Dr inż. Izabela Horzela
Akademia Sztuki Wojennej
ORCID: 0000-0003-1778-9004
e-mail: i.horzela@akademia.mil.pl

Bezpieczeństwo informacji w procesach logistycznych

Information security in logistics processes

Streszczenie

Bezpieczeństwo informacji w logistyce stało się nieodzownym czynnikiem gwarantującym zarówno skuteczność, jak i odporność przedsiębiorstw w erze Logistyki 4.0. Celem artykułu jest ocena znaczenia bezpieczeństwa informacji w procesach logistycznych poprzez identyfikację i analizę kluczowych zagrożeń oraz ocenę roli standardów, regulacji prawnych i nowoczesnych technologii w kształtowaniu kierunków rozwoju ochrony informacji i budowie odporności systemów logistycznych. W artykule zaprezentowano kompleksowy przegląd zagrożeń informacyjnych, które dotykają sektor TSL – od zaawansowanych ataków cybernetycznych, przez awarie infrastrukturalne, po pomyłki i błędy ludzkie – a także problemy wynikające ze współpracy z partnerami zewnętrznymi. Autorka przeanalizowała rolę modeli zarządzania bezpieczeństwem oraz znaczenie nowoczesnych technologii w ochronie danych i redukcji ryzyka incydentów. Przedstawiono zalecenia dotyczące integracji systemów bezpieczeństwa, wdrażania innowacyjnych rozwiązań technologicznych oraz poprawy kompetencji cyfrowych pracowników zgodnie z analizą literatury i przykładami praktycznymi. Artykuł, będący zarówno przeglądem dorobku naukowego, jak i praktycznym przewodnikiem, dostarcza niezbędnej wiedzy potrzebnej do budowy systemów logistycznych charakteryzujących się bezpieczeństwem i odpornością.

Słowa kluczowe

bezpieczeństwo informacji, Logistyka 4.0, zarządzanie ryzykiem, ciągłość działania, technologie cyfrowe

Abstract

In an age of Logistics 4.0, information security in logistics is essential for both efficiency and resilience of enterprises. The aim of this article is to evaluate the importance of information security in logistics processes by identifying and analysing key threats, as well as assessing the role of standards, legal regulations, and modern technologies in shaping the directions of information security development and building the resilience of logistics systems. This article summarizes the major information-security threats faced by the TSL industry, from sophisticated cyberattacks and infrastructure failures to human mistakes and errors, and the challenges of cooperating with external partners. Recommendations for integrating security systems, implementing innovative technological solutions, and improving employee digital competencies are made in light of literature review and practical examples. The above article serves as both a briefing as well as an instructive manual to know more on how to construct secure and well-resilient logistics systems.

Keywords

information security, Logistics 4.0, risk management, business continuity, digital technologies

JEL: F50, H56, D83, L86

Wprowadzenie

Środowisko informacyjne współczesnego biznesu jest złożone i dynamiczne. Zglobalizowane łańcuchy produkcyjne, szybki rozwój technologii wiedzy, rozwijająca się automatyzacja procesów i rosnące uzależnienie od cyfryzacji danych sprawiły, że informacja stała się kluczowym zasobem dla organizacji (Nowak, 2025).

Bezpieczeństwo informacji, definiowane jako ochrona przed nieautoryzowanym dostępem, utratą, modyfikacją lub zniszczeniem danych, jest kluczowym warunkiem pomyślnego i odpornego funkcjonowania współczesnych systemów logistycznych (Whitman & Mattord, 2021). Rola i znaczenie informacji w logistyce od dawna wykracza poza tradycyjne rozumienie przepływu danych związanych z dostawami czy zamówieniami. Organizacje wykorzystują Internet Rzeczy (IoT), sztuczną inteligencję (AI), technologię blockchain i zaawansowane rozwiązania analityki danych jako codzienną praktykę do planowania i monitorowania procesów w erze

Logistyki 4.0 (Bielecki i in., 2024). W rezultacie każdy element infrastruktury IT może stać się punktem ataku lub awarii (Leligou i in., 2024). Rosnąca liczba incydentów w sektorze TSL jest dowodem na to, że organizacje nie są w pełni przygotowane do odpowiedniego zabezpieczenia swoich zasobów informacyjnych (VECTO, 2023).

W ostatnich latach pojawiło się wiele regulacji prawnych dotyczących bezpieczeństwa informacji. Ważnym aktem prawnym jest dyrektywa NIS2 (2022/2555), ponieważ stosując się do niej, firmy z branży logistycznej muszą wdrażać zarządzanie ryzykiem i raportować w dziedzinie danych, aby informować zarząd o incydentach związanych z bezpieczeństwem (Cyberbezpieczni OPTeam, 2025). Odświeżono również zbiór norm ISO/IEC 27000. Norma PN-EN ISO/IEC 27001:2023-08 ma na celu rozwój zintegrowanego spojrzenia na bezpieczeństwo informacji, co ma pomóc organizacjom świadomie chronić swoje zasoby informacyjne z myślą o budowaniu bezpiecznych procedur pracy, uwzględniając jednocześnie zmieniające się ryzyko wewnętrzne oraz zewnętrzne. Powyższe wymagania stanowią w Polsce wyzwanie biznesowe i organizacyjne, dlatego wiele firm TSL nie sformułowało jeszcze strategii zarządzania informacją ani nie zadbało o procedury zarządzania ciągłością działania (Logistyka.net.pl, 2024).

Bezpieczeństwo informacji w logistyce jest niezwykle ważne. Po pierwsze, jest częścią zarządzania operacyjnego i gwarantuje ciągłość i niezawodność przepływu informacji między organizacją a partnerami w łańcuchu dostaw (Enache, 2023). Ma wpływ na wiarygodność i konkurencyjność organizacji na rynku światowym. Naruszenia bezpieczeństwa informacji mogą prowadzić do strat finansowych, a także utraty zaufania klientów i partnerów biznesowych (Gurtu & Johny, 2021).

Z raportu VECTO (2023) wynika, że 68% firm transportowych doświadczyło nieautoryzowanego dostępu do systemów lub danych w ciągu ostatnich dwóch lat, podczas gdy tylko jedna trzecia z nich zaktualizowała swoje plany reagowania na incydenty. Janczewska i Janczewski (2021) zauważyli, że zarządzanie ryzykiem informacyjnym w logistyce jest bardziej reaktywne niż proaktywne, a wszystkie działania są inicjowane po ataku. Firmy nie starają się systemowo zapobiegać zagrożeniom.

Artykuł ma charakter analityczny i przeglądowy, skupia się na identyfikacji krytycznych zagrożeń oraz opracowaniu rekomendacji i rozwiązań dla branży TSL. W artykule skoncentrowano się przede wszystkim na:

- przedstawieniu standardów bezpieczeństwa informacji w logistyce;
- analizie incydentów i zagrożeń występujących w procesach logistycznych;
- ocenie stosowanych środków bezpieczeństwa informacji;
- zaproponowaniu kierunków rozwoju w obszarze bezpieczeństwa informacji w procesach logistycznych.

Niniejszy artykuł przyjmuje podejście interdyscyplinarne, łącząc aspekty zarządzania, IT i bezpieczeństwa, aby umożliwić osiągnięcie całościowego spojrzenia na problem ochrony informacji we współczesnych procesach logistycznych.

Bezpieczeństwo informacji: ujęcie teoretyczne i znaczenie dla logistyki

Istota i koncepcje bezpieczeństwa informacji

Bezpieczeństwo informacji jest kluczowym elementem funkcjonowania organizacji (zwłaszcza w sektorze logistycznym). Są to działania podejmowane w celu ochrony danych przed nieautoryzowanym dostępem, zmianą, utratą lub zniszczeniem, które zapewniają, że integralność, poufność i dostępność danych są utrzymane (Whitman & Mattord, 2021). W rzeczywistości bezpieczeństwo informacji nie odnosi się tylko do systemów IT, ale także do procedur organizacyjnych, szkoleń personelu czy bezpieczeństwa sprzętu (Kobis, 2021).

W przypadku logistyki bezpieczeństwo informacji jest jeszcze ważniejsze, ponieważ łańcuch dostaw wykorzystuje dane, które mają charakter strategiczny, komercyjny i operacyjny. Mogą one dotyczyć poziomów zapasów, lokalizacji miejsc wysyłki, dat transportu, informacji o klientach czy umów z dostawcami. Utrata lub naruszenie integralności informacji może znacznie zaburzyć codzienne funkcjonowanie organizacji, powodując szkody finansowe lub problemy z wiarygodnością (Latsiou & Lambrinoudakis, 2026).

Podstawowym modelem stosowanym w zarządzaniu bezpieczeństwem informacji jest model CIA (poufność, integralność, dostępność), który definiuje trzy filary ochrony danych (Żywucka-Kozłowska & Dziembowski, 2023):

1) Poufność – zapewnienie, żeby tylko osoby upoważnione miały dostęp do danych.

2) Integralność – zapewnienie, żeby informacje były poprawne i kompletne, odporne na nieautoryzowane zmiany.

3) Dostępność – zapewnienie upoważnionym użytkownikom ciągłego dostępu do danych, nawet w przypadku awarii systemów i/lub ataków cybernetycznych.

W literaturze proponuje się uzupełnienie modelu CIA o dodatkowe filary ochrony danych: autentyczność procesu, odpowiedzialność i audytowalność (Szymonik i in., 2024).

Problemy w obszarze zarządzania bezpieczeństwem informacji w branży logistycznej są analizowane pod kątem procesowym, strategicznym i technologicznym. Podejście procesowe opiera się na cyklu PDCA (planuj – wykonaj – sprawdź – działaj). Kładzie się w nim nacisk na to, aby ocena ryzyka mogła być przeprowadzana w odpowiednim czasie, a procedury bezpieczeństwa podlegały ciągłemu doskonaleniu. Wykorzystanie tego cyklu jest typowe dla standardu ISO. W perspektywie strategicznej bezpieczeństwo informacji jest postrzegane jako źródło przewagi konkurencyjnej i współpracy

w łańcuchu dostaw (Christopher, 2000). Z kolei perspektywa technologiczna opisuje wdrażanie technologii IT w organizacjach, takich jak: szyfrowanie danych, zapory ogniowe, systemy wykrywania i zapobiegania włamaniom (IDS/IPS), IoT czy blockchain (Łapka, 2025; Szymonik i in., 2024).

Jeśli organizacje chcą skutecznie kontrolować bezpieczeństwo informacji, powinny mieć zintegrowane strategie procesowe, strategiczne i technologiczne, oraz uwzględnić perspektywę prawną i organizacyjną dotyczącą funkcjonowania organizacji (Hlynskyy, Dovhun & Pochopień, 2025; Nyszk, 2019).

Normy i regulacje w zakresie bezpieczeństwa informacji

Zarządzanie bezpieczeństwem informacji w organizacji wymaga oparcia się na normach, które określają parametry zarządzania procesami i zapewniają ich zgodność z zapisami dokumentów. Normy używane są do ujednolicenia procesu identyfikacji ryzyka, wdrażania zabezpieczeń i monitorowania skuteczności funkcjonowania firm logistycznych.

Systemowe podejście do zarządzania bezpieczeństwem informacji w organizacjach logistycznych opisane jest w normach ISO/IEC 27001:2022 (PN-EN ISO/IEC 27001:2023-08 – polskie wydanie) oraz ISO 28000:2022:

- ISO/IEC 27001:2022 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji – Wymagania" – określa wymagania dla systemu zarządzania bezpieczeństwem informacji (SZBI), który identyfikuje zagrożenia, analizuje ryzyka oraz sprawdza skuteczność zabezpieczeń.
- ISO 28000:2022 „System zarządzania bezpieczeństwem łańcucha dostaw – Wymagania" – ma na celu ochronę bezpieczeństwa i odporności łańcucha dostaw przed ryzykiem operacyjnym i informacyjnym (ISO, 2022).

Jednoczesne wdrożenie obu norm prowadzi do powstania zintegrowanego systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie logistycznym (Enache, 2023; Staniewska, 2021).

Akty prawne istotne przy tworzeniu SZBI to dyrektywa NIS2 (2022/2555) oraz rozporządzenie (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (tzw. RODO).

Dyrektywa NIS2 (2022/2555) nakłada na organizacje obowiązek opracowania i wdrożenia mechanizmów zmniejszania ryzyka cybernetycznego oraz zgłaszania takich incydentów w odpowiedni sposób. W celu ochrony danych osobowych stosuje się wymagania rozporządzenia RODO (2016), które wzywa do harmonizacji przepisów dotyczących tej ochrony w całej UE (Cyberbezpieczni OPTeam, 2025; Logistyka.net.pl, 2024). Przepisy te są wdrażane przez przedsiębiorstwa (także z branży TSL) i wymagają od nich przygotowania polityki bezpieczeństwa, przeprowadzania audytów i szkoleń (Janczewska & Janczewski, 2021; VECTO, 2023).

Zapewnienie zgodności z normami dotyczącymi bezpieczeństwa informacji, w szczególności ISO 27001 i ISO 28000, jest punktem wyjścia do zarządzania informacjami i ich właściwej ochrony. Ponadto wdrożenie norm ma wpływ na zwiększenie odporności organizacji na zagrożenia informacyjne oraz pomaga zadbać o ciągłość, stabilność i efektywność procesów w łańcuchach dostaw.

Znaczenie bezpieczeństwa informacji w logistyce

Informacja jest kluczowym zasobem w każdym systemie logistycznym. Umożliwia planowanie, koordynację i monitorowanie przepływu towarów i usług w łańcuchu dostaw. Informacje wykorzystywane przez firmy logistyczne obejmują dane operacyjne (zamówienia, stan zapasów, harmonogramy dostaw, lokalizacje wysyłki) oraz dane strategiczne (np. dane kontrahentów, warunki umów, prognozy popytu i podaży) (Adamek, 2024).

Bezpieczeństwo informacji zapewnia płynne działanie procesów i zmniejsza ryzyko zakłóceń w funkcjonowaniu przedsiębiorstwa. Dotyczy to przykładowo systemu zarządzania transportem (TMS), który łączy wiele źródeł danych, takich jak systemy GPS, systemy magazynowe (WMS), aplikacje klienckie itp. Utrata danych lub ich nieautoryzowana modyfikacja może zatem powodować zakłócenia w dostawach, wzrost kosztów operacyjnych lub naruszenia zobowiązań kontraktowych (Gurtu & Johny, 2021).

W większości nowoczesnych systemów wiele punktów jest podatnych na naruszenia bezpieczeństwa informacji. Najważniejsze z nich to:

1) Bazy danych i systemy IT – będące głównym repozytorium informacji osobowych, finansowych i operacyjnych. Naruszenie ich integralności może prowadzić do braku kontroli nad łańcuchem dostaw (Szymonik i in., 2024).

2) Infrastruktura komunikacyjna – sieci internetowe, VPN, IoT i systemy telemetryczne, które przesyłają dane w czasie rzeczywistym. Luki lub nieprawidłowości w ich zabezpieczeniach mogą prowadzić do przechwycenia informacji lub ataków typu MITM (*man-in-the-middle*) (Boiko, Shendryk & Boiko, 2018).

3) Wspólne interfejsy z partnerami zewnętrznymi – udostępnianie danych dostawcom, przewoźnikom, konsumentom i operatorom magazynów bez odpowiednich mechanizmów uwierzytelniania i szyfrowania naraża informacje na ryzyko wycieku (Hlynskyy, Dovhun & Pochopień, 2025).

4) Pracownicy i urządzenia końcowe – komputery, laptopy, telefony, urządzenia IoT oraz kompetencje pracowników bezpośrednio przekładają się na bezpieczeństwo informacji. Utrata danych wynika z niewiedzy,

słabości ludzkich, braku szkoleń lub nieprzestrzegania procedur (VECTO, 2023).

Przedsiębiorstwa logistyczne doświadczają różnorodnych skutków naruszenia bezpieczeństwa informacji. Najczęstsze konsekwencje obejmują:

- Szkody finansowe – koszty wynikające z awarii systemów IT, płatności na rzecz klientów, kary administracyjne za nieprzestrzeganie przepisów (VECTO, 2023; Janczewska & Janczewski, 2021).
- Zakłócenia w łańcuchu dostaw – opóźnienia w dystrybucji zamówień, błędy dystrybucji, problemy z zapasami.
- Utratę zaufania klientów i/lub partnerów – ważne dla firm e-commerce, operatorów logistycznych obsługujących wielu klientów (Hlynskyy, Dovhun & Pochopień, 2025).
- Nieprzestrzeganie prawa – niespełnianie wymogów dyrektywy NIS2, RODO lub norm ISO może prowadzić do sankcji administracyjnych i kar finansowych (Cyberbezpieczni OPTeam, 2025; Logistyka.net.pl, 2024).

W Polsce procedury dotyczące bezpieczeństwa informacji nie są wystarczająco wdrożone, zwłaszcza przez małe i średnie przedsiębiorstwa z sektora TSL. Zaledwie 32% przedsiębiorstw posiada plany reagowania na incydenty, a aż 68% firm doświadczyło problemów z bezpieczeństwem danych w ciągu ostatnich dwóch lat (VECTO, 2023).

Aby zagwarantować bezpieczeństwo informacji i efektywnie nimi zarządzać, należy stosować model interdyscyplinarny, łączący osoby z umiejętnościami menedżerskimi, IT i logistycznymi. W praktyce może to obejmować:

- opracowanie polityk bezpieczeństwa informacji i protokołów reagowania na incydenty (Enache, 2023);
- wykorzystanie sprzętu zabezpieczającego, w tym: szyfrowania danych, Internetu Rzeczy, zapór sieciowych, monitorowania sieci, wykrywania włamań, IoT z certyfikowaną komunikacją (Bielecki i in., 2024; Leligou i in., 2024);
- podnoszenie kwalifikacji i wiedzy personelu w zakresie bezpieczeństwa informacji (Kobis, 2021).
- współpracę w łańcuchu dostaw – udostępnianie informacji na podstawie specyfikacji ISO 27001 i ISO 28000 (Boyens et al., 2022).

Tego rodzaju multidyscyplinarne podejście pozwala minimalizować ryzyko, a także zapewnić większą efektywność operacyjną i zmniejszać liczbę przestojów i błędów w procesach logistycznych.

Zagrożenia informacyjne w procesach logistycznych

Przepływ informacji jest niezbędny do realizacji procesów logistycznych, ale liczba i złożoność tych procesów sprawiają, że są one podatne na naruszenia bezpieczeństwa danych. Powszechność cyfryzacji i rosnąca automatyzacja procesów logistycznych oznaczają również obecność wielu złożonych zagrożeń informacyjnych.

Bezpieczeństwo informacji charakteryzuje się wielowymiarowością, obejmującą aspekty technologiczne, organizacyjne i ludzkie, co prowadzi do większego ryzyka naruszeń bezpieczeństwa. Żywucka-Kozłowska i Dziembowski (2023) wyjaśniają, że skuteczny system zarządzania bezpieczeństwem informacji integruje trzy obszary: technologię, ludzi oraz zarządzanie i organizację. To podejście pozwala na podział zagrożeń informacyjnych w logistyce na cztery główne grupy:

- cybernetyczne (hacking, malware i nieautoryzowany dostęp do systemów IT),
- fizyczne (uszkodzenie materiału, kradzież i sabotaż infrastruktury technicznej),
- ludzkie (błędy, zaniedbania lub brak świadomości pracowników),
- organizacyjne i partnerskie (wymiana informacji, współpraca z podmiotami w łańcuchu dostaw).

Identyfikacja takich kategorii zagrożeń pozwala na wykrycie problemów z bezpieczeństwem i realizację odpowiednich praktyk zarządzania ryzykiem informacyjnym w obszarze logistyki.

Nowo zidentyfikowane kategorie zagrożeń informacyjnych w logistyce powiązane są z Logistyką 4.0, która skupia się na technologiach cyfrowych. Technologie te pozwalają wpływać na efektywność procesów, ale jednocześnie niosą ze sobą nowe zagrożenia informacyjne. Internet Rzeczy (IoT) i urządzenia telemetryczne, które są używane m.in. do monitorowania transportu i lokalizacji ładunku, są szczególnie podatne na ataki MITM, podszywanie się pod urządzenia sieciowe lub ingerowanie w przesyłane dane. Ze względu na ich ogromną ilość i względny brak zabezpieczeń technicznych stanowią one potencjalne słabe ogniwo w infrastrukturze logistycznej (Wołczański, 2021).

Blockchain i powiązane z tą technologią inteligentne kontrakty mają na celu uzyskanie większej przejrzystości i bezpieczeństwa transakcji w łańcuchu dostaw. Jednak w rzeczywistości pojawiają się problemy, które dotyczą niepowodzeń wdrożeniowych, niewłaściwego zarządzania kluczami kryptograficznymi lub braku audytu kodu. W efekcie prowadzi to do naruszenia integralności danych, strat finansowych i utraty reputacji (Boyens i in., 2022).

Zarówno polskie, jak i zagraniczne korporacje logistyczne borykają się z tym samym problemem bezpieczeństwa informacji, a konkretne przykłady potwierdzają, że wpływ tych zdarzeń ma zarówno charakter operacyjny, jak i strategiczny.

W Polsce takie problemy pojawiły się w roku 2024 r., kiedy to magazyn ILS Logistics w Zakroczymiu zawiódł z powodu awarii autonomicznych robotów magazynowych w sekcji sortowania, co skutkowało opóźnieniami w realizacji zamówień. Brak planu awaryjnego sprawił, że minęło dużo czasu, zanim udało się przejść na procesy ręczne, a brak szkolenia pracowników utrudniał diagnozę i naprawę. Konsekwencją były

opóźnienia w dostawach i utrata zaufania klientów (Logistyka.net.pl, 2024).

Herbapol Lublin również musiał stawić czoła zagrożeniu. Z powodu ataku ransomware firma była zmuszona tymczasowo wyłączyć część swoich systemów IT, a sprawcy zażądali okupu w wysokości 900 000 dol. Prewencyjne wyłączenie sklepu internetowego firmy w obawie przed wyciekiem danych klientów okazało się skuteczne. Atak ten spowodował awarię kanału e-commerce, zwiększone koszty reagowania na kryzys i utratę reputacji.

Wśród najbardziej nagłośnionych światowych incydentów był atak ransomware NotPetya na grupę A.P. Moller-Maersk w Danii w 2017 r. Z powodu paraliżu infrastruktury IT operatora w około 600 obiektach, w tym portach i terminalach oraz centrach dystrybucji na całym świecie, została wstrzymana obsługa klienta, co spowodowało straty w wysokości 200–300 mln dol. (CNBC, 2017).

Podobny los spotkał w Australii firmę Booktopia zajmującą się zakupami elektronicznymi. Awaria systemu automatyzacji magazynu, wartego 12 mln dol. australijskich, wywołała znaczne zakłócenia w realizacji zamówień. Brak funduszy na naprawy spowodował, że firma musiała ogłosić bankructwo i zwolnić pracowników (Warehouse Automation, 2024).

Przypadki z Polski, Danii i Australii potwierdzają, że zaawansowane rozwiązania technologiczne mogą stać się przyczyną kryzysu, jeśli nie zadba się o odpowiednie procedury zarządzania ryzykiem i strategię ciągłości działania. Skuteczne zarządzanie zagrożeniami informatycznymi wymaga od firmy zadbania o odpowiednie monitorowanie systemu, przeprowadzania audytów i szkoleń, opracowania polityki reagowania na incydenty z uwzględnieniem regulacji prawnych i standardów branżowych.

Technologiczne wsparcie bezpieczeństwa informacji w logistyce

Znaczenie technologii w ochronie informacji

Rozwój logistyki, szczególnie Logistyki 4.0, wiąże się z nieustanną cyfryzacją procesów i wykorzystaniem technologii informatycznych – od systemów zarządzania danymi po Internet Rzeczy, blockchain i sztuczną inteligencję. Każdy z tych elementów jest integralną częścią nowoczesnych łańcuchów dostaw. Jednak ich zastosowanie wykracza poza samo automatyzowanie i usprawnianie operacji, stanowią one również kluczowe narzędzia do ochrony informacji i zmniejszania prawdopodobieństwa incydentów bezpieczeństwa.

Nowoczesna logistyka opiera się na systemach IT i cyfryzacji procesów. Technologia informacyjna nie tylko ułatwia przepływ towarów, ale także zapewnia monitorowanie ryzyka informacyjnego w czasie rzeczywistym. Ten proces jednak powinien wymagać wprowadzenia odpowiednich zabezpieczeń, aby zapewnić integralność, poufność i dostępność danych firmy. Konsekwencją niedostatecznych rozwiązań technologicznych jest większa podatność na zagrożenia cybernetyczne, awarie infrastruktury i błędy ludzkie.

Systemy bezpieczeństwa informacji w logistyce można podzielić na: systemy klasy ERP, TMS/WMS, systemy monitorowania i kontroli sieci oraz rozwiązania do szyfrowania i uwierzytelniania.

Systemy klasy ERP i TMS/WMS są podstawowymi komponentami współczesnej technologii logistycznej, która łączy dane operacyjne i finansowe przedsiębiorstwa, takie jak monitorowanie zamówień, poziomy zapasów, harmonogram transportu i przepływ towarów (Laudon & Laudon, 2022). Ważne jest zastosowanie odpowiednich zabezpieczeń systemów w odniesieniu do bezpieczeństwa łańcucha dostaw, aby zapewnić ciągłość działania biznesu i zmniejszyć ryzyko przerw w produkcji.

Systemy monitorowania i kontroli sieci, w tym zapory sieciowe, systemy wykrywania włamań (IDS) i systemy zapobiegania włamaniom (IPS) zabezpieczają infrastrukturę IT przed nieautoryzowanym dostępem, atakami DDoS i innymi zagrożeniami zewnętrznymi (Stallings, 2022). Dobrze skonfigurowane i ciągle monitorowane narzędzia umożliwiają szybkie wykrywanie incydentów i zmniejszanie ich wpływu na działalność logistyczną. Z drugiej strony, szyfrowanie danych w formie przechowywanej i przesyłanej, MFA (uwierzytelnianie wieloskładnikowe), podpisy cyfrowe i certyfikaty bezpieczeństwa zwiększają poufność, integralność i dostępność danych wykorzystywanych przez firmy logistyczne (Stallings, 2021). Włączenie takich technologii wraz z mechanizmami bezpieczeństwa i kontrolą dostępu zmniejsza prawdopodobieństwo wycieków danych i naruszeń wrażliwych danych biznesowych.

IoT, blockchain i AI w zarządzaniu bezpieczeństwem informacji

Rozwój zaawansowanych technologii cyfrowych, w tym Internetu Rzeczy (IoT), blockchain i sztucznej inteligencji (AI), nie tylko przyspiesza i ułatwia przepływ produktów i informacji, ale także stawia nowe wyzwania w zakresie bezpieczeństwa informacji, wymagając ochrony i zapewnienia zgodności z przepisami i standardami.

Internet Rzeczy (IoT) odgrywa coraz większą rolę w logistyce. Pozwala monitorować przesyłki, warunki ich magazynowania czy transportu w czasie rzeczywistym. Czujniki IoT zbierają dane o lokalizacji, temperaturze, wilgotności i wstrząsach, co pozwala na szybkie reagowanie i rozwiązywanie potencjalnych problemów (Translogis, 2024). Jednocześnie każde urządzenie IoT jest potencjalnym źródłem zagrożeń, które mogą wynikać z braku skutecznego szyfrowania, luk w oprogramowaniu i braku kontroli dostępu.

Konsekwencje mogą prowadzić do przechwycenia lub manipulacji informacjami. Dlatego dzisiaj standardem dla firm logistycznych jest rozwiązanie Security by Design oparte na IoT, które zakłada, że zabezpieczenia powinny być wdrażane na początku procesu projektowania systemu, co czyni system bardziej odpornym na cyberataki (Translogis, 2024).

Zapewnienie integralności danych to obszar zastosowania technologii rozproszonych, w tym blockchainu. Blockchain to platforma, która udostępnia swoim użytkownikom zdecentralizowane, niezmienne rejestry danych, zapewniające poprawę przejrzystości i integralności informacji o produktach w łańcuchu dostaw. W logistyce blockchain umożliwia (Prajzner, 2020):

- śledzenie przesyłek i dokumentacji przewozowej,
- weryfikację kontraktów handlowych i automatyczne realizowanie płatności (*smart contracts*),
- ograniczenie ryzyka fałszowania danych oraz oszustw w transakcjach.

Przykłady zastosowania technologii rozproszonych rejestrów można znaleźć w globalnych sieciach dostaw w sektorach spożywczym, farmaceutycznym i motoryzacyjnym. Technologia blockchain pozwala na szybkie wykrywanie zarówno rozbieżności, jak i anomalii w tych sieciach, zmniejsza straty wynikające z błędów i oszustw.

W firmach w polskim segmencie TSL technologia ta jest nadal projektem pilotażowym, prowadzonym głównie przez dużych operatorów współpracujących z międzynarodowymi partnerami (Logistyka.net.pl, 2019).

Technologia blockchain gwarantuje integralność danych, podczas gdy AI i zaawansowana analiza danych umożliwiają przewidywanie zagrożeń i reakcję w czasie rzeczywistym. AI przyczynia się także do zwiększenia bezpieczeństwa informacji w logistyce poprzez (Nezianya, Adebayo & Ezeliora, 2024):

- wykrywanie anomalii w czasie rzeczywistym,
- przewidywanie zagrożeń,
- przewidywanie incydentów i awarii systemu,
- automatyczną reakcję na błędne zdarzenia, np.: blokowanie złośliwych sesji w systemie IT.

Sztuczna inteligencja AI może być szczególnie przydatna w dużych i skomplikowanych łańcuchach dostaw, gdzie ręczna kontrola danych nie byłaby technicznie wykonalna. Zastosowanie AI w polskich przedsiębiorstwach nadal jest rzadkie, ale rośnie liczba projektów pilotażowych związanych z monitorowaniem bezpieczeństwa systemów transportowych i usług IT (ID Logistics, 2024).

Technologie informatyczne w świetle norm i regulacji

Zastosowanie nowoczesnych technologii informatycznych musi być realizowane zgodnie z obowiązującymi standardami i przepisami prawnymi. Do istotnych norm należą ISO 27001, ISO 28000, a ważne regulacje prawne to: dyrektywa dotycząca cyberbezpieczeństwa (NIS2), rozporządzenie GDPR oraz ustawa

Tabela 1
Porównanie kluczowych norm i regulacji dotyczących bezpieczeństwa informacji

Dokument/norma	Zakres i cel	Obszar zastosowania	Kluczowe wymagania/obowiązki
ISO/IEC 27001	System zarządzania bezpieczeństwem informacji (ISMS)	Organizacje różnej wielkości, w tym logistyczne	Ochrona poufności, integralności i dostępności danych; identyfikacja i zarządzanie ryzykiem; procedury reagowania na incydenty (Whitman & Mattord, 2021)
ISO 28000	System zarządzania bezpieczeństwem w łańcuchu dostaw	Logistyka, transport, magazyny	Identyfikacja zagrożeń w łańcuchu dostaw, procedury reagowania na incydenty, zapewnienie ciągłości operacyjnej (Staniewska, 2021)
Dyrektywa UE o cyberbezpieczeństwie (NIS2)	Zwiększenie bezpieczeństwa sieci i systemów ICT w UE	Sektory krytyczne, w tym transport i logistyka	Zarządzanie ryzykiem, obowiązek zgłaszania incydentów, wdrożenie środków bezpieczeństwa, audyty i kontrola zgodności (dyrektywa NIS2, s. 8–12)
RODO (2016/679)	Ochrona danych osobowych	Wszystkie podmioty przetwarzające dane osobowe w UE	Zgody na przetwarzanie, ochronę danych, zgłaszanie naruszeń, prawa osób, których dane dotyczą (Adamek, 2024)
Ustawa o krajowym systemie cyberbezpieczeństwa (2018)	Wdrożenie krajowego systemu cyberbezpieczeństwa	Operatorzy usług kluczowych, dostawcy usług cyfrowych w Polsce	Zgłaszanie incydentów, zapewnienie bezpieczeństwa systemów ICT, wdrożenie środków ochronnych, kontrola i audyty (Dz.U. 2018, poz. 1560, s. 3–10)

Źródło: opracowanie własne na podstawie: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2); Adamek, 2024; Staniewska, 2021; Whitman & Mattord, 2021; Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r. W tabeli 1 porównano standardy i regulacje w zakresie bezpieczeństwa informacji. Zgodność rozwiązań IoT, blockchain, systemów AI z wymienionymi aktami prawnymi jest niezbędna, aby zapewnić skuteczne zarządzanie ryzykiem i ochronę danych na poziomie krajowym i międzynarodowym (PwC Polska, 2024; Logistyka.net.pl, 2024). Zapewnienie zgodności technologii z normami w logistyce pozwala na ochronę danych, ale również zwiększa efektywność procesów logistycznych, skraca czas reagowania na awarie oraz zmniejsza ryzyko operacyjne. Systemy zintegrowane z normami pozwalają w logistyce na:

- zwiększenie odporności łańcucha dostaw na zagrożenia informacyjne,
- zmniejszenie negatywnych skutków incydentów lub awarii,
- pomoc menedżerom w podejmowaniu decyzji na podstawie aktualnych danych,
- spełnienie wymagań prawnych i regulacyjnych zarówno lokalnych, jak i globalnych.

Sukces we wdrożeniu technologii ostatecznie zależy od jej właściwego dopasowania do wymagań organizacji, kompetencji pracowników i współpracy z partnerami w łańcuchu dostaw (zob. Staniewska, 2021).

Zarządzanie ryzykiem i ciągłość działania w logistyce

Zarządzanie ryzykiem informacyjnym

Zarządzanie ryzykiem informacyjnym rozumie się jako systematyczną identyfikację, ocenę i kontrolę zagrożeń związanych z informacjami i systemami IT w celu ochrony integralności, poufności i dostępności danych w organizacji (Whitman & Mattord, 2021).

Tabela 2
Cykl PDCA w kontekście logistyki i zarządzania ryzykiem informacyjnym

Etap PDCA	Działania w logistyce	Przykłady zastosowania w logistyce
Planowanie (*plan*)	Identyfikacja ryzyka, analiza procesów logistycznych, określenie potencjalnych zagrożeń dla informacji	Mapowanie przepływu danych w TMS/WMS, analiza punktów krytycznych w łańcuchu dostaw, przewidywanie zagrożeń cybernetycznych
Wdrażanie (*do*)	Wdrożenie procedur zapobiegawczych, zabezpieczeń technicznych i działań minimalizujących skutki incydentów	Instalacja zapór, systemów IDS/IPS, szyfrowanie danych, szkolenia personelu w zakresie bezpieczeństwa informacji
Sprawdzanie (*check*)	Regularna kontrola skuteczności wdrożonych zabezpieczeń, analiza incydentów, audyty wewnętrzne	Testy penetracyjne systemów IT, audyt bezpieczeństwa magazynów, analiza raportów incydentów w logistyce
Doskonalenie (*act*)	Aktualizacja procedur, szkoleń, technologii na podstawie wyników audytów i nowych zagrożeń	Modernizacja systemów ERP/TMS/WMS, aktualizacja polityk bezpieczeństwa, wprowadzenie nowych rozwiązań IT dla monitoringu IoT i AI

Źródło: Whitman & Mattord, 2021.

Tabela 3
Metody oceny ryzyka informacyjnego w logistyce

Metoda	Opis	Przykład zastosowania w logistyce
Jakościowa analiza ryzyka (*qualitative risk assessment*)	Subiektywna ocena prawdopodobieństwa i wpływu zagrożeń	Ocena ryzyka cyberataków w małych magazynach
Ilościowa analiza ryzyka (*quantitative risk assessment*)	Ocena ryzyka na podstawie danych liczbowych i statystyk	Symulacja awarii systemów TMS i WMS w globalnej firmie logistycznej
Mieszana analiza ryzyka (*semi-quantitative risk assessment*)	Łączy ocenę jakościową z elementami ilościowymi	Ocena zagrożeń w procesach magazynowych i transportowych
Analiza rodzajów i skutków wad (FMEA – *failure mode and effects analysis)*	Analiza potencjalnych trybów awarii i ich skutków	Wdrożenie robotyki magazynowej i automatyzacji sortowania paczek
Analiza bow-tie (*bow-tie analysis*)	Graficzne przedstawienie przyczyn i skutków zagrożeń oraz działań kontrolnych	Wizualizacja ryzyka w łańcuchu dostaw e-commerce
Analiza scenariuszowa (*scenario analysis*)	Tworzenie hipotetycznych scenariuszy incydentów i ocena ich skutków	Testowanie reakcji na awarię systemów IoT w transporcie

Źródło: Hubbard, 2020.

Zarządzanie ryzykiem informacyjnym w logistyce odnosi się do zagrożeń wpływających na integralność, poufność i dostępność danych w procesach logistycznych. Proces ten obejmuje ryzyka techniczne (awarie systemów IT, ataki cybernetyczne), ryzyka organizacyjne (błędy ludzkie i niewłaściwe procedury) oraz ryzyka związane z zewnętrznymi partnerami w łańcuchu dostaw (Boyens i in., 2022). Oceny ryzyka mogą być przeprowadzane zgodnie z cyklem PDCA (*plan–do–check–act*), który obejmuje pięć kluczowych faz, jak przedstawiono w tabeli 2.

Oprócz cyklu PDCA istnieje wiele innych metod oceny ryzyka, które można zastosować w logistyce i zarządzaniu ryzykiem informacyjnym, umożliwiających systematyczną identyfikację, analizę i ograniczanie zagrożeń. Należą do nich: FMEA, analiza scenariuszowa, analiza Bow-Tie, analiza ryzyka jakościowa, ilościowa i mieszana. Wybrane oceny ryzyka przedstawiono w tabeli 3.

Ocena ryzyka jest istotną częścią systemu zarządzania bezpieczeństwem informacji i jest jednym z fundamentów normy ISO/IEC 27001. Umożliwia wykrywanie, kategoryzację i kontrolę ryzyk, które mogą zagrozić integralności, poufności i dostępności danych. Wyniki analizy ryzyka determinują decyzje dotyczące środków kontrolnych i kierunków działań na rzecz ochrony informacji. Ocena ryzyka w praktyce nie kończy się, jest to proces powtarzalny, stanowiący punkt wyjścia do budowy polityki bezpieczeństwa informacji, uwzględniający stosowane zabezpieczenia techniczne i organizacyjne czy planowanie ciągłości działania.

Planowanie ciągłości działania w logistyce

Planowanie ciągłości działania (BCP) to zorganizowany proces identyfikacji potencjalnych zagrożeń dla organizacji oraz ustanawiania sformalizowanych protokołów w celu zachowania i szybkiego przywrócenia kluczowych operacji biznesowych w przypadku zakłóceń. Obejmuje on analizę ryzyka, tworzenie planów awaryjnych, procesy odzyskiwania danych i testowanie rozwiązań, aby utrzymać ciągłość działania krytycznych operacji (Whitman & Mattord, 2021).

Planowanie ciągłości działania to proces opracowywania strategii i procedur zapewniających ciągłość strategicznych (krytycznych) procesów biznesowych w całej organizacji przy jednoczesnej minimalizacji skutków incydentów lub awarii systemów IT (Christopher, 2000). Główne etapy planowania ciągłości działania w logistyce obejmują:

- analizę wpływu na biznes (BIA – *business impact analysis*) – identyfikacja krytycznych procesów logistycznych, systemów informacyjnych i zasobów, których utrata może zakłócić działalność firmy;
- opracowanie strategii odzyskiwania – określenie ważności systemów IT i operacji oraz alternatywne lokalizacje centrów danych i kopii zapasowych (*disaster recovery*).
- wdrożenie procedur awaryjnych – instrukcje dla pracowników, harmonogramy odzyskiwania systemów i odzyskiwania komunikacji z partnerami w łańcuchu dostaw;
- testowanie i aktualizację planów – regularne sprawdzanie planu i aktualizacja planów zgodnie ze zmianami technologicznymi i organizacyjnymi (GS1 Polska, 2024; Bielecki i in., 2024).

Plany BCP zyskują na popularności i są coraz częściej wdrażane w polskich przedsiębiorstwach branży TSL, jednak nie zostały jeszcze wystarczająco ustandaryzowane. Raport GS1 (2024) pokazuje, że tylko ok. 1/3 firm posiada procedury ciągłości działania, które uwzględniają zagrożenia cybernetyczne.

Audyty bezpieczeństwa i reakcja na incydenty

Planowanie ciągłości działania organizacji wskazuje priorytety i strategie, ale samo w sobie jest niewystarczające, gdy organizacja nie kontroluje systematycznie skuteczności wdrożonych rozwiązań. Dlatego kolejnym krokiem są audyty bezpieczeństwa oraz procedury reagowania na incydenty, dzięki którym można zweryfikować założenia BCP, zidentyfikować luki i odpowiednio wcześnie zareagować na zagrożenie.

Audyty bezpieczeństwa informacji pomagają organizacjom ocenić skuteczność wdrażania środków bezpieczeństwa, zidentyfikować luki lub obszary wymagające poprawy oraz opracowywać zalecenia dotyczące działań korygujących. Skuteczne audyty obejmują (Staniewska, 2021):

- przegląd polityk i procedur bezpieczeństwa,
- testy penetracyjne systemów IT,
- analizę incydentów i sposobów zarządzania nimi,
- ocenę współpracy z partnerami w łańcuchu dostaw.

Oprócz przeprowadzania audytów należy również opracować procedury reagowania na incydenty (*incident response*, IR). Procedury te obejmują identyfikację nieprawidłowości lub ataków, określenie skali incydentu na podstawie tego, co się wydarzyło, śledzenie jego pochodzenia w systemie, usuwanie przyczyn źródłowych incydentu, przywracanie systemów i procesów do normalnego stanu operacyjnego, aktualizację polityk, planów i środków bezpieczeństwa (Whitman & Mattord, 2021).

W logistyce procedura reagowania na incydenty stanowi istotny element systemu zarządzania bezpieczeństwem informacji. Oznacza to, że każdy scenariusz kryzysowy wspiera zastosowanie ulepszeń proceduralnych. Wdrożenie zintegrowanego planu IR może pomóc w zmniejszeniu wpływu cyberataków, zminimalizowaniu przestojów operacyjnych oraz utrzymaniu zaufania klientów i partnerów.

Podsumowanie

Bezpieczeństwo danych w procesach logistycznych stało się dziś jednym z najważniejszych filarów zarządzania w sektorze TSL. W erze Logistyki 4.0 informacja stała się zasobem strategicznym, porównywalnym pod względem znaczenia z kapitałem finansowym i materialnym. Ochrona danych jest niezbędna do utrzymania ciągłości działania, przewagi konkurencyjnej i zaufania między partnerami w łańcuchu dostaw.

Artykuł omawia teoretyczne i praktyczne podstawy zarządzania bezpieczeństwem informacji w logistyce z uwzględnieniem norm (ISO/IEC 27001, ISO 28000) i regulacji prawnych, które obejmują dyrektywę NIS2, rozporządzenie RODO i ustawę o krajowym systemie cyberbezpieczeństwa. W treści podkreśla się również, jak zaawansowane technologie, takie jak Internet Rzeczy, blockchain i sztuczna inteligencja, prowadzą do zwiększenia efektywności systemów logistycznych, ale także generują potrzebę ochrony informacji w tych systemach.

Część empiryczna obejmuje najważniejsze zagrożenia informacyjne dla logistyki (tj. cybernetyczne, fizyczne, ludzkie i organizacyjne) oraz wskazuje, jak te zagrożenia wpłynęły na firmy zarówno w kraju, jak i za granicą. Omówiono także wybrane modele zarządzania ryzykiem oraz znaczenie planowania ciągłości działania (BCP) i audytów bezpieczeństwa dla efektywnego funkcjonowania ISMS w organizacjach. Podkreślono, że sukces systemów zarządzania bezpieczeństwem informacji zależy nie tylko od wyboru technologii, ale także od kultury organizacyjnej, samoświadomości pracowników i współpracy między partnerami w łańcuchu dostaw.

Rekomendacje

Bezpieczeństwo danych logistycznych to nie tylko techniczna konieczność – to ekonomiczny imperatyw i prawdziwy czynnik konkurencyjności, który wzmacnia odporność firm na nieprzewidywalne wyzwania. Po przeanalizowaniu literatury i studiów przypadków sformułowano praktyczne zalecenia do rozważenia dla firm logistycznych. Obejmują one:

1) Zintegrowane zarządzanie bezpieczeństwem informacji – firmy logistyczne muszą wdrożyć zintegrowane rozwiązania, które spełniają nie tylko normy ISO/IEC 27001 i ISO 28000, ale także uwzględnią wszystkie procesy w łańcuchu dostaw.

2) Planowanie ciągłości działania – przedsiębiorstwa muszą wdrażać i oceniać plany awaryjne, które mogą obejmować systemy ERP, WMS, TMS, a także szeroko zakrojoną infrastrukturę IoT; w tych planach powinny przewidzieć scenariusze z cyberatakami, nagłe przerwy w dostawie prądu i nieoczekiwane problemy z oprogramowaniem.

3) Bezpieczne projektowanie technologii (Security by Design) – organizacje będą musiały włączać do projektu nie tylko kwestie bezpieczeństwa, ale także zasady szyfrowania, mechanizmy autoryzacji i zakładać ograniczanie ilości przechowywanych danych.

4) Podnoszenie kompetencji cyfrowych personelu – przedsiębiorstwa muszą ciągle prowadzić szkolenia z zakresu cyberbezpieczeństwa, reagowania na incydenty i ochrony danych osobowych, aby zmniejszyć ryzyko błędu ludzkiego.

5) Stały monitoring i audyt – firmy muszą regularnie monitorować i przeprowadzać audyty systemów oraz okresowe testy penetracyjne, audyty bezpieczeństwa informacji i testy zgodności wdrożonych procedur.

W wymiarze naukowym zauważono potrzebę rozszerzenia badań w obszarze wpływu sztucznej inteligencji, technologii blockchain i Internetu Rzeczy na bezpieczeństwo danych w branży logistycznej. Przyszłe badania powinny skupić się na przesyłaniu i dzieleniu się danymi w łańcuchach dostaw z zachowaniem poufności i integralności informacji. Ponadto ekonomicznie opłacalne byłoby tworzenie modeli do pomiaru i szacowania strat wynikających z incydentów bezpieczeństwa w firmach sektora TSL. Przydatne byłoby również opracowanie polskich modeli referencyjnych dla audytów bezpieczeństwa i planów ciągłości działania, które można by dostosować do potrzeb sektora logistycznego w Polsce.

Bibliografia/References

Adamek, K. (2024). *Ochrona danych osobowych po ludzku*. Karol Adamek.

Bielecki, M., Wiśniewski, Z., Dukic, G., & Dujak, D. (2024). Supply Chain 4.0: What the supply chains of the future might look like. *Engineering Management in Production and Services, 16*(1), 45–60. https://doi.org/10.2478/emj-2024-0006

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Computer Science, 149*, 65–70. https://doi.org/10.1016/j.procs.2019.01.108

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management. *Transportation Research Part E: Logistics and Transportation Review, 146*, 102217. https://doi.org/10.1016/j.tre.2020.102217

Christopher, M. (2000). *Logistyka i zarządzanie łańcuchem dostaw*. Polskie Centrum Doradztwa Logistycznego.

CNBC. (2017, 28 lipca). *Maersk hit by NotPetya cyberattack, halts global operations*. https://www.cnbc.com/2017/07/28/maersk-hit-by-notpetya-cyberattack.html

Cyberbezpieczni OPTeam. (2025). *Dyrektywa NIS2: Kompleksowy przegląd wymagań w zakresie cyberbezpieczeństwa*. https://cyberbezpieczni.opteam.pl/artykuly/dyrektywa-nis2--kompleksowy-przeglad-wymagan-w-zakresie-cyberbezpieczenstwa-7.html

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz.UE L 333 z 27.12.2022, s. 80–152.

Enache, G. I. (2023). Logistics security in the era of big data, cloud computing and IoT. *Proceedings of the International Conference on Business Excellence, 17*(1), 188–199. https://doi.org/10.2478/picbe-2023-0021

GS1 Polska. (2024). *Raport – ESG w TSL. Jesteśmy gotowi?* https://gs1pl.org/app/uploads/2024/12/ESG-w-TSL.-Jestesmy-gotowi-GS1.pdf

Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks, 9*(1), 1–16.

Hlynskyy, N., Dovhun, O., & Pochopień, J. (2025). Digitalization and cybersecurity in companies and chains: Challenges and opportunities. *Scientific Journal of Bielsko-Biala School of Finance and Law, 29*(1). https://doi.org/10.19192/wsfip.sj1.2025.7

Hubbard, D. (2020). *Failure of risk management: Why it's broken and how to fix it*. Wiley. https://doi.org/10.1002/9781119521914

ID Logistics. (2024). *Czy AI wspiera logistykę kontraktową w Polsce? K+ Research by Insight Lab.* https://www.id-logistics.com/media/2024/10/Czy-AI-wspiera-logistyke-kontraktowa-w-Polsce.pdf

International Organization for Standardization. (2022). ISO 28000:2022 – Security management systems for the supply chain.

Janczewska, D., & Janczewski, J. (2021). Zarządzanie ryzykiem na rynku usług logistycznych. *Zarządzanie Innowacyjne w Gospodarce i Biznesie, 2*(33), 151–163. https://doi.org/10.25312/2391-5129.33/2021_10djjj

Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions, 31*(1), 61–78. https://doi.org/10.37190/ord210104

Latsiou, A., & Lambrinoudakis, C. (2026). Cyber supply chain risk management: From threats to treatment. *International Journal of Information Security, 25*, 40. https://doi.org/10.1007/s10207-025-01207-9

Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.

Leligou, H. C., et al. (2024). Cybersecurity in supply chain systems: The farm-to-fork use case. *Electronics, 13*(1), 215. https://doi.org/10.3390/electronics13010215

Logistyka.net.pl. (2024, 9 kwietnia). *Pierwszy w Polsce magazyn z robotami Skypod® w pełni funkcjonalny*. https://www.logistyka.net.pl/aktualnosci/item/96233-pierwszy-w-polsce-magazyn-z-robotami-skypod-w-pelni-funkcjonalny

Łapka, W. (2025). Cyberbezpieczeństwo w logistyce: wyzwania, zagrożenia i najlepsze praktyki. *Logistyka,* (1), 60–63.

Nezianya, M. C., Adebayo, A. O., & Ezeliora, P. (2024). A critical review of machine learning applications in supply chain risk management. *World Journal of Advanced Research and Reviews, 23*(3), 1554–1567. https://doi.org/10.30574/wjarr.2024.23.3.2760

Nowak, P. A. (2025). *Systemy informatyczne w organizacjach*. Wydawnictwo Uniwersytetu Łódzkiego. https://doi.org/10.18778/8331-809-7

Nyszk, Ł. (2019). Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM. *Gospodarka Materiałowa i Logistyka*, (5), 472–483.

Picus Security. (2023). *The Blue Report*. https://static.rainfocus.com

Prajzner, G. (2020). *Blockchain – korzyści dla logistyki*. https://www.logistyka.net.pl/bank-wiedzy/item/90729-blockchain-korzysci-dla-logistyki

PwC Polska. (2024). *Gotowi na sztuczną inteligencję*. https://www.pwc.pl/pl/publikacje/gotowi-na-sztuczna-inteligencje-raport.html

Roszczyk-Krowicka, D. (2024). *Od sztucznej inteligencji po elektryfikację – nowe technologie w logistyce 2024*. https://www.logistyka.net.pl/bank-wiedzy/item/95645-od-sztucznej-inteligencji-po-elektryfikacje-nowe-technologie-w-logistyce-2024

Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson.

Staniewska, E. (2021). Wybrane aspekty zarządzania bezpieczeństwem łańcuchów dostaw. *Systemy Logistyczne Wojsk, 54*, 135–148. https://doi.org/10.37055/slw/140379

Szczepanik, T., & Sobala, N. (2021). *Zarządzanie ryzykiem w systemach logistycznych*. Politechnika Częstochowska.

Szymonik, A., Szymonik, A., Dymyt, M., & Wincewicz-Bosy, M. (2024). Cybersecurity threats and practices in the logistics industry in Poland. *European Research Studies Journal, 27*(3), 1108–1123. https://doi.org/10.35808/ersj/3855

Translogis. (2024). *Internet rzeczy (IoT) w logistyce – czym jest? Jak działa?* https://www.translogis.pl/pl/nws/internet-rzeczy-iot-w-logistyce-czym-jest-jak-dziala

Tyburczy, M. (2019). *Rewolucyjny blockchain i logistyka*. https://www.logistyka.net.pl/bank-wiedzy/item/90729

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.

VECTO. (2023). *Cyberbezpieczeństwo w polskich firmach*. https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2023.pdf

Warehouse Automation. (2024). *Automation project leads to disastrous results.* https://www.warehouseautomation.ca/news/12-million-automation-failure-leads-to-clients-bankruptcy-n4s7s-w9r4h

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Wołczański, T. (2021). Inteligentne technologie Przemysłu 4.0 w logistyce bezpieczeństwa pracy. *Ekonomika i Organizacja Logistyki, 6*(4), 113–123. https://doi.org/10.22630/EIOL.2021.6.4.32

Żywucka-Kozłowska, E., & Dziembowski, R. (2023). Wokół definicji cyberbezpieczeństwa. *Cybersecurity and Law, 10*(2), 123–132. https://doi.org/10.35467/cal/174923

Dr inż. Izabela Horzela

Doktor nauk ekonomicznych w dyscyplinie nauki o zarządzaniu, absolwentka Wydziału Organizacji i Zarządzania Politechniki, adiunkt na Wydziale Zarządzania i Dowodzenia Akademii Sztuki Wojennej. Absolwentka Wydziału Organizacji i Zarządzania Politechniki Śląskiej. Jej zainteresowania naukowe obejmują zarządzanie, jakość oraz zarządzanie procesami w organizacjach. Autorka licznych artykułów i referatów naukowych, uczestniczka i współorganizatorka krajowych i międzynarodowych konferencji naukowych.

Dr inż. Izabela Horzela

PhD in Economics (Management Sciences), graduate of the Faculty of Organization and Management, Silesian University of Technology. Assistant Professor at the Faculty of Management and Command, War Studies University. Her research focuses on management, quality, and process management in organizations. She is the author of numerous scientific articles and papers and has actively participated in and co-organized national and international scientific conferences.