej infrastruktury IT potrzebnej do stworzenia własnego centrum danych. Możliwe do wyróżnienia są trzy rodzaje chmury obliczeniowej: prywatną, publiczną, hybrydową [14].

Chmury obliczeniowe są dostarczane w kilku modelach, aby sprostać coraz większym wymaganiom, jakie stawiane są przez użytkowników. Do najpopularniejszych modeli zalicza się [14]:

- oprogramowanie jako usługa (ang. *Software as a Service*),
- platformę jako usługę (ang. *Platform as a Service*),
- infrastrukturę jako usługę (ang. *Infrastructure as a Service*),
- wszystko jako usługę (ang. *Everything as a Service*), to jest rozwiązanie, które wykorzystuje chmurę hybrydową oraz jeden z pozostałych modeli lub ich kombinację.

Połączenie najnowszych technologii teleinformatycznych, przemysłu oraz Internetu stanowi podstawy koncepcji Przemysłu 4.0. Pojęcie to stało się bardzo popularnym hasłem, pod którym kryją się zmiany sektora przemysłowego. Przemysł 4.0 jest elementem kształtowania się dynamicznego rozwoju przemysłowego, a jego kluczowe technologie przedstawione zostały w tabeli 1.

Tabela 1. Kluczowe technologie wykorzystywane w koncepcji Przemysłu 4.0 [2,14,30]

Technologia	Inteligentny produkt	Użytkownik
<ul style="list-style-type: none"> • Protokoły internetowe IPv6 • Przemysłowe sieci przesyłu danych (<i>fieldbus systems</i>) • Przemysłowy Ethernet (<i>industrial Ethernet</i>) • Wirtualna sieć prywatna (VPN) • Chmura obliczeniowa (<i>cloud computing</i>) • Standardy bezprzewodowych sieci komputerowych (Wi-Fi) • Standardy bezprzewodowej radiowej komunikacji krótkiego zasięgu (Bluetooth, NFC) • Otwarte, neutralne, kompatybilne standardy wymiany danych (XML, AutomationML – AML) • Łączność między urządzeniami/przedmiotami (<i>M2M, Car2Car</i>) • Internet Rzeczy (Internet of Things) 	<ul style="list-style-type: none"> • Produkt dostosowany do potrzeb użytkownika i dostępny na żądanie (<i>customised and on demand</i>) • Kod dwuwymiarowy oraz metka radiowa (QR code, RFID) • Identyfikacja pojazdów wg kodów VIN (<i>autoindent</i>) • Techniki szybkiego wytwarzania m.in. addytywne wytwarzanie (<i>additive manufacturing</i>), druk 3D, selektywne spiekanie laserem (<i>sintering</i>) • Inteligentna metka (<i>smart tag</i>) • Systemy cyber-fizyczne (CPS) • Cybernetyka (<i>cybernetics</i>) • Robotyka i program sterujący (kod NC) • Utrzymanie zapobiegawcze (<i>predictive maintenance</i>) • Inteligentne obiekty (<i>smart objects</i>) 	<ul style="list-style-type: none"> • Analiza danych (data analysis), analityka biznesowa (BI) • Informatyczne systemy do planowania produkcji (ERP, PLM, APS) • Projektowanie wspomagane komputerowo (CAD, CAM, MES) • Architektura systemów informatycznych opartych o usługi (SOA, <i>Simulation</i>) • Programowanie adaptacyjne (<i>adaptive programming</i>) • Cyber-fizyczne systemy produkcji (CPPS) • Rozszerzona rzeczywistość (<i>augmented reality</i>) • Urządzenia ubieralne (<i>wearables</i>) • Współpracujące roboty (<i>collaborative robots</i>) • Sztuczna inteligencja (<i>artificial intelligence</i>) • Zwinna fabryka (<i>resilient factory</i>)

Podsumowując, można wyróżnić kilka najważniejszych idei oraz pojęć, które związane są z kompleksową koncepcją Przemysłu 4.0 [3, 10, 28, 31]:

- **Internet of Things** – są to technologie, które umożliwiają podłączenie niemal każdego urządzenia do Internetu, a także zdalny dostęp do podłączonych

urządzeń, dając możliwość zarządzania nimi z każdego miejsca z dostępem do Internetu. Zjawisko to określane jest jako Przemysłowy Internet Rzeczy (ang. *Industrial Internet of Things*). Jedną z przykładowych aplikacji technologii IIoT jest zintegrowana, bezprzewodowa sieć monitorowania. W jej skład wchodzi setki bezprzewodowych czujników, których wdrożenie jest szybsze, tańsze oraz prostsze od czujników przewodowych;

- **Smart Factory** – jest to koncepcja nowoczesnej fabryki, która opiera się o tzw. systemy cyber-fizyczne oraz Przemysłowy Internet Rzeczy. Obecnie dąży się do stanu, w którym fabryka przyszłości będzie w pełni autonomiczna – rozpoczynając od zautomatyzowania procesów planowania produkcji, a skończywszy na samej produkcji oraz utrzymaniu ruchu. Jednym z założeń inteligentnej fabryki jest możliwość jej komunikacji z innymi zakładami, której celem ma być optymalizacja produkcji oraz dostosowywanie się do dynamicznych zmian w wymaganiach stawianych przez klientów. Elementami tworzącymi Smart Factory są również chmury obliczeniowe, autonomiczny transport wewnętrzny bądź zastosowanie druku 3D;
- **systemy cyber-fizyczne** – rozumiane jako kompletne, inteligentne struktury, które obejmują w sobie maszyny podejmujące decyzje autonomiczne oraz mające możliwość komunikowania się globalnie z innymi zespołami na świecie. Idea ta może doprowadzić do powstawania nowych, skomplikowanych i dynamicznie zmieniających się struktur organizacyjnych, dzięki którym możliwe będzie osiągnięcie niemożliwych do tej pory poziomów efektywności, przy jednoczesnej minimalizacji wpływu czynnika ludzkiego. Maszyny, które mają potencjalnie być częścią nowoczesnych systemów cyber-fizycznych, muszą cechować wysoki stopień automatyzacji oraz informatyzacji, a ponad to muszą one wykorzystywać zaawansowane algorytmy z zakresu sztucznej inteligencji;
- **chmury obliczeniowe** – technologia, która pozwala na zdalne przetwarzanie danych dzięki użyciu bezpiecznych serwerów. Przede wszystkim obejmują one systemy analityczne oraz kalkulacyjne. Dzięki centralizacji przechowywania danych przedsiębiorstwa mogą oszczędzić zarówno czas jak i pieniądze – to wszystko za sprawą mniejszej ilości zasobów, jakie potrzebne są dla działania takiego systemu. Kolejną kluczową cechą takich systemów jest dostępność do danych praktycznie z każdego miejsca, posiadającego dostęp do usługi;
- **wytwarzanie responsywne** – założenie zakładające elastyczne dostosowywanie produkcji biorące pod uwagę dynamicznie zmieniające się wymagania stawiane przez klientów – ma to na celu dostarczenie takiego produktu, który spełnia jego wymagania. Ważnym elementem jest również możliwość dostosowania produkcji w zależności od sytuacji na rynku;
- **rozszerzona rzeczywistość** – są to wszelkie nowoczesne metody, których zadaniem jest prezentacja wirtualnych obiektów. Pozwala ona na bardziej intuicyjne oraz przejrzyste przedstawianie danych. Spektrum zastosowań jest ogromne – począwszy od szkolenia nowych pracowników, przez prezentację nowych parametrów maszyn, po planowanie ustawienia maszyn na hali, bądź planowanie nowych stanowisk produkcyjnych;
- **szybkie prototypowanie** – wszystkie metody pozwalające na przyspieszenie, przy jednoczesnym zmniejszeniu ryzyka i kosztów, w ramach procesów powstawania oraz rozwoju produktu. Są to na przykład metody takie jak

- wirtualne prototypowanie (z wykorzystaniem np. oprogramowania CAE, ang. *Computer Aided Engineering*) oraz technologia druku 3D;
- **BigData** – struktury obejmujące duże ilości danych, które cechuje różnorodność i złożoność. Aby z nich korzystać konieczna jest inwestycja w odpowiednią infrastrukturę pozwalającą na przetwarzanie i analizę danych w czasie rzeczywistym. Wprowadzenie BigData możliwy jest dzięki postępującemu spadkowi kosztów związanych z przechowywaniem danych. Dzięki BigData możliwy jest również rozwój technologii Internetu Rzeczy (IoT) w zupełnie nowych dziedzinach. Systemy BigData pozwalają na łączenie danych z różnych obszarów, takich jak np.: stan pracy maszyn, wielkość produkcji, awaryjność, jakość wytwarzanego produktu – w oparciu o takie dane menadżerom łatwiej jest podjąć odpowiednie decyzje;
 - **Cyber-bezpieczeństwo** – gwałtowny wzrost ilości urządzeń podłączonych do Internetu oraz rozpowszechnienie przekazywania i przetwarzania danych wykorzystując przy tym internet związany jest ze zwiększającym się ryzykiem ataku hakerskiego. Zakres ochrony przed cyber-zagrożeniami obejmuje zastosowanie nowoczesnych systemów, których zadaniem jest ochrona danych oraz zastosowanie systemów o „bezpiecznej” architekturze.

2. Zastosowanie danych w chmurze w przedsiębiorstwach produkcyjno-usługowo-handlowych

Obecnie można zaobserwować największe skupienie informatyki wokół tematów obiegu danych. Autorzy podjęli tego typu tematykę między innymi w publikacjach [4-6]. Dane są zbierane masowo, zarówno przez Internet Rzeczy, jak i Internet ludzi – dane są zbierane w każdy sposób, poprzez komunikatory, maile, e-zakupy, e-bankowość. Warto zaznaczyć, że szacowana ilość handlu internetowego typu przedsiębiorstwo-klient to zaledwie 15% wykonywanych transakcji, 85% to handel pomiędzy przedsiębiorstwami. Jest on jednak ukryty przed internautami, dane widoczne są jedynie dla partnerów biznesowych [1].

Jednym z rodzajów przedsiębiorstw korzystających z danych w chmurze są globalne firmy logistyczne. Dane w chmurze są dla nich szansą na poprawę jakości funkcjonowania przedsiębiorstwa, podwyższenia konkurencyjności oraz zwiększenia elastyczności w realizowaniu potrzeb klientów. Przykładem może być firma logistyczna CEVA Logistics, dla której dostawcą usług informatycznych z zakresu chmury obliczeniowej jest firma IBM [17].

Firma Rackspace Hosting przeprowadziła badania, celem których było poznanie najczęściej wykorzystywanych przez przedsiębiorstwa usług, w ramach chmury obliczeniowej. Na ich podstawie stworzono listę dziesięciu z nich [9, 17]:

- przechowywanie i udostępnianie danych,
- obsługa baz danych,
- obsługa systemów CRM,
- obsługa poczty elektronicznej,
- usługi dla aplikacji internetowych,
- tworzenie i przechowywanie kopii zapasowych danych,
- hosting stron internetowych,
- handel internetowy,

- badania, projektowanie oraz testowanie,
- wykorzystanie chmur jako chmury prywatne lub hybrydowe.

Wykorzystanie chmury obliczeniowej niesie ze sobą szereg korzyści. Do jednych z najważniejszych można zaliczyć [9]:

- brak konieczności rozbudowywania infrastruktury informatycznej – przedsiębiorstwo nie ponosi niepotrzebnych kosztów inwestycyjnych na tworzenie własnej infrastruktury informatycznej. Rozwiązany jest również problem związany z utrzymaniem takiej struktury, jej rozbudowywaniem, serwisowaniem oraz modernizowaniem,
- brak konieczności zatrudniania wykwalifikowanej kadry informatycznej – jest to powiązane z brakiem konieczności posiadania własnej infrastruktury informatycznej - jej brak powoduje, że zatrudnienie specjalistów, których zadaniem jest dbanie o jej poprawne działanie zostaje zrzucone na dostawcę usług,
- dostęp do danych z dowolnego miejsca – w przypadku chmury obliczeniowej dostęp do zasobów i danych jest uzyskiwany przez przeglądarkę internetową, co eliminuje problem braku mobilności w przypadku tradycyjnych rozwiązań. Wyeliminowana jest również konieczność posiadania zaawansowanych aplikacji służących do udzielania dostępu do zasobów z innego miejsca niż z komputera znajdującego się fizycznie w miejscu pracy,
- wydajność i elastyczność – charakter branży wykorzystującej chmurę obliczeniową ma tutaj istotną rolę – w zależności od niego zapotrzebowanie na przestrzeń na dysku bądź moc obliczeniową może różnić się w różnych okresach w ciągu roku. W przypadku podejścia tradycyjnego powoduje to wzrost kosztów utrzymania infrastruktury informatycznej, gdyż musi być ona dostosowana do najwyższego możliwego zapotrzebowania nawet wtedy, gdy jest ono wykorzystywane bardzo rzadko. Rozwiązania *cloud computing* pozwalają na natychmiastowe dostosowania programowe oraz sprzętowe do aktualnego zapotrzebowania przedsiębiorstwa,
- bezpieczeństwo danych – w tradycyjnym modelu, w którym przedsiębiorstwo posiada własną infrastrukturę IT, musi ono samo zadbać o bezpieczeństwo danych. W przypadku wykorzystania chmury zabezpieczenie danych (w tym tworzenie kopii zapasowych) jest zadaniem dostawcy usług.

3. Bezpieczeństwo danych w procesach produkcyjnych

Obecnie zachodzący rozwój w globalnej gospodarce w dużej mierze opiera się na wykorzystaniu cyfrowych technologii, których zadaniem jest wspieranie działalności gospodarczej [13]. Coraz częściej cyfryzacji podlegają już nie tylko procesy związane z komunikacją, ale również procesy produkcyjne, procesy związane z zarządzaniem przedsiębiorstwem oraz procesy usługowe. Efektem tego jest opieranie się działalności przedsiębiorstw na systemach informatycznych, których zadaniem jest przesyłanie, gromadzenie i przetwarzanie coraz większej ilości danych [5]. Dla przedsiębiorstw produkcyjnych cyfryzacja przynosi wiele korzyści, które wynikają głównie z usprawnienia procesów gospodarczych, zwiększenia efektywności w komunikowaniu się oraz zmniejszenia błędów w procesach polegających na analizie danych [7]. Obecnie panuje powszechna zgoda dotycząca

pochylenia się nad problemem cyberbezpieczeństwa w kontekście zapewnienia bezpieczeństwa dla funkcjonowania przedsiębiorstwa. Problem ten zyskuje na znaczeniu w połączeniu z koncepcją Przemysłu 4.0, w którym zdalna łączność oraz wykorzystanie dostępnej na rynku komercyjnym infrastruktury odsłania system przedsiębiorstwa na szeroki wachlarz zagrożeń. Zagrożenia cyberbezpieczeństwa są z reguły bardziej dynamiczne niż klasyczne zagrożenia związane z bezpieczeństwem. W związku z tym badanie możliwości rekonfiguracyjnych systemu opartego na koncepcji Przemysłu 4.0 może być sporym wyzwaniem dla przyszłych inżynierów, zwłaszcza w przypadku naruszenia bezpieczeństwa systemu i danych (tabela 2) oraz badania w jaki sposób wpływają one na funkcjonowanie całego przedsiębiorstwa.

Tabela 2. Działania mające na celu ochronę danych przed zagrożeniami [12]

Obszar ochrony	Działanie
Zarządzanie personelem	<ul style="list-style-type: none"> - Regularne szkolenie personelu (z zakresu poufności systemów bezpieczeństwa, używanych haseł, ochrony kart identyfikacyjnych, sposobów zachowania w przypadku ataku). - Ograniczenie dostępu do danych. - Podnoszenie generalnej wiedzy nt. zagrożeń. - Zabronienie używania nieodpowiednich nośników danych.
Działania proceduralne/organizacyjne	<ul style="list-style-type: none"> - Izolacja sieci wewnętrznych od sieci zewnętrznych (o ile jest to możliwe biorąc pod uwagę rodzaj działalności) - Odpowiednia ochrona pomieszczeń, w których znajdują się komputery (serwery) - Używanie mocnych haseł dla każdego urządzenia. - Przygotowanie procedur w przypadku ataku hakerskiego. - Ciągłe doskonalenie organizacji w zakresie bezpieczeństwa danych. - Systematyczne tworzenie kopii bezpieczeństwa.
Działania techniczne	<ul style="list-style-type: none"> - Używanie zapór ogniowych (firewall) na różnych poziomach (sieć, aplikacje, wymiana danych) - Używanie różnorodnych filtrów wprowadzając dane. - Używanie rozwiązań z zakresu kryptografii. - Używanie podpisu elektronicznego. - Przechowywanie danych w chmurze. - Wykorzystywanie technologii kognitywnych.
Użycie programów typu antywirus	<ul style="list-style-type: none"> - Wykorzystanie zaktualizowanych programów antywirusowych oraz programów niszczących wirusy oraz naprawiających uszkodzone pliki. - Zgłaszanie działań realizowanych w ramach systemu (określanie potencjalnych naruszeń).

Postęp technologiczny oraz coraz częstsze wykorzystanie technologii informatycznych w przemyśle powoduje wzrost liczby cyberataków. Próbując nadążyć za postępem, przedsiębiorstwa tworzą systemy zabezpieczeń oraz procedury postępowania i reagowania na tego typu ataki. Jednak nie jest to łatwy proces ze względu na szereg barier tj. między innymi brak wiedzy z zakresu cyberbezpieczeństwa oraz ochrony przed nim, brak technicznych możliwości do stworzenia odpowiedniej klasy zabezpieczeń bądź brak aktualizowanych i skutecznych procedur bezpieczeństwa – takich, które uwzględniałyby zmienny różnorodny charakter danych, jakie

przedsiębiorstwo chce zabezpieczyć. Przedsiębiorstwa przetwarzają oraz przechowują różne typy danych. Różne typy danych mają zróżnicowaną wrażliwość, którą można ogólnie wytłumaczyć jako poziom potencjalnych strat, jakie poniesie przedsiębiorstwo w przypadku ich udostępnienia lub wykradzenia. W zależności od tego czynnika dobierane są odpowiednie poziomy i systemy zabezpieczeń. Jest to podstawowy etap w procesie konstruowania systemu zabezpieczeń danych. Najczęściej przechowywane typy danych to [2]:

- dane osobowe pracowników (w tym wynagrodzenia oraz szczegóły stosowanych systemów motywacyjnych),
- informacje handlowe (ceny towarów i usług, harmonogramy i plany sprzedaży, stawki za oferowane usługi itp.),
- informacje o klientach oraz dane transakcyjne,
- dane związane z zapasami przedsiębiorstwa,
- harmonogram produkcji,
- dane związane z siecią dystrybucji oraz jej funkcjonowaniem,
- dane związane z transportem,
- dane finansowe przedsiębiorstwa (koszty działalności, przychody, mierniki rentowności),
- baza wiedzy przedsiębiorstwa (know-how, patenty, technologie, sposoby organizowania pracy, strategie konkurencyjne),
- szereg informacji rynkowych i marketingowych (strategie rozwoju firmy, plany przyszłych inwestycji, plany kampanii marketingowych).

Obecnie zauważalny jest coraz większy stopień stosowania systemów wykorzystujących sieci komputerowe w działaniu organizacji. Działanie to może spowodować utratę kontroli nad przetwarzaniem informacji, które kiedyś były przechowywane i przetwarzane w tradycyjnych centrach danych. W takiej sytuacji coraz istotniejsze staje się zrozumienie przez przedsiębiorstwa natury zagrożeń oraz ryzyka związanego z bezpieczeństwem danych. Warty podkreślenia jest fakt, że problemy w odniesieniu do bezpieczeństwa systemów komputerowych są często unikalne, dlatego ich zrozumienie jest istotne w kontekście wdrożenia efektywnych środków bezpieczeństwa. Rosnące znaczenie tego problemu przyczynia się do powstawania różnego rodzaju opracowań i wytycznych, których celem jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa dla systemów danych.

4. Źródła informacji oraz potencjalne zagrożenia cyberatakami

Jednym z elementów postępującej cyfryzacji jest coraz częstsze wykorzystanie Internetu w procesach zachodzących w przedsiębiorstwach produkcyjnych.

Internet Rzeczy może znaleźć szerokie zastosowanie w tzw. Inteligentnej produkcji (ang. *smart manufacturing*). Koncepcja ta zawiera w sobie wiele rozwiązań z zakresu produkcji i logistyki, których zadaniem jest optymalizacja produkcji, procesów kontroli oraz poprawa jakości. Wszechobecna komunikacja, postępujący rozwój mikrorobotyki, coraz częstsze dostosowywanie produktów do potrzeb indywidualnych, możliwe jest dzięki odpowiedniemu oprogramowaniu, co znacząco zmienia świat produkcji. Smart Manufacturing obejmuje w sobie [11, 15]:

- uczenie maszynowe (ang. *machine learning*) – inteligentne, automatyczne podejmowanie decyzji,

- *Networking* – zarządzanie i kontrola urządzeń produkcyjnych poprzez sieć,
- optymalizowanie procesów – szybkie prototypowanie produktów oraz ich wytwarzanie, ulepszanie procesów i optymalizowanie łańcucha dostaw.

Przestępstwa związane z danymi komputerowymi są ściśle połączone z rozwojem nowych technologii informatycznych, mimo że często definicja takiego przestępstwa różni się w zależności od źródła. Można przyjąć, że przestępstwa tego typu obejmują wszelkie zachowania niezgodne z prawem z zakresu funkcjonowania danych elektronicznych, nieautoryzowanego przetwarzania danych, będącego naruszeniem praw do oprogramowania komputerowego, jak również bezpośrednio połączonego z nimi nośnika używanego do przetwarzania danych i obiegu danych komputerowych, całych systemów obiegu danych oraz samego komputera [15,18-22,24].

Międzynarodowa Organizacja Policji Kryminalnej (Interpol) komputerowe przestępstwa definiuje jako te skierowane bezpośrednio przeciwko systemom komputerowym, jak również te przestępstwa, w których komputer został użyty jako narzędzie. Zaliczają się do niej [11, 16, 22, 23, 26]:

- nielegalne naruszenie praw dostępu do zasobów informacyjnych, w szczególności hakowanie, przechwytywanie danych, kradzież czasu,
- nieautoryzowana zmiana danych przy użyciu „bomb logicznych”, błędów komputerowych oraz wirusów (takich jak np. wirusy typu „Trojan”),
- oszustwa z użyciem komputera jako narzędzia; w szczególności wyróżnia się oszustwa związane z płatnościami, fałszowanie urządzeń wejściowych lub wyjściowych (przy użyciu np. kart magnetycznych), podawanie nieprawdziwych błędów identyfikacyjnych, oszustwa związane z systemami związanymi ze sprzedażą, oszustwa przy użyciu systemów telekomunikacyjnych,
- kradzież programów komputerowych (nielegalne użycie programów) w szczególności gier komputerowych, oprogramowania komputerowego,
- sabotaż sprzętu lub oprogramowania komputerowego,
- przestępstwa przy użyciu systemów *Bulletin Board* (są to systemy, które służą wymianie wiadomości oraz plików przy wykorzystaniu sieci),
- posiadanie materiałów niezgodnych z prawem,
- szeroko pojęta przestępczość internetowa (oszustwa, wyłudzenia itp.).

Oprócz zagrożeń związanych z łamaniem prawa, coraz większe wykorzystanie systemów, danych komputerowych jak i Internetu Rzeczy niosą za sobą również inne zagrożenia. Można wyróżnić dwie grupy, w których zawierają się takie zagrożenia:

- z zakresu szeroko pojmowanego charakteru społecznego,
- z zakresu technologicznego (technicznego).

Zagrożenia o charakterze społecznym mają i będą mieć dynamiczny, różnorodny charakter podlegający ciągłym zmianom. Można jednak wyróżnić kilka zagrożeń, które mogą być następstwem postępu technologicznego [12]:

- bezrobocie. Zaawansowane technologicznie programy rozpoznawania mowy i systemy rozpoznawania pytań do budowania odpowiedzi, mogą spowodować wyraźny spadek zatrudnienia w obszarach szeroko rozumianego obszaru informacji (przykładem są firmy Call Center). W podobny sposób bezrobocie będą generowały takie branże jak na przykład: monitoring, kontrola jakości, automatyka, konserwacja oprogramowania, aktualizacja oprogramowania i systemów komputerowych, logistyka oraz planowanie (np. planowanie produkcji);

- zagrożenia związane z bezpieczeństwem. Obecnie istniejące systemy zbierania i przetwarzania danych opierają się na algorytmach, jednak nie samo zbieranie i przetwarzanie danych jest w tym przypadku problemem. Zagrożenie zaczyna się w momencie, w którym następuje podejmowanie decyzji na bazie zebranych i przetworzonych danych. Problemem jest ograniczona możliwość skończonych przypadków systemów podejmujących takie decyzje, które przez techników zostały wprowadzone do systemu jako możliwe scenariusze. Systemy takie mogą okazać się niebezpieczne w przypadkach, które nie zostały ujęte w jakimś scenariuszu – nie sposób przewidzieć również jak takie systemy zachowają się w przypadku zdarzeń losowych;
- zagrożenia związane z wolnością i prywatnością. Aktualne wykorzystanie Sieci oraz Internetu Rzeczy w działaniu przedsiębiorstw oraz w życiu codziennym daje obszerną wiedzę o przepływach finansowych, przyzwyczajeniach, preferencjach oraz potencjalnych planach na przyszłość. Dane takie mogą być wykorzystane w różny sposób przez osoby trzecie.

5. Podsumowanie

Firmy decydujące się na wykorzystanie najnowszych technologii informatycznych coraz częściej zyskują istotną przewagę nad tymi, które decydują się na pozostanie przy metodach konwencjonalnych. Obecnie cyfryzacja obejmuje tak duży obszar, że możliwości rozwoju i powstawania coraz to nowszych technologii jest nieograniczona. Przedsiębiorstwa decydujące się na cyfryzację swoich systemów powinny zadbać zarówno o odpowiednie systemy informatyczne, dopasowane do rodzaju działalności oraz wielkości firmy, jak i o odpowiednie szkolenia pracowników. Nie powinno się zapominać, że człowiek często jest największym zagrożeniem systemów informatycznych, stąd tak istotne jest zadbanie o przekazanie pracownikom przedsiębiorstwa odpowiedniej wiedzy z zakresu działania rozwiązań IT. Wykorzystywanie najnowszych technologii wiąże się również z ryzykiem, decydując się na rozwiązania z zakresu cyfryzacji należy zadbać o bezpieczeństwo zarówno ludzi, jak i danych, którymi operuje przedsiębiorstwo.

LITERATURA

1. CELLARY W.: Przemysł 4.0 i Gospodarka 4.0, XXXII Olimpiada Wiedzy Ekonomicznej Gospodarka światowa. Wolny handel czy protekcjonizm, Biuletyn PTE Nr 3, Sierpień 2019, s. 48-49.
2. CHOROŚ P.: Wykorzystanie analityki biznesowej w Internecie rzeczy, w: P. Kolenda (red.), Internet Rzeczy w Polsce, Raport, iaB Polska, s. 4, - 12.
3. IWAŃSKI T.: Przemysł 4.0 i wszystko jasne., Napędy i sterowanie, Nr 1, Styczeń 2017, s. 22-23.
4. KACZMAR-KOLNY E., KOLNY D., MLECZKO J.: Rozwiązania Business Intelligence jako wsparcie w controllingu finansowym, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, Bielsko-Biała, 2020, s. 147-156.

5. KOLNY D.: Nowoczesne systemy informowania kierownictwa w małych i średnich przedsiębiorstwach, Wydawnictwo Uczelniane Politechniki Koszalińskiej, Koszalin, 2021, s. 36-49.
6. KOLNY D., CIEŚLA B., MLECZKO J.: Dynamiczna wizualizacja danych produkcyjnych jako wsparcie procesu zarządzania w MŚP, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, Bielsko-Biała, 2019, s. 105-114.
7. KSIAŻKIEWICZ D.: Bezpieczeństwo danych w procesach biznesowych, CYFRYZACJA GOSPODARKI I SPOŁECZEŃSTWA, Gdańska Akademia Bankowa, Gdańsk 2016, s. 60.
8. KWIATKOWSKA M. E.: Rozwój Internetu rzeczy – szanse i zagrożenia, Internetowy Kwartalnik Antymonopolowy i Regulacyjny, 2014, nr 8(3), s. 60-70.
9. LEMAŃSKA E., OLSZEWSKA K., RYBAK K.: Cloud computing jako narzędzie optymalizacji wykorzystania zasobów przedsiębiorstwa., Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie nr 25 t.2 (2017), s. 94-104.
10. MAJ I. Internet Rzeczy i zagrożenia z nim związane, Bezpieczeństwo. Teoria i Praktyka”2015, Oficyna Wydawnicza AFM, s. 55-56.
11. MALUCHA M.: Internet Rzeczy – kontekst technologiczny i obszary zastosowań, Studia i Prace WNEIS US, nr. 54/2, 2018 r., s. 51-69.
12. MROCZKO F., KUHL F.: Selected safety problems of the information systems, Prace naukowe WSZIP T. 43 (4) 2017, s. 49-51.
13. OMAR J., SLJIVO I., HABLI I., HAWKINS R.: Challenges of safety assurance for industry 4.0., 13th European Dependable Computing Conference (EDCC). IEEE, 2017.
14. PIERIEGUD J.: Cyfryzacja gospodarki i społeczeństwa – wymiar globalny, europejski i krajowy, Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, Gdańsk 2016, s. 11-13.
15. Por. GRZELAK M., LIEDEL K.: Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, „Bezpieczeństwo Narodowe” nr 22, II–2012, s. 131.
16. SAWICKI M.: Podział i definicja cyberprzestępstw, Prokuratura i prawo 7–8, 2012, s. 241-252.
17. TRZOP A.: Przegląd rozwiązań z zakresu przemysłu 4.0 stosowanych w obszarze logistyki, Zeszyty Naukowe Politechniki Poznańskiej, Organizacja i Zarządzanie nr 81, 2020, s. 242
18. Ustawa Kodeks karny z 6 czerwca 1997 r. (Dz.U. z 1997 nr. Nr 88, poz. 553 ze zmian.)
19. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 2002 nr 101 poz. 926).
20. Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. jedn.: Dz.U. 2006 nr 90 poz. 631).
21. Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń.
22. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, Bruksela, z dnia 22 maja 2007 r.,
23. Komunikat Komisji do Parlamentu europejskiego, Rady oraz Komitetu Regionów - W kierunku ogólnej strategii zwalczania cyberprzestępczości {SEK(2007) 641} {SEK(2007)642}, <https://eur-lex.europa.eu 10.10.2022 r.>

24. Konwencja o Prawach Dziecka przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. ratyfikowana przez Prezydenta Polski na mocy ustawy z dnia 21 września 1990 r. o ratyfikacji Konwencji o prawach dziecka, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r.
25. The digital transformation of industry, Roland Berger Strategy Consultants, BDI, 2015, https://bdi.eu/media/presse/publikationen/information-und-telekommunikation/Digital_Transformation.pdf, 10.10.2022
26. Internet Security Threat Report, Vol. 21, Symantec, April 2016, s. 8-9, <https://www.symantec.com/content/> 10.10.2022
27. Serwis internetowy firmy Boss Computers, <https://boss.net.pl/co-to-jest-internet-rzeczyinternet-of-things/>, 31.05.2022
28. Serwis internetowy Dataspace, <https://dataspace.pl/blog/chmura-obliczeniowa-cloud-computing-rozlozona-na-czesci-pierwsze/> 25.07.2022
29. Serwis internetowy firmy HighSolutions, <https://highsolutions.pl/blog/wpis/czym-jest-transformacja-cyfrowa-analiza-przeprowadzenia-transformacji-krok-po-kroku>, 01.06.2022
30. <https://www.gov.pl/web/cyfryzacja/internet-rzeczy>, 10.10.2022
31. <https://www.iab.org.pl/wp-content/uploads/2016/05/Raport-Internet-Rzeczy-w-Polsce.pdf>, 10.10.2022