mgr inż. Ewa Brodacz
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-6469-9159

dr inż. Ewa Stamirowska-Krzaczek
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-6653-9055

dr inż. Justyna Siwiela-Tomaszczyk
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-2303-9285

Angelika Stopa
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0004-2908-3273

Michał Wrześniewski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0007-5021-8568

https://doi.org/10.29316/9788368103205_4

CYBERZAGROŻENIA W ŁAŃCUCHU DOSTAW ŻYWNOŚCI – WPŁYW CYBERATAKÓW NA SEKTOR ROLNO-SPOŻYWCZY I BEZPIECZEŃSTWO WEWNĘTRZNE PAŃSTWA

CYBER THREATS IN THE FOOD SUPPLY CHAIN – THE IMPACT OF CYBERATTACKS ON THE AGRI-FOOD SECTOR AND NATIONAL INTERNAL SECURITY

Streszczenie

W rozdziale przeanalizowano wpływ cyberzagrożeń na sektor rolno-spożywczy oraz

Summary

This chapter analyzes the impact of cyber threats on the agri-food sector and their

ich konsekwencje dla bezpieczeństwa wewnętrznego państwa. Przedstawiono strukturę współczesnego łańcucha dostaw żywności i opisano główne technologie wykorzystywane w rolnictwie cyfrowym, takie jak Internet rzeczy (IoT), systemy SCM, automatyzacja oraz blockchain. Omówiono kluczowe zagrożenia cybernetyczne, w tym ataki ransomware, sabotaż infrastruktury krytycznej, manipulację danymi oraz szpiegostwo przemysłowe. Wskazano ekonomiczne, społeczne, polityczne, środowiskowe i zdrowotne skutki cyberataków na sektor spożywczy. Zaproponowano strategie budowania odporności sektora, w tym wdrażanie międzynarodowych norm bezpieczeństwa (ISO/IEC 27001, NIST), szyfrowanie danych, szkolenia pracowników i implementację technologii blockchain. Rozdział omawia również dobre praktyki międzynarodowe oraz rekomendacje dla Polski. Podkreślono, że cyberbezpieczeństwo sektora żywnościowego powinno być integralnym elementem strategii bezpieczeństwa narodowego.

Słowa kluczowe: bezpieczeństwo żywnościowe, cyberzagrożenia, sektor rolno-spożywczy, ransomware, blockchain, bezpieczeństwo narodowe

consequences for national internal security. It presents the structure of the modern food supply chain and describes the main technologies used in digital agriculture, such as the Internet of Things (IoT), supply chain management (SCM) systems, automation, and blockchain. Key cybersecurity threats are discussed, including ransomware attacks, sabotage of critical infrastructure, data manipulation, and industrial espionage. The chapter identifies the economic, social, political, environmental, and health impacts of cyberattacks on the food sector. It proposes strategies to enhance sector resilience, including the implementation of international security standards (ISO/IEC 27001, NIST), data encryption, employee training, and blockchain deployment. The chapter also reviews international best practices and provides recommendations for Poland. It emphasizes that cybersecurity in the food sector should be an integral part of national security strategies.

Keywords: food security, cyber threats, agri-food sector, ransomware, blockchain, national security

Wstęp

Współczesne państwa opierają swoją odporność wewnętrzną na wielu filarach. Jednym z kluczowych jest bezpieczeństwo żywnościowe. Stabilny dostęp do żywności, zarówno pod względem ilości, jakości oraz dostępności ekonomicznej, wpływa bezpośrednio na spokój społeczny, stabilność gospodarczą jak i polityczną suwerenność kraju[1]. W dobie globalizacji i postępującej digitalizacji sektor rolno-spożywczy stał się celem cyberataków, które mogą destabilizować dostawy żywności na masową skalę.

[1] J. Clapp, *Food, Politics, and Society: Toward a Critical Research Agenda*, Global Food Security, nr 28, art. 100476, 2021,

Łańcuch dostaw żywności, obejmujący produkcję, przetwórstwo, logistykę, dystrybucję i sprzedaż detaliczną, jest obecnie silnie zależny od technologii informatycznych[2]. Internet rzeczy (IoT), systemy zarządzania łańcuchem dostaw (SCM), blockchain oraz systemy automatyzacji i robotyzacji bez wątpienia usprawniły wiele procesów w sektorze rolno-spożywczym, ale również każdy z tych systemów, mimo korzyści, może stać się potencjalnym celem ataków ze strony cyberprzestępców czy nawet wrogich państw[3].

Narastające zagrożenia cybernetyczne w sektorze rolno-spożywczym to nie tylko problem technologiczny – mogą one realnie wpłynąć na stabilność państwa: od gwałtownych wzrostów cen żywności, poprzez destabilizację społeczną, aż po strategiczne osłabienie suwerenności gospodarczej[4]. Ataki ransomware, sabotaż infrastruktury krytycznej, manipulacja danymi logistycznymi czy cyberatak na inteligentne systemy rolnicze mogą prowadzić do przerw w dostawach podstawowych produktów żywnościowych, wzrostu inflacji, a w skrajnych przypadkach – nawet do kryzysów humanitarnych.

Celem niniejszego rozdziału jest analiza kluczowych cyberzagrożeń w łańcuchu dostaw żywności oraz ocena ich konsekwencji dla gospodarki i bezpieczeństwa narodowego. Ponadto wskazane zostaną możliwe strategie zabezpieczenia sektora rolno-spożywczego oraz przykłady dobrych praktyk na poziomie międzynarodowym.

Niniejszy rozdział został opracowany na podstawie analizy literatury przedmiotu oraz dostępnych danych i raportów dotyczących cyberzagrożeń w sektorze rolno-spożywczym. W procesie badawczym zastosowano metodę przeglądu systematycznego, uwzględniając publikacje naukowe, raporty rządowe, dokumenty organizacji międzynarodowych oraz studia przypadków rzeczywistych incydentów cybernetycznych.

Dobór materiału opierał się na następujących kryteriach:

- publikacje z recenzowanych czasopism naukowych wydanych w latach 2010-2024,
- raporty i wytyczne renomowanych instytucji, takich jak FAO, ENISA, CISA, FDA, OECD, NIST,

[2] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (Updated Edition)*, W. W. Norton & Company, New York 2020.

[3] National Academies of Sciences, Engineering and Medicine, *Science Breakthroughs to Advance Food and Agricultural Research by 2030*, National Academies Press, Washington 2020.

[4] L. Bodin, L. A. Gordon, *Cybersecurity Risk Management for Critical Infrastructure: A Food Supply Chain Perspective*, Journal of Risk Research, nr 23(7-8), 2020, s. 1048-1060.

- studia przypadków głośnych ataków cybernetycznych na sektor rolno-spożywczy (m.in. atak na JBS Foods),
- opracowania dotyczące zastosowania technologii blockchain, IoT, SCM oraz systemów automatyzacji w rolnictwie i przetwórstwie.

Analiza obejmowała identyfikację kluczowych typów zagrożeń, ocenę ich potencjalnych skutków dla bezpieczeństwa wewnętrznego państw oraz przegląd istniejących strategii prewencji i reagowania. Zastosowano podejście jakościowe, ukierunkowane na syntetyzowanie aktualnego stanu wiedzy oraz formułowanie rekomendacji dla polityk publicznych.

Współczesny łańcuch dostaw żywności i jego podatność na cyberzagrożenia

Struktura łańcucha dostaw żywności

Łańcuch dostaw żywności obejmuje pięć głównych etapów: produkcję, przetwórstwo, logistykę, dystrybucję i sprzedaż detaliczną. Każdy z tych elementów jest w coraz większym stopniu zinformatyzowany i zależny od infrastruktury cyfrowej[5]. Współczesne gospodarstwa rolne wykorzystują precyzyjne systemy zarządzania plonami i zasobami, zakłady przetwórcze polegają na zautomatyzowanych liniach produkcyjnych, a firmy logistyczne oraz sieci handlowe zarządzają zapasami w czasie rzeczywistym.

Rosnąca kompleksowość łańcucha dostaw zwiększa jego podatność na cyberzagrożenia. Rozwój handlu elektronicznego w branży spożywczej oraz rosnące znaczenie platform e-commerce jeszcze bardziej potęgują to ryzyko – jak pokazuje analiza Goik i Ciupak[6], wzrost częstotliwości zakupów żywności online i rozproszenie danych logistycznych wymagają nowego podejścia do bezpieczeństwa cyfrowego w tym obszarze. Wzajemne powiązania pomiędzy różnymi podmiotami (rolnicy, przetwórcy, dystrybutorzy, detaliści) oznaczają, że skuteczny cyberatak na jeden element systemu może doprowadzić do efektu domina i zakłóceń w całym sektorze[7].

---

[5] M. M. Aung, Y. S. Chang, *Traceability in a food supply chain: Safety and quality perspectives*, Food Control, nr 39, 2014, s. 172-184.

[6] D. Goik, M. Ciupak, *Dostawy żywności w systemie e-commerce – ich przyszłość i uwarunkowania*, Problemy Drobnych Gospodarstw Rolnych, nr 2, 2018, s. 23-33.

[7] A. Miremadi, A. Moeini, B. Ajirloo, *IoT-Based Smart Agriculture: Cybersecurity Issues and Challenges*, Journal of Ambient Intelligence and Humanized Computing, 2022.

Technologie wykorzystywane w sektorze rolno-spożywczym

Internet rzeczy (IoT) i inteligentne systemy zarządzania rolnictwem. Internet rzeczy w rolnictwie (Agri-IoT) obejmuje wykorzystanie czujników, dronów, autonomicznych pojazdów i innych urządzeń umożliwiających precyzyjne zarządzanie uprawami, nawadnianiem czy hodowlą zwierząt[8]. Chociaż technologie te zwiększają wydajność i zmniejszają zużycie zasobów, są one narażone na cyberataki, takie jak przejęcie kontroli nad urządzeniami czy manipulacja danymi.

Oprogramowanie do zarządzania łańcuchem dostaw (SCM). Nowoczesne systemy SCM umożliwiają monitorowanie i koordynowanie przepływu surowców i produktów w czasie rzeczywistym. Naruszenia w tych systemach mogą prowadzić do poważnych zakłóceń dostaw, manipulacji zamówieniami, czy fałszowania dokumentacji logistycznej[9].

Automatyzacja i robotyzacja w produkcji żywności. Zakłady przetwórstwa żywności coraz częściej wykorzystują roboty do pakowania, sortowania i kontroli jakości produktów. Zautomatyzowane linie produkcyjne, sterowane cyfrowo, są jednak podatne na ataki typu ransomware lub sabotaż, co może całkowicie sparaliżować produkcję[10].

Blockchain jako potencjalne zabezpieczenie przed fałszerstwami. Blockchain, jako rozproszona baza danych, może zwiększyć przejrzystość i bezpieczeństwo łańcucha dostaw żywności, umożliwiając śledzenie produktów „od pola do stołu”[11]. Jak zauważa Kosior[12], technologia ta może w istotny sposób podnieść wiarygodność informacji o pochodzeniu i jakości żywności, szczególnie w kontekście szybkiej identyfikacji źródeł zagrożeń. Niemniej jednak nie jest ona wolna od słabości – m.in. błędów implementacyjnych

[8] S. Wolfert i in., *Big Data in Smart Farming – A review*, Agricultural Systems, nr 153, 2017, s. 69-80.

[9] H. Min, G. Zhou, *Supply chain modeling: past, present and future*, Computers & Industrial Engineering, nr 43(1-2), 2002, s. 231-249.

[10] F. Tian, Z. Li, Y. Liu, *Food Supply Chain Digitalization: Opportunities and Challenges*, Computers and Electronics in Agriculture, nr 186, 2021, art. 106184.

[11] F. Casino, T. K. Dasaklis, C. Patsakis, *A systematic literature review of blockchain-based applications: Current status, classification and open issues*, Telematics and Informatic,s nr 36, 2019, s. 55-81.

[12] K. Kosior, *Potencjał technologii blockchain w zapewnianiu bezpieczeństwa i jakości żywności*, Żywność. Nauka. Technologia. Jakość, nr 25(4), 2018, s. 22-31.

czy luk w warstwie użytkowej, które mogą zostać wykorzystane przez cyberprzestępców.

Główne luki bezpieczeństwa w systemach cyfrowych sektora spożywczego

Sektor rolno-spożywczy często nie posiada zaawansowanych mechanizmów ochrony cybernetycznej, co czyni go atrakcyjnym celem dla atakujących [13]. Główne luki bezpieczeństwa obejmują:

- niski poziom aktualizacji oprogramowania i firmware'u urządzeń IoT,
- brak szkoleń z zakresu cyberhigieny wśród rolników i pracowników sektora,
- ograniczone inwestycje w cyberbezpieczeństwo w porównaniu z innymi sektorami krytycznymi,
- uzależnienie od zewnętrznych dostawców technologii, co zwiększa ryzyko łańcuchowe.

Główne zagrożenia cybernetyczne w sektorze rolno-spożywczym

Ataki ransomware – paraliżowanie systemów przetwórczych i logistycznych. Jednym z najpoważniejszych zagrożeń dla sektora rolno-spożywczego są ataki typu ransomware. Polegają one na szyfrowaniu systemów informatycznych firmy i żądaniu okupu za ich odblokowanie. Skutki takich ataków są katastrofalne: zatrzymanie produkcji, zakłócenie logistyki, utrata danych produkcyjnych i finansowych.

Przykładem jest atak ransomware na JBS Foods w 2021 r. największego na świecie producenta mięsa, który doprowadził do czasowego zamknięcia zakładów przetwórczych w USA, Kanadzie i Australii[14]. Koszty związane z okupem oraz zakłóceniem łańcucha dostaw szacowano na dziesiątki milionów dolarów. Zestawienia incydentów opracowane przez CSIS[15] wskazują, że liczba cyberataków na sektor spożywczy rośnie, a ich skala coraz częściej obejmuje całe kraje. Ataki ransomware nie tylko wpływają na produkcję i dostawy

[13] N. Kshetri, *Blockchain's roles in strengthening cybersecurity and protecting privacy*, Telecommunications Policy nr 42(4), 2018, s. 327-339.

[14] L. H. Newman, *Hackers Hit the World's Largest Meat Supplier With Ransomware*, *Wired Magazine*, 2021.

[15] Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents*, Washington 2021.

żywności, ale mogą również wywoływać panikę konsumencką i destabilizować rynki rolno-spożywcze[16].

Ataki na infrastrukturę krytyczną. Łańcuch dostaw żywności jest uzależniony od infrastruktury krytycznej, takiej jak dostawy wody, energii elektrycznej i chłodnictwa. Cyberataki na te elementy mogą spowodować masowe straty w sektorze rolnym i spożywczym.

W 2021 r. odnotowano cyberatak na zakład uzdatniania wody w Oldsmar na Florydzie, gdzie hakerzy próbowali zwiększyć poziom ługu sodowego w wodzie do niebezpiecznego poziomu[17]. Choć nie był to atak na sektor spożywczy per se, pokazuje on potencjalne zagrożenia dla bezpieczeństwa żywności i zdrowia publicznego poprzez manipulację infrastrukturą wodną.

Manipulacja danymi i sabotaż łańcucha dostaw. Cyberprzestępcy mogą manipulować danymi w systemach zarządzania łańcuchem dostaw: zmieniać daty przydatności do spożycia, fałszować certyfikaty jakości lub zmieniać trasy dostaw, prowadząc do strat finansowych i ryzyka zdrowotnego dla konsumentów[18]. Sabotaż logistyczny może polegać na przekierowywaniu dostaw na fałszywe adresy lub celowym opóźnianiu transportu łatwo psujących się produktów.

Ataki na inteligentne rolnictwo. Automatyczne systemy nawadniania, nawożenia czy karmienia zwierząt są podatne na przejęcie przez cyberprzestępców. Skutki takich ataków mogą być katastrofalne, np. zatrzymanie podlewania upraw w okresie suszy lub przedawkowanie nawozów, prowadzące do ich zniszczenia[19]. Ataki na inteligentne gospodarstwa mogą mieć także charakter długofalowy – trudny do wykrycia sabotaż, powodujący stopniowe obniżanie plonów i jakości produktów.

Kradzież danych i szpiegostwo przemysłowe. Sektor rolno-spożywczy gromadzi cenne dane: o metodach uprawy, recepturach produktów, dostawcach czy klientach. Kradzież tych danych może służyć zarówno celom komercyjnym, jak i strategicznym. Szpiegostwo przemysłowe w rolnictwie

[16] A. Clopton, *Ransomware: Paralyzing Critical Infrastructure*, Journal of Cybersecurity nr 8(1), 2022, art. 1-14.

[17] U.S. Department of Homeland Security, *CISA Insights: Mitigating Attacks Against Critical Infrastructure*, Washington 2021.

[18] H. Boyes i in., *The Industrial Internet of Things (IIoT): An Analysis Framework*, Computers in Industry nr 101, 2018, s. 1-12.

[19] S. Wolfert i in., *Big Data…, op. cit.*

i przemyśle spożywczym jest coraz częściej notowane, a jego skutki obejmują zarówno bezpośrednie straty finansowe, jak i długofalowe poważne ryzyko utraty konkurencyjności[20].

Skutki cyberataków dla bezpieczeństwa wewnętrznego państwa

Skutki ekonomiczne: wzrost cen żywności i straty w sektorze rolnym i spożywczym. Cyberataki na sektor rolno-spożywczy mogą prowadzić do znaczących strat finansowych. Zakłócenia w produkcji i logistyce powodują wzrost cen produktów spożywczych, a także zmniejszenie podaży na rynku[21]. W przypadku długotrwałych zakłóceń, takich jak ataki ransomware na przetwórnie lub dostawców żywności, skutkiem może być gwałtowna inflacja cen podstawowych produktów. Ponadto straty finansowe ponoszą przedsiębiorstwa sektora – koszty obejmują okup, przestoje produkcyjne, odszkodowania, a także inwestycje w odbudowę i zabezpieczenie systemów[22]. Średni koszt przestoju w sektorze spożywczym może sięgać milionów dolarów dziennie.

Skutki społeczne: panika konsumentów, braki żywnościowe, destabilizacja rynków. W przypadku poważnych zakłóceń w dostawach żywności może dojść do paniki konsumenckiej – podobnie jak obserwowano to podczas pandemii COVID-19 przy brakach papieru toaletowego czy produktów pierwszej potrzeby[23]. Wzrost niepewności prowadzi do wykupywania zapasów, co tylko pogłębia braki i potęguje niestabilność. Zakłócenia w sektorze spożywczym mogą także powodować destabilizację rynków pracy (np. w rolnictwie sezonowym), wzrost bezrobocia w sektorach powiązanych oraz ogólne obniżenie poziomu życia ludności[24]. Jak zauważa IFRC[25], brak dostępu do żywności wynikający z zakłóceń systemowych – w tym cyfrowych – może prowadzić do napięć społecznych i humanitarnych kryzysów. Według UNDRR[26], zakłócenia w sektorach podstawowych, takich jak żywność, mogą prowadzić

[20] D. Manheim, *Cybersecurity and Agriculture: Threats and Impacts*, Journal of Agricultural and Environmental Ethics, nr 31(4), 2018, s. 581-600.

[21] OECD, *Strengthening Agricultural Resilience in the Face of Multiple Risks*, Paryż 2020.

[22] N. Kshetri, *Blockchain's roles…,* op. cit.

[23] D. Laborde i in., *COVID-19 risks to global food security*, Science, nr 369(6503), 2020, s. 500-502.

[24] J. Clapp, *Food, Politics…,* op. cit.

[25] International Federation of Red Cross and Red Crescent Societies (IFRC), *World Disasters Report 2021: Hunger and Food Insecurity*, Genewa 2021.

[26] United Nations Office for Disaster Risk Reduction (UNDRR), *Global Assessment Report on Disaster Risk Reduction*, Genewa 2019.

do tzw. kaskadowych skutków społecznych i destabilizacji funkcjonowania całych regionów.

Skutki polityczne: zagrożenia dla suwerenności żywnościowej. Bezpieczeństwo żywnościowe jest nieodłącznym elementem suwerenności narodowej. Długotrwałe lub powtarzające się cyberataki na sektor rolno-spożywczy mogą zmusić państwa do zwiększonego importu żywności lub zawierania niekorzystnych umów handlowych[27]. Osłabienie własnych zdolności produkcyjnych i logistycznych prowadzi do utraty kontroli nad podstawowymi zasobami strategicznymi, co może być wykorzystywane jako element presji politycznej przez inne państwa lub grupy interesów[28].

Skutki środowiskowe: skutki ataków na systemy nawożenia, pestycydy i gospodarkę wodną. Cyberataki na systemy zarządzania nawożeniem i gospodarką wodną mogą mieć poważne konsekwencje środowiskowe. Niewłaściwe dawkowanie nawozów lub pestycydów może prowadzić do skażenia gleby i wód gruntowych, zniszczenia plonów oraz długofalowego pogorszenia jakości środowiska rolniczego[29]. Uszkodzenie lub sabotaż systemów nawadniania może prowadzić do strat w produkcji rolniczej, a w skrajnych przypadkach – do pustynnienia terenów rolnych.

Skutki zdrowotne: ryzyko zatruć żywności i przerwania dostaw podstawowych produktów. Manipulacja danymi dotyczącymi bezpieczeństwa żywności (takimi jak daty przydatności do spożycia lub parametry przechowywania) może zwiększać ryzyko zatruć żywności[30]. Dodatkowo przerwanie dostaw podstawowych produktów, takich jak mleko, chleb czy mięso, prowadzi do niedoborów żywieniowych w populacji. Ataki mogą również wpływać na ograniczenie dostępu do specjalistycznych produktów żywieniowych dla osób chorych (np. żywność bezglutenowa, żywność medyczna), co stwarza dodatkowe zagrożenia dla zdrowia publicznego.

---

[27] FAO, *The State of Food Security and Nutrition in the World 2021*, Food and Agriculture Organization of the United Nations, Rzym 2021.

[28] D. Barkin, *Food Sovereignty: A Critical Dialogue*, Globalizations, nr 16(7), 2019, s. 1047-1065..

[29] Y. Zhang, R. Deng, J. Weng, *Smart farming cyber security: A review*, Computers and Electronics in Agriculture, nr 140, 2017, s. 297-310.

[30] R. Smith, A. Young, *Food safety vulnerabilities and cybersecurity risks*, British Food Journal, nr 123(12), 2021, s. 4047-4063.

Strategie zabezpieczenia sektora rolno-spożywczego przed cyberatakami

Budowanie odporności cybernetycznej poprzez wdrażanie norm i standardów bezpieczeństwa (np. NIST, ISO/IEC 27001). Podstawowym elementem zabezpieczania sektora rolno-spożywczego jest implementacja uznanych norm bezpieczeństwa informacyjnego. W polskim kontekście działania te wpisują się w założenia ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r., która – jak wskazuje Terlikowski (2018 r.) – wyznacza ramy funkcjonowania krajowych i sektorowych zespołów reagowania na incydenty oraz identyfikuje zagrożenia cyfrowe jako jeden z kluczowych elementów bezpieczeństwa wewnętrznego państwa[31]. Standardy, takie jak ISO/IEC 27001 definiują wymagania dla systemów zarządzania bezpieczeństwem informacji, obejmując audyty ryzyk, zarządzanie incydentami i ciągłość działania[32]. W kontekście polskim szczególnie istotne wydają się wnioski Najwyższej Izby Kontroli (2022 r.), która wskazuje, że mimo istnienia wielu mechanizmów nadzoru nad bezpieczeństwem żywności, systemy te charakteryzują się poważnymi brakami organizacyjnymi i kompetencyjnymi[33]. Ich uzupełnienie – także w zakresie cyberbezpieczeństwa – stanowi jeden z kluczowych warunków zwiększenia odporności sektora na zagrożenia cyfrowe. Dodatkowo wytyczne amerykańskiego Narodowego Instytutu Standaryzacji i Technologii (NIST), takie jak Cybersecurity Framework[34], dostarczają praktycznych narzędzi oceny ryzyk i projektowania planów odporności cybernetycznej w sektorach krytycznych, w tym w łańcuchu dostaw żywności.

Ulepszanie systemów szyfrowania danych i ochrony infrastruktury krytycznej. Wdrożenie zaawansowanych technik szyfrowania transmisji danych (np. szyfrowanie end-to-end) oraz ochrony baz danych może znacząco utrudnić przechwycenie wrażliwych informacji[35]. Konieczne jest również stosowanie segmentacji sieci, ochrony przed atakami typu DDoS oraz zabezpieczenia

[31] T. Terlikowski, *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów*, Zeszyty Naukowe SGSP, nr 71(2), 2018, s. 137-150.

[32] ISO/IEC, *ISO/IEC 27001:2013 Information Security Management Systems – Requirements*, International Organization for Standardization, Genewa 2013.

[33] Najwyższa Izba Kontroli, *System kontroli bezpieczeństwa żywności w Polsce – stan obecny i pożądane kierunki zmian*, Warszawa 2022.

[34] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg 2018.

[35] W. Stallings, *Cryptography and Network Security: Principles and Practice* (7 ed.), Pearson, Boston 2017.

systemów SCADA i ICS, które zarządzają automatyzacją w produkcji i przetwórstwie żywności[36]. Jak podkreśla U.S. Department of Homeland Security[37], sektor żywnościowy powinien być traktowany na równi z innymi sektorami infrastruktury krytycznej w zakresie ochrony przed cyberatakami. Wymaga to wdrażania dedykowanych procedur zarządzania ryzykiem oraz reagowania na incydenty w czasie rzeczywistym.

Współpraca sektora publicznego i prywatnego w zakresie monitorowania cyberzagrożeń. Ze względu na złożoność i transgraniczny charakter zagrożeń, niezbędna jest ścisła współpraca między sektorem prywatnym, instytucjami państwowymi i organizacjami międzynarodowymi[38]. Tworzenie wspólnych centrów reagowania na incydenty (CSIRT), platform wymiany informacji o zagrożeniach (ISAC) oraz publicznych baz danych zagrożeń cybernetycznych (np. MITRE ATT&CK) pozwala na szybsze wykrywanie i neutralizowanie zagrożeń.

Programy szkoleniowe dla rolników, producentów i dystrybutorów żywności. Jednym z najczęstszych wektorów ataku jest człowiek – tzw. czynnik ludzki. W sektorze rolno-spożywczym, gdzie często brakuje zaawansowanej wiedzy informatycznej, edukacja w zakresie podstaw cyberbezpieczeństwa jest kluczowa[39].

Programy szkoleniowe powinny obejmować:

- rozpoznawanie prób phishingu,
- stosowanie silnych haseł,
- aktualizowanie oprogramowania,
- bezpieczne korzystanie z urządzeń IoT.

Implementacja technologii blockchain w śledzeniu dostaw żywności. Blockchain może zwiększyć odporność łańcucha dostaw poprzez transparentność transakcji i niezmienność zapisów danych[40]. Przykładowo: rejestracja każdej partii żywności od produkcji do sprzedaży w rozproszonej sieci bloków danych pozwala na szybkie wykrywanie fałszerstw i sabotażu. Dodatkowo

[36] M. Krotofil, D. Gollmann, *Industrial control systems security: What is happening?*, Industrial Control Systems Security (ICSS) Workshop**,** 2013.

[37] U.S. Department of Homeland Security, *CISA Insights…,* op. cit.

[38] L. Bodin, L. A. Gordon, *Cybersecurity Risk Management…,* op. cit.

[39] SANS Institute, *Security Awareness Report: Managing Human Risk*, 2020.

[40] F. Casino i in., *A systematic literature review…,* op. cit.

zastosowanie smart kontraktów może automatyzować procesy kontroli jakości i płatności.

Przykłady dobrych praktyk i międzynarodowe regulacje.

Polityki cyberbezpieczeństwa w sektorze rolno-spożywczym w USA, UE i Azji. W USA bezpieczeństwo sektora rolno-spożywczego jest jednym z priorytetów w narodowej strategii cyberbezpieczeństwa. Ustawa Food Safety Modernization Act (FSMA) rozszerzyła uprawnienia FDA w zakresie monitorowania i zapobiegania zagrożeniom dla łańcucha dostaw żywności[41]. W 2022 r. Departament Rolnictwa (USDA) opublikował wytyczne dla rolników dotyczące cyberhigieny oraz rozpoczął wdrażanie programów pilotażowych w zakresie cyberodporności gospodarstw rolnych. Dodatkowo inicjatywa Cybersecurity and Infrastructure Security Agency (CISA) wspiera sektor spożywczy poprzez analizy zagrożeń i rekomendacje dotyczące ochrony infrastruktury krytycznej[42].

W UE sektor rolno-spożywczy został zaliczony do sektorów krytycznych w ramach dyrektywy NIS2[43]. Dyrektywa nakłada obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych przez przedsiębiorstwa spożywcze w celu minimalizowania ryzyka cyberzagrożeń. Zgodnie z przewodnikiem dla branży spożywczej (Dyrektywa 2022/2555), producenci żywności są zobowiązani m.in. do przeprowadzania regularnych analiz ryzyka, opracowywania planów ciągłości działania, monitorowania zabezpieczeń u swoich dostawców, a także zgłaszania istotnych incydentów do odpowiednich organów w ciągu 24 godzin od ich wykrycia. Przedsiębiorstwa muszą również prowadzić rejestry działań związanych z cyberbezpieczeństwem, w tym dokumentować szkolenia i audyty[44]. Dodatkowo Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) opracowuje regularne raporty dotyczące zagrożeń w sektorze spożywczym i wytyczne dotyczące budowania odporności cybernetycznej w rolnictwie cyfrowym[45].

[41] U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)*, Washington 2011.

[42] CISA, *Cybersecurity Best Practices for the Food and Agriculture Sector*, Washington 2021.

[43] European Union, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2022.

[44] Dyrektywa 2022/2555, *Przewodnik dla branży spożywczej – Bezpieczeństwo żywności w praktyce*, Wydawnictwo Wiedza i Praktyka, Warszawa 2024.

[45] ENISA, *Threat Landscape for the Food Sector*, Luksemburg 2022.

W Japonii strategia „Society 5.0" obejmuje budowę bezpiecznego rolnictwa cyfrowego, a rząd finansuje programy wsparcia dla rolników wdrażających bezpieczne systemy IoT[46]. W Chinach rozwój „inteligentnego rolnictwa" jest powiązany z inwestycjami w systemy blockchain i AI zabezpieczające łańcuch dostaw żywności[47].

Przykłady udanych inicjatyw zabezpieczających łańcuch dostaw żywności.

Food Safety Modernization Act (USA). FSMA zmieniła podejście do bezpieczeństwa żywności z reaktywnego na proaktywne, nakładając obowiązek analiz zagrożeń i wdrażania planów prewencyjnych przez producentów i dystrybutorów[48]. W kontekście cyberzagrożeń oznacza to także konieczność oceny ryzyka w systemach cyfrowych.

IBM Food Trust to platforma blockchain umożliwiająca śledzenie produktów żywnościowych od producenta do konsumenta w sposób niezmienny i transparentny[49]. W projekt zaangażowane są takie firmy jak Walmart czy Nestlé, co znacząco poprawia bezpieczeństwo dostaw i szybkość reakcji na potencjalne zagrożenia.

Australian Food and Grocery Council – Cybersecurity Guidelines. Australia przyjęła w 2020 r. wytyczne dla przemysłu spożywczego dotyczące cyberbezpieczeństwa, obejmujące m.in. ochronę systemów SCADA oraz zarządzanie incydentami w łańcuchu dostaw[50].

Rekomendacje dla Polski i innych krajów w zakresie wzmacniania cyberbezpieczeństwa sektora żywnościowego:

- uwzględnienie sektora rolno-spożywczego w krajowych strategiach cyberbezpieczeństwa,
- obowiązkowe audyty cyberbezpieczeństwa dla dużych producentów i przetwórców żywności,
- wspieranie inwestycji w bezpieczne technologie cyfrowe w rolnictwie i logistyce,

[46] Cabinet Office Japan, *Society 5.0 Strategy: Outline and Implementation*, Tokio 2020.

[47] L. Zhou, Y. Zhang, W. Ma, *Smart agriculture: Cybersecurity issues and challenges*, International Journal of Agricultural Sustainability, 2022.

[48] U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)…,* op. cit.

[49] IBM, *IBM Food Trust: Blockchain for Food Transparency*, 2021.

[50] Australian Food and Grocery Council, *Cybersecurity Guidelines for the Food and Grocery Industry*, Canberra 2020.

- edukacja i szkolenia z zakresu cyberhigieny dla rolników, przetwórców i handlowców,
- tworzenie krajowych i regionalnych platform wymiany informacji o zagrożeniach.

Podsumowanie

Dzisiejszy łańcuch dostaw żywności, choć bardzo wydajny i oparty na globalnych powiązaniach, staje się coraz bardziej narażony na ataki cybernetyczne. Postępująca cyfryzacja – obejmująca m.in. Internet rzeczy, systemy SCM, automatyzację oraz blockchain – z jednej strony przyspiesza i porządkuje procesy, z drugiej jednak otwiera nowe ścieżki potencjalnych zagrożeń. Warto zaznaczyć, że technologie takie jak blockchain mogą zwiększać bezpieczeństwo danych i ograniczać możliwość fałszerstw, jednak nie stanowią pełnej ochrony przed zaawansowanymi formami cyberataków.

Analiza przeprowadzona w niniejszym rozdziale wskazuje na kilka istotnych wniosków:

- Kluczowe zagrożenia obejmują ataki ransomware, sabotaż infrastruktury krytycznej, manipulację danymi logistycznymi, przejęcie kontroli nad inteligentnymi systemami rolniczymi oraz kradzież danych.
- Wpływ cyberataków na sektor rolno-spożywczy jest wielowymiarowy: od strat finansowych i wzrostu cen żywności, poprzez destabilizację społeczną, aż po zagrożenia polityczne, środowiskowe i zdrowotne.
- Bezpieczeństwo cybernetyczne sektora żywnościowego stało się bezpośrednim elementem bezpieczeństwa wewnętrznego państwa. Utrata kontroli nad produkcją i dystrybucją żywności może prowadzić do utraty suwerenności gospodarczej i wzrostu podatności kraju na presję zewnętrzną.
- Odpowiednie strategie zabezpieczające obejmują wdrażanie międzynarodowych standardów bezpieczeństwa (ISO/IEC 27001, NIST), poprawę ochrony danych, współpracę publiczno-prywatną, programy edukacyjne dla pracowników sektora oraz wdrażanie technologii blockchain.
- Dobre praktyki międzynarodowe pokazują, że skuteczna prewencja wymaga zarówno regulacji prawnych, jak i inwestycji technologicznych oraz budowy świadomości zagrożeń na wszystkich poziomach łańcucha dostaw.

- Rekomendacje dla Polski i innych krajów obejmują stworzenie krajowych programów cyberodporności sektora rolno-spożywczego, obowiązkowe audyty bezpieczeństwa, oraz rozbudowę programów edukacyjnych dla rolników i przetwórców.

W obliczu rosnącego zagrożenia cyberatakami, państwa powinny traktować bezpieczeństwo żywnościowe nie tylko jako element polityki rolnej, lecz przede wszystkim jako fundament bezpieczeństwa narodowego. Rozwój technologii cyfrowych musi iść w parze z rozwojem narzędzi ochrony przed cyberzagrożeniami, aby zapewnić stabilność dostaw żywności i co za tym idzie – ochronę obywateli.

Potrzeba dalszych badań w tym obszarze jest pilna – szczególnie w zakresie oceny skuteczności nowych technologii ochronnych, tworzenia modeli predykcyjnych zagrożeń oraz strategii zarządzania ryzykiem cybernetycznym w sektorze żywnościowym.

Polska, podobnie jak inne kraje, powinna rozwijać zintegrowane strategie prewencji i edukacji. Przykładem dobrych praktyk regionalnych może być Alliance for a Green Revolution in Africa (AGRA), która od 2021 r. publikuje raporty *Food Security Monitor*, analizujące czynniki destabilizujące bezpieczeństwo żywnościowe, w tym także wybrane aspekty zagrożeń cyfrowych w państwach Afryki Subsaharyjskiej[51]. Na poziomie strategicznym podkreśla się również konieczność budowania odporności cybernetycznej jako integralnego elementu zapewniania bezpieczeństwa żywnościowego, co znajduje wyraz m.in. w opracowaniach Agricultural and Food Security Council[52].

Literatura

1. Agricultural and Food Security Council, *Ensuring Food Security through Cyber Resilience*, 2020.
2. Alliance for a Green Revolution in Africa (AGRA), *Food Security Monitor*, 2021.
3. Aung M. M., Chang Y. S., *Traceability in a food supply chain: Safety and quality perspectives*, „Food Control" nr 39, 172-184, 2014.
4. Australian Food and Grocery Council, *Cybersecurity Guidelines for the Food and Grocery Industry*, Canberra 2020.

[51] Alliance for a Green Revolution in Africa, *Food Security Monitor*, Nairobi 2021.

[52] Agricultural and Food Security Council, *Ensuring Food Security through Cyber Resilience*, 2020.

5. Barkin D., *Food Sovereignty: A Critical Dialogue*, „Globalizations" nr 16(7), 1047-1065, 2019.
6. Bodin L., Gordon L. A., *Cybersecurity Risk Management for Critical Infrastructure: A Food Supply Chain Perspective*, „Journal of Risk Research" nr 23(7-8), 1048-1060, 2020.
7. Boyes H., Hallaq B., Cunningham J., Watson T., *The Industrial Internet of Things (IIoT): An Analysis Framework*, „Computers in Industry" nr 101, 1-12, 2018.
8. Cabinet Office Japan, *Society 5.0 Strategy: Outline and Implementation*, Tokio 2020.
9. Casino F., Dasaklis T. K., Patsakis C., *A systematic literature review of blockchain-based applications: Current status, classification and open issues*, „Telematics and Informatics" nr 36, 55-81, 2019.
10. Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents*, Washington 2021.
11. CISA, *Cybersecurity Best Practices for the Food and Agriculture Sector*, Cybersecurity and Infrastructure Security Agency, Washington 2021.
12. Clapp J., *Food, Politics, and Society: Toward a Critical Research Agenda*, „Global Food Security" nr 28, art. 100476, 2021.
13. Clopton A., *Ransomware: Paralyzing Critical Infrastructure*, „Journal of Cybersecurity" nr 8(1), art. 1-14, 2022,
14. ENISA, *Threat Landscape for the Food Sector*, European Union Agency for Cybersecurity, 2022.
15. European Union, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2022.
16. FAO, *The State of Food Security and Nutrition in the World 2021*, Food and Agriculture Organization of the United Nations, Rzym 2021.
17. Food and Agriculture Organization of the United Nations (FAO), *Digital Technologies in Agriculture and Rural Areas*, 2020.
18. U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)*, Washington 2011.
19. Goik D., Ciupak M., *Dostawy żywności w systemie e-commerce – ich przyszłość i uwarunkowania*, „Problemy Drobnych Gospodarstw Rolnych" nr 2, 2018.
20. IBM, *IBM Food Trust: Blockchain for Food Transparency*, 2021.
21. International Federation of Red Cross and Red Crescent Societies (IFRC), *World Disasters Report 2021: Hunger and Food Insecurity*, Genewa 2021.
22. International Food Policy Research Institute (IFPRI), *Building Resilient Food Systems*, 2020.
23. ISO/IEC, *ISO/IEC 27001:2013 Information Security Management Systems – Requirements*, International Organization for Standardization, Genewa 2013.
24. Kosior K., *Potencjał technologii blockchain w zapewnianiu bezpieczeństwa i jakości żywności*, „Żywność. Nauka. Technologia. Jakość" nr 25(4), 2018.
25. Krotofil M., Gollmann D., *Industrial control systems security: What is happening?*, „Industrial Control Systems Security (ICSS) Workshop", 2013.
26. Kshetri N., *Blockchain's roles in strengthening cybersecurity and protecting privacy*, „Telecommunications Policy" nr 42(4), 1027-1038, 2017.

27. Laborde D., Martin W., Swinnen J., Vos R., *COVID-19 risks to global food security*, „Science" nr 369(6503), 2020.
28. Manheim D., *Cybersecurity and Agriculture: Threats and Impacts*, „Journal of Agricultural and Environmental Ethics" nr 31(4), 2018.
29. Min H., Zhou G., *Supply chain modeling: past, present and future*, „Computers & Industrial Engineering" nr 43(1-2), 2002.
30. Miremadi A., Moeini A., Ajirloo B., *IoT-Based Smart Agriculture: Cybersecurity Issues and Challenges*, „Journal of Ambient Intelligence and Humanized Computing", 2022.
31. Najwyższa Izba Kontroli, *System kontroli bezpieczeństwa żywności w Polsce – stan obecny i pożądane kierunki zmian*, Warszawa 2022.
32. National Academies of Sciences, Engineering and Medicine, *Science Breakthroughs to Advance Food and Agricultural Research by 2030*, Washington 2020.
33. Newman L. H., *Hackers Hit the World's Largest Meat Supplier With Ransomware*, „Wired Magazine", 2021.
34. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg 2018.
35. OECD, *Strengthening Agricultural Resilience in the Face of Multiple Risks*, Paris 2020.
36. SANS Institute, *Security Awareness Report: Managing Human Risk*, 2020.
37. Schneier B., *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (Updated Edition), W. W. Norton & Company, New York 2020.
38. Smith R., Young A., *Food safety vulnerabilities and cybersecurity risks*, „British Food Journal" nr 123(12), 2021.
39. Stallings W., *Cryptography and Network Security: Principles and Practice* (7 ed.), Pearson, Boston 2017.
40. Terlikowski T., *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów*, „Zeszyty Naukowe SGSP" nr 71(2), 2018.
41. Tian F., Li Z., Liu Y., *Food Supply Chain Digitalization: Opportunities and Challenges*, „Computers and Electronics in Agriculture" nr 186, art. 106184, 2021.
42. U.S. Department of Homeland Security, *CISA Insights: Mitigating Attacks Against Critical Infrastructure*, Washington 2021.
43. United Nations Office for Disaster Risk Reduction (UNDRR), *Global Assessment Report on Disaster Risk Reduction*, Genewa 2019.
44. Wolfert S., Ge L., Verdouw C., Bogaardt M. J., *Big Data in Smart Farming – A review*, „Agricultural Systems" nr 153, 2017.
45. World Economic Forum, *The Future of the Last-Mile Ecosystem*, Geneva 2020.
46. Zhang Y., Deng R., Weng J., *Smart farming cyber security: A review*, „Computers and Electronics in Agriculture" nr 140, 2017.
47. Zhou L., Zhang Y., Ma W., *Smart agriculture: Cybersecurity issues and challenges*, „International Journal of Agricultural Sustainability", 2022.