Marta Chodyka[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_23

MODEL ZARZĄDZANIA INCYDENTEM CYBERBEZPIECZEŃSTWA W ADMINISTRACJI ODPOWIEDZIALNEJ ZA OCHRONĘ GRANIC

A MODEL FOR MANAGING CYBERSECURITY INCIDENTS IN THE ADMINISTRATION RESPONSIBLE FOR BORDER PROTECTION

Streszczenie

Rozdział przedstawia model zarządzania incydentem cyberbezpieczeństwa w administracji odpowiedzialnej za ochronę granic. Punktem wyjścia jest założenie, że incydent w systemach granicznych nie jest wyłącznie zdarzeniem technicznym, lecz zdarzeniem wpływającym na ciągłość funkcji państwa: identyfikację osób, kontrolę przepływów, wymianę danych, komunikację kryzysową oraz zaufanie do decyzji administracyjnych. Problem badawczy dotyczy sposobu ujęcia procesu obsługi incydentu tak, aby obejmował jednocześnie wymiar techniczny, operacyjny, prawny i komunikacyjny. Celem opracowania jest zaproponowanie modelu interpretacyjno-aplikacyjnego, który łączy fazy reagowania na incydent z wymaganiami

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl

cyberodporności i ciągłości działania. Zastosowano analizę dokumentów prawnych, standardów i literatury oraz modelowanie koncepcyjne oparte na scenariuszu referencyjnym. Wyniki wskazują, że skuteczność reakcji zależy od jasnych progów eskalacji, wspólnego obrazu sytuacji, integracji ról, zdolności do pracy w stanie kontrolowanej degradacji oraz wykorzystania wniosków po incydencie do wzrostu dojrzałości organizacyjnej.

Słowa kluczowe: incydent cyberbezpieczeństwa, zarządzanie incydentem, administracja publiczna, ochrona granic, cyberodporność, ciągłość działania

Abstract

The chapter presents a model for managing a cybersecurity incident in public administration responsible for border protection. It assumes that an incident in border-management systems is not merely a technical event, but one that affects the continuity of state functions: identity verification, control of flows, data exchange, crisis communication, and trust in administrative decisions. The research problem concerns how to frame incident handling to cover the technical, operational, legal, and communication dimensions simultaneously. The aim of the study is to propose an interpretative and application-oriented model that integrates incident response phases with the requirements of cyber resilience and business continuity. The study applies legal document analysis, standards and literature review, and conceptual model design based on a reference scenario. The findings indicate that an effective response depends on clear escalation thresholds, a common operational picture, role integration, the ability to operate in a controlled-degraded mode, and the use of post-incident lessons to increase organisational maturity.

Keywords: cybersecurity incident, incident management, public administration, border protection, cyber resilience, business continuity

Wstęp

Administracja odpowiedzialna za ochronę granic funkcjonuje w środowisku, w którym incydent cyberbezpieczeństwa może szybko uzyskać znaczenie wykraczające poza obszar teleinformatyczny. Zakłócenie systemu odpraw, bazy danych, kanału łączności, systemu identyfikacji albo komunikacji publicznej może wpływać na zdolność państwa do wykonywania funkcji granicznej. W tym sensie incydent nie jest jedynie problemem administratora systemu, lecz zdarzeniem administracyjnym i operacyjnym, które wymaga decyzji kierowniczych, prawnych, organizacyjnych i komunikacyjnych. Podstawowy kontekst instytucjonalny wyznaczają przepisy

krajowego systemu cyberbezpieczeństwa oraz regulacje unijne dotyczące zarządzania ryzykiem, raportowania incydentów i współpracy między podmiotami (Kancelaria Sejmu, 2018). Dyrektywa NIS 2 wzmacnia podejście oparte na zarządzaniu ryzykiem, odpowiedzialności kierownictwa, ciągłości działania i współpracy transgranicznej (Dyrektywa (UE) 2022/2555, 2022). W administracji granicznej wymagania te powinny być interpretowane przez pryzmat funkcji publicznej, ponieważ skutki incydentu mogą dotyczyć nie tylko dostępności systemu, ale także legalności decyzji, integralności danych, bezpieczeństwa personelu i zaufania do instytucji.

Problem badawczy opracowania można sformułować następująco: jaki model zarządzania incydentem cyberbezpieczeństwa odpowiada potrzebom administracji odpowiedzialnej za ochronę granic, jeżeli incydent wpływa jednocześnie na systemy teleinformatyczne, procesy operacyjne, przepływ informacji, komunikację i ciągłość funkcji państwa? Problem ten ma charakter teoretyczno-aplikacyjny. Teoretycznie dotyczy relacji między cyberbezpieczeństwem, cyberodpornością, zarządzaniem kryzysowym i bezpieczeństwem państwa (Kitler, 2011; Wiśniewski, 2013). Aplikacyjnie wymaga określenia ról, progów eskalacji, przepływów informacji, trybów pracy awaryjnej i mechanizmów uczenia się po incydencie. Celem naukowym jest opracowanie modelu zarządzania incydentem, który łączy klasyczne fazy obsługi incydentu z wymaganiami administracji publicznej i specyfiką systemów granicznych. Celem szczegółowym jest wskazanie, jak w jednym modelu powiązać detekcję techniczną, kwalifikację wpływu na funkcję graniczną, decyzję o eskalacji, utrzymanie procesu w stanie ograniczonej sprawności, odtworzenie usług i analizę po incydencie. Celem praktycznym jest zaproponowanie ram, które mogą zostać wykorzystane przy tworzeniu planów reagowania, playbooków, ćwiczeń, audytów i szkoleń. Metodologia ma charakter jakościowy i diagnostyczno-projektowy. Wykorzystano analizę dokumentów prawnych, standardów i literatury, a następnie modelowanie koncepcyjne. Analiza dokumentów jest zasadna, ponieważ badany problem obejmuje źródła o różnym statusie: akty prawne, standardy, raporty instytucjonalne, publikacje naukowe i opracowania metodyczne (Bowen, 2009; Mayring, 2000). Modelowanie pozwala przekształcić wymagania formalne i ustalenia literatury w uporządkowaną procedurę zarządzania incydentem. W badaniu przyjęto także scenariusz referencyjny: zakłócenie dostępności

systemu wspierającego odprawę, połączone z fałszywą informacją o zamknięciu przejścia oraz koniecznością pracy w trybie awaryjnym. Taki scenariusz łączy wymiar techniczny, operacyjny, prawny i komunikacyjny. Dobór źródeł podporządkowano trzem kryteriom. Uwzględniono literaturę z zakresu bezpieczeństwa państwa i funkcjonowania instytucji publicznych (Żurawski i in., 2025). Wykorzystano standardy dotyczące reagowania na incydenty, cyberodporności i ciągłości działania (Nelson i in., 2025). Dodatkowo włączono publikacje dotyczące bezpieczeństwa danych, zarządzania incydentami, systemów bezpieczeństwa w organizacjach publicznych oraz sprawności działania w warunkach kryzysowych (Chodyka, 2025; Wołejszo i in., 2021; Żurawski i in., 2025).

Incydent cyberbezpieczeństwa jako zdarzenie administracyjne i operacyjne

W klasycznym ujęciu cyberbezpieczeństwa ochronę informacji opisuje się przez pryzmat poufności, integralności i dostępności. W systemach granicznych znaczenie tych kategorii należy interpretować w związku z funkcją publiczną. Naruszenie poufności może oznaczać ujawnienie danych osobowych, dokumentowych lub biometrycznych. Naruszenie integralności może prowadzić do decyzji podjętych na podstawie danych błędnych, niepełnych albo zmanipulowanych (Chodyka, Dalba-Gołaszewska, 2025). Naruszenie dostępności może skutkować opóźnieniem odprawy, wzrostem kolejek, koniecznością pracy manualnej i zwiększeniem ryzyka błędu operacyjnego (Ciekanowski, Wojciechowska-Filipek, 2019).

Incydent cyberbezpieczeństwa w administracji granicznej powinien być zatem kwalifikowany nie tylko według typu technicznego, ale przede wszystkim według wpływu na funkcję graniczną. Ten sam problem techniczny może mieć różne skutki w zależności od natężenia ruchu, miejsca wystąpienia, dostępności procedur zastępczych, znaczenia przetwarzanych danych oraz stopnia zależności od systemów zewnętrznych. Krótkotrwała niedostępność aplikacji pomocniczej może pozostać zdarzeniem technicznym, natomiast krótkotrwała niedostępność systemu referencyjnego w godzinach szczytu może wymagać decyzji operacyjnej i komunikacyjnej. NIST SP 800-61 Rev. 3 ujmuje reagowanie na incydenty jako element szerszego zarządzania ryzykiem cyberbezpieczeństwa i wiąże je z funkcjami NIST

Cybersecurity Framework 2.0 (Nelson i in., 2025; NIST, 2024). To przesunięcie jest istotne dla administracji publicznej, ponieważ obsługa incydentu nie może być izolowana od zarządzania ryzykiem, odpowiedzialności kierownictwa, komunikacji i odtwarzania funkcji. Z perspektywy systemów granicznych szczególne znaczenie ma powiązanie reagowania i odtwarzania z funkcją zarządzania, ponieważ bez jasnych ról decyzyjnych można przywrócić komponent techniczny, ale nie odtworzyć procesu operacyjnego.

Incydent w systemie granicznym ma co najmniej cztery wymiary. Wymiar techniczny dotyczy systemów, sieci, kont, logów, konfiguracji, danych i dostępności usług. Wymiar operacyjny obejmuje odprawę, kontrolę, kolejki, bezpieczeństwo personelu i decyzje o trybie pracy. Wymiar prawny dotyczy ochrony danych, zabezpieczenia dowodów, obowiązków raportowych i zgodności działań z procedurami. Wymiar komunikacyjny obejmuje informowanie personelu, podróżnych, partnerów instytucjonalnych oraz reagowanie na dezinformację (Ciekanowski i in., 2025). Dopiero łączna ocena tych wymiarów pozwala ustalić rzeczywisty poziom incydentu. Z tego względu zasadne jest wyróżnienie kilku poziomów wpływu. Poziom monitorowania obejmuje zdarzenia techniczne bez istotnego wpływu na funkcję graniczną. Poziom operacyjny dotyczy zdarzeń ograniczających sprawność procesu, na przykład wydłużających odprawę lub wymagających pracy w trybie zastępczym. Poziom prawny pojawia się wtedy, gdy istnieje podejrzenie naruszenia danych lub konieczność zabezpieczenia materiału dowodowego. Poziom informacyjny dotyczy sytuacji, w których incydentowi towarzyszy dezinformacja, presja medialna albo rozbieżność komunikatów. Poziom krytyczny występuje wtedy, gdy zakłócona zostaje podstawowa zdolność realizacji funkcji granicznej. Takie ujęcie jest spójne z prakseologicznym rozumieniem sprawności działania w organizacjach odpowiedzialnych za bezpieczeństwo. W warunkach kryzysu istotne jest nie tylko posiadanie zasobów, lecz także zdolność ich skoordynowanego użycia, utrzymania kontroli nad procesem i podejmowania decyzji przy niepełnej informacji (Wołejszo, Feltynowski, 2023; Wołejszo i in., 2021). W administracji granicznej oznacza to konieczność projektowania reakcji nie jako sekwencji czynności technicznych, lecz jako procesu dowodzenia, koordynacji i utrzymania funkcji publicznej.

Model zarządzania incydentem w administracji odpowiedzialnej za ochronę granic

Proponowany model ma charakter fazowy i funkcjonalny. Fazy porządkują przebieg reakcji, natomiast funkcjonalność modelu wynika z odniesienia każdej fazy do utrzymania zadania publicznego. Model obejmuje osiem faz: przygotowanie, wykrycie, kwalifikację, eskalację, ograniczenie skutków, utrzymanie funkcji, odtwarzanie oraz uczenie się. Fazy te nie zawsze występują liniowo. W praktyce część działań może przebiegać równolegle, szczególnie wtedy, gdy zespół techniczny izoluje incydent, pion operacyjny uruchamia tryb ograniczony, a komórka komunikacyjna przygotowuje komunikat etapowy. Przygotowanie obejmuje wskazanie ról, list kontaktowych, kanałów zapasowych, playbooków, procedur pracy awaryjnej, zasad komunikacji i scenariuszy ćwiczeń. Bez tej fazy pozostałe etapy stają się improwizacją. Wykrycie powinno obejmować zarówno sygnały techniczne, jak i sygnały operacyjne z terenu. Alert z systemu monitoringu ma inne znaczenie, jeżeli równocześnie rośnie kolejka, pojawia się niespójność danych albo w przestrzeni informacyjnej rozpowszechniany jest fałszywy komunikat. Kwalifikacja polega na ocenie wpływu zdarzenia na funkcję graniczną. Nie wystarcza ustalenie, czy wystąpił atak, awaria lub błąd konfiguracji. Konieczne jest ustalenie, czy zdarzenie wpływa na identyfikację osób, weryfikację dokumentów, wymianę informacji, dostępność danych referencyjnych, bezpieczeństwo personelu, ochronę danych albo komunikację publiczną. Eskalacja powinna wynikać z wcześniej ustalonych progów, a nie z uznaniowej oceny pojedynczej osoby. Progi mogą dotyczyć czasu niedostępności, liczby dotkniętych stanowisk, podejrzenia naruszenia danych, konieczności przejścia na tryb manualny, ryzyka dezinformacji albo potrzeby powiadomienia CSIRT i kierownictwa.

Ograniczenie skutków obejmuje działania techniczne i organizacyjne. Do działań technicznych należą między innymi izolacja segmentu, blokada kont, zabezpieczenie logów, przełączenie usług i ograniczenie propagacji zakłócenia. Do działań organizacyjnych należy zmiana organizacji ruchu, uruchomienie procedury manualnej, wzmocnienie obsady, przekazanie instrukcji personelowi, przygotowanie komunikatu oraz ustalenie zasad dokumentowania decyzji. Faza utrzymania funkcji jest szczególnie ważna z perspektywy cyberodporności. Celem nie jest natychmiastowy powrót do

pełnej automatyzacji, lecz bezpieczne utrzymanie minimalnej funkcji na akceptowalnym poziomie (ISO, 2019). Odtwarzanie obejmuje przywrócenie usług, weryfikację integralności danych, synchronizację rekordów powstałych w trybie awaryjnym, analizę logów, potwierdzenie bezpieczeństwa środowiska i decyzję o powrocie do normalnego trybu pracy. Działania po incydencie powinny obejmować raport, przegląd decyzji, identyfikację luk, aktualizację procedur, korektę konfiguracji, wnioski szkoleniowe oraz ocenę relacji z dostawcami. NIST SP 800-184 podkreśla, że odzyskiwanie po zdarzeniu wymaga nie tylko odtworzenia usług, lecz także walidacji i komunikacji (Bartock i in., 2016). Fazy modelu przedstawiono w Tabeli 1. Model wymaga również jednoznacznego przypisania ról. Rola techniczna odpowiada za analizę systemów, logów, konfiguracji i zabezpieczeń. Rola operacyjna odpowiada za wpływ incydentu na odprawę, decyzje w terenie i organizację pracy. Rola prawna odpowiada za ochronę danych, obowiązki raportowe, zabezpieczenie dowodów i zgodność działań. Rola komunikacyjna odpowiada za przekaz do personelu, podróżnych, mediów i partnerów. Rola kierownicza odpowiada za priorytety, akceptację ryzyka resztkowego, przejście między trybami pracy i decyzję o powrocie do normalnego działania. Przepływ informacji powinien być dwukierunkowy. Zespół techniczny przekazuje informacje o naturze zdarzenia, ale pion operacyjny informuje o rzeczywistym wpływie na proces graniczny. Komunikacja publiczna raportuje sygnały z otoczenia informacyjnego, a prawnicy określają ograniczenia publikacji, raportowania i przetwarzania danych. Bez takiego przepływu decyzje mogą być podejmowane na podstawie niepełnego obrazu sytuacji. Dlatego model powinien opierać się na jednej karcie incydentu, aktualizowanej w czasie i obejmującej status techniczny, wpływ operacyjny, decyzje, komunikaty, ryzyka prawne i kolejne kroki.

Progi eskalacji i tryby pracy są elementami łączącymi model z praktyką. Tryb normalny oznacza pełną funkcjonalność systemów. Tryb podwyższonej czujności oznacza zwiększony monitoring i gotowość zespołów. Tryb degradacji kontrolowanej oznacza ograniczenie automatyzacji i uruchomienie procedur zastępczych przy zachowaniu rozliczalności decyzji. Tryb krytyczny oznacza minimalny zakres funkcji oraz priorytet bezpieczeństwa osób, danych i procesu. Takie tryby powinny być opisane przed incydentem, ponieważ w warunkach presji czasu trudniej uzgadniać kryteria działania.

Tabela 1. Fazy modelu zarządzania incydentem cyberbezpieczeństwa w administracji granicznej

Faza	Cel	Decyzja kluczowa	Dowód wykonania
Przygotowanie	zapewnienie gotowości ról, procedur, kanałów i playbooków	zatwierdzenie planu reagowania i trybów pracy	aktualny plan, lista kontaktowa, scenariusze ćwiczeń
Wykrycie	rozpoznanie anomalii technicznej lub operacyjnej	czy zdarzenie wymaga kwalifikacji jako incydent	alert, zgłoszenie, zapis w rejestrze zdarzeń
Kwalifikacja	ocena wpływu na funkcję graniczną i dane	poziom incydentu i zakres oddziaływania	wstępny obraz sytuacji, ocena skutków
Eskalacja	uruchomienie właściwych ról i podmiotów	kogo powiadomić i kto podejmuje decyzję	lista powiadomień, decyzja kierownicza
Ograniczenie skutków	zatrzymanie propagacji zakłócenia i zabezpieczenie dowodów	co izolować, co utrzymać, co wyłączyć	logi, decyzje techniczne, zapis działań
Utrzymanie funkcji	zapewnienie minimalnej zdolności odprawy i komunikacji	tryb degradacji kontrolowanej albo tryb krytyczny	karta incydentu, instrukcje dla personelu
Odtwarzanie	przywrócenie usług i integralności procesu	czy system może wrócić do pracy normalnej	raport odtworzeniowy, walidacja danych
Uczenie się	zwiększenie dojrzałości organizacyjnej po zdarzeniu	jakie procedury, umowy i szkolenia zmienić	raport poincydentowy, plan działań korygujących

Źródło: opracowanie własne.

Znaczenie progów eskalacji wzmacniają regulacje unijne dotyczące poważnych zagrożeń i incydentów. Akt w sprawie cybersolidarności rozwija unijne podejście do wykrywania, przygotowania i reagowania na zagrożenia cybernetyczne i incydenty, co potwierdza, że zarządzanie incydentem nie jest wyłącznie sprawą wewnętrzną pojedynczej jednostki (Rozporządzenie (UE) 2025/38, 2025). W systemach granicznych ma to szczególne znaczenie, ponieważ zakłócenie lokalne może wpływać na współpracę z partnerami, wymianę danych i zaufanie do procesu transgranicznego.

Wyniki analizy i zastosowanie modelu

Przeprowadzona analiza prowadzi do pięciu zasadniczych wyników. Po pierwsze, zarządzanie incydentem w administracji granicznej wymaga połączenia modelu technicznego i modelu misji. Samo przywrócenie aplikacji, serwera lub łączności nie oznacza jeszcze przywrócenia funkcji granicznej.

Konieczne jest odtworzenie danych, kolejki operacyjnej, komunikacji, ścieżki audytu i zdolności do uzasadnienia decyzji podjętych w czasie zakłócenia. Po drugie, skuteczna reakcja wymaga wspólnego obrazu sytuacji. W incydencie granicznym informacje pochodzą z wielu źródeł: logów, stanowisk odpraw, zgłoszeń personelu, komunikacji publicznej, dostawców, partnerów zewnętrznych i mediów. Jeżeli każda komórka organizacyjna posiada własną wersję zdarzenia, rośnie ryzyko opóźnienia, sprzecznych decyzji i niespójnych komunikatów. Ćwiczenia Cyber Europe wskazują, że koordynacja i wspólny obraz sytuacji są kluczowe dla gotowości i odporności cyberbezpieczeństwa (ENISA, 2024). Po trzecie, centralnym elementem modelu jest praca w stanie degradacji kontrolowanej. Cyberodporność nie polega na założeniu, że wszystkie systemy będą zawsze dostępne. Polega na tym, że instytucja wie, które funkcje utrzymać, jakie dane są minimalnie niezbędne, kiedy przejść na tryb manualny lub częściowo manualny, jak dokumentować decyzje i jak później zsynchronizować zaległe dane. W tym sensie odporność jest zdolnością operacyjną, a nie wyłącznie stanem infrastruktury. Po czwarte, szczególnego znaczenia nabiera integralność danych i rozliczalność procesu. Decyzja podjęta na podstawie danych błędnych, niepełnych lub niespójnych może być formalnie zgodna z procedurą, a jednocześnie wadliwa z punktu widzenia funkcji bezpieczeństwa. Dlatego plan reagowania powinien obejmować walidację danych, zabezpieczenie logów, odtworzenie ścieżki decyzji, kontrolę wpisów dokonanych w trybie offline i mechanizmy ponownej weryfikacji spraw po przywróceniu systemu. Po piąte, działania po incydencie powinny prowadzić do wzrostu dojrzałości organizacyjnej. Raport poincydentowy nie może być wyłącznie dokumentem zamykającym sprawę. Powinien wskazywać, które decyzje były spóźnione, jakie dane były niedostępne, które role były niejasne, jakie umowy z dostawcami wymagają doprecyzowania i które scenariusze ćwiczeń należy zmienić. Badania nad skutecznością systemów zarządzania incydentami bezpieczeństwa informacji wskazują, że efektywność reakcji zależy nie tylko od technologii, lecz także od automatyzacji, kompetencji, skrócenia czasu detekcji i reakcji oraz integracji zarządzania incydentami ze strategią bezpieczeństwa.

Model może być zastosowany w planach reagowania na incydenty. Plan powinien obejmować role, listę kontaktową, progi eskalacji, tryby pracy, zasady komunikacji wewnętrznej i zewnętrznej, procedury zabezpieczenia

dowodów, kryteria przejścia na tryb awaryjny oraz kryteria powrotu do normalnego działania. Nie powinien być dokumentem wyłącznie formalnym. Jego użyteczność zależy od tego, czy może zostać wykorzystany w pierwszych minutach incydentu, kiedy informacje są niepełne, a presja operacyjna rośnie. Drugim zastosowaniem są playbooki scenariuszowe. W administracji granicznej powinny one obejmować co najmniej niedostępność systemu odpraw, podejrzenie naruszenia danych, niespójność danych referencyjnych, fałszywy komunikat w mediach społecznościowych, awarię dostawcy oraz konieczność pracy w trybie manualnym. Każdy playbook powinien wskazywać pierwsze działania, role, kanały komunikacji, decyzje progowe, minimalne dane, zasady dokumentowania i kryteria zakończenia. Trzecim zastosowaniem są ćwiczenia. Ćwiczenie typu tabletop pozwala sprawdzić role, decyzje i progi eskalacji. Ćwiczenie techniczne pozwala sprawdzić logi, kopie, izolację i odtwarzanie. Ćwiczenie zintegrowane łączy oba wymiary i jest najbardziej użyteczne, ponieważ ujawnia problemy na styku zespołów. Scenariusz nie powinien ograniczać się do ogólnego hasła o cyberataku. Powinien opisywać sekwencję zdarzeń: opóźnienia w odprawie, alert z monitoringu, zgłoszenia funkcjonariuszy, fałszywy komunikat, pytania mediów, decyzję o trybie manualnym i synchronizację danych po odtworzeniu systemu. Czwartym zastosowaniem jest audyt dojrzałości. Instytucja może ocenić, czy posiada aktualne playbooki, czy zna zależności od dostawców, czy ma kanały zapasowe, czy personel zna procedurę zgłoszenia, czy potrafi odtworzyć dane po pracy offline i czy wyniki ćwiczeń prowadzą do korekty planów. Badania dotyczące systemów zarządzania bezpieczeństwem w organizacjach publicznych wskazują, że wyższa dojrzałość systemu zarządzania wiąże się z lepszą zdolnością reagowania i większą odpornością organizacyjną (Chodyka i in., 2026). Piątym zastosowaniem są szkolenia i komunikacja wewnętrzna. Personel operacyjny powinien wiedzieć, jak rozpoznać objawy incydentu, kiedy eskalować problem, jak pracować w trybie ograniczonym i jak dokumentować decyzje. Personel techniczny powinien rozumieć skutki operacyjne swoich działań, na przykład izolacji komponentu lub wyłączenia usługi. Kierownictwo powinno być przygotowane do podejmowania decyzji przy niepełnej informacji. Komórka komunikacyjna powinna dysponować komunikatami etapowymi, które informują o ograniczeniach, nie ujawniają szczegółów wrażliwych i ograniczają ryzyko dezinformacji.

Szóstym zastosowaniem jest zarządzanie relacjami z dostawcami. Umowy powinny określać czasy reakcji, tryb wsparcia podczas incydentu, obowiązek informowania o podatnościach, dostęp do logów, udział w ćwiczeniach, procedury odtworzeniowe i zasady współpracy w sytuacji awaryjnej. W systemach granicznych dostawca nie jest wyłącznie podmiotem serwisowym. W czasie incydentu staje się elementem łańcucha reakcji i może wpływać na zdolność utrzymania funkcji publicznej. Znaczenie bezpieczeństwa infrastruktury krytycznej i zależności międzysektorowych potwierdzają także analizy dotyczące zarządzania bezpieczeństwem w warunkach rosnących cyberzagrożeń (Chodyka i in., 2025).

Model może być wdrażany przez minimalny pakiet operacyjny obejmujący kartę incydentu, matrycę eskalacji, listę kontaktową, playbooki scenariuszowe i formularz wniosków po incydencie. Dokumenty te powinny być krótkie, aktualne, dostępne offline i testowane w ćwiczeniach. Ich celem nie jest zwiększenie biurokracji, lecz zapewnienie podstawy do szybkiej, rozliczalnej i skoordynowanej decyzji. Ocena modelu powinna obejmować zarówno metryki ilościowe, jak i jakościowe. Użyteczne są wskaźniki czasu wykrycia, czasu kwalifikacji, czasu eskalacji, czasu przejścia na tryb awaryjny, czasu odtworzenia funkcji oraz liczby decyzji wymagających korekty. Nie powinny one jednak zastępować oceny jakości decyzji. Szybkość reakcji nie zawsze oznacza adekwatność. Decyzja powinna być terminowa, udokumentowana, proporcjonalna, zgodna z procedurą i ukierunkowana na utrzymanie funkcji państwa.

Wnioski z raportów krajowych i europejskich potwierdzają, że zarządzanie incydentami wymaga nie tylko narzędzi technicznych, lecz także zdolności organizacyjnych, współpracy, świadomości zagrożeń i gotowości do działania w warunkach presji (CERT Polska, 2026). W administracji granicznej oznacza to konieczność traktowania zarządzania incydentem jako część polityki cyberodporności, a nie wyłącznie jako procedury technicznej.

Wnioski

Incydent cyberbezpieczeństwa w administracji odpowiedzialnej za ochronę granic jest zdarzeniem wielowymiarowym. Jego obsługa wymaga integracji zespołów technicznych, operacyjnych, prawnych, komunikacyjnych i kierowniczych. Brak tej integracji zwiększa ryzyko opóźnienia,

niespójności działań, błędów decyzyjnych oraz utraty zaufania do procesu. Zaproponowany model ośmiu faz pozwala połączyć obsługę incydentu z wymaganiami cyberodporności i ciągłości działania. Najważniejszym elementem modelu jest utrzymanie funkcji granicznej w stanie kontrolowanej degradacji. Oznacza to zdolność do pracy przy ograniczonej dostępności systemów, zachowania minimalnych danych, dokumentowania decyzji i późniejszego odtworzenia integralności procesu.

Model ma zastosowanie w planach reagowania, playbookach, ćwiczeniach, audytach dojrzałości, szkoleniach i zarządzaniu relacjami z dostawcami. Jego wartość polega na tym, że przenosi zarządzanie incydentem z poziomu reakcji technicznej na poziom funkcji państwa. W praktyce oznacza to, że skuteczność reakcji powinna być oceniana nie tylko przez czas usunięcia awarii, ale także przez zdolność utrzymania odprawy, ochrony danych, komunikacji i rozliczalności decyzji. Zaproponowany model ma charakter interpretacyjno-aplikacyjny. Nie zastępuje audytu konkretnej architektury systemowej ani oceny procedur wdrożonych w poszczególnych jednostkach organizacyjnych, lecz wyznacza ramy takiej analizy. Dalsze badania powinny obejmować walidację modelu przez studia przypadków, wywiady eksperckie, ćwiczenia typu tabletop i cyber range, analizę danych incydentowych oraz pomiar skuteczności trybów pracy awaryjnej w różnych typach punktów granicznych. Szczególnie istotne będzie ustalenie, w jakim stopniu model pozwala identyfikować luki odpowiedzialności, zależności krytyczne, słabe punkty komunikacji oraz ryzyka wynikające z pracy na danych niepełnych lub niespójnych.

Literatura

1. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K. (2016). *Guide for cybersecurity event recovery (NIST SP 800-184).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184
2. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027
3. CERT Polska. (2026). *Raport roczny z działalności CERT Polska w 2025 roku*. NASK – Państwowy Instytut Badawczy.

4. Chodyka, M. (2025). Bezpieczeństwo baz danych jako element odporności cybernetycznej Sił Zbrojnych. W D. Brążkiewicz, M. Chodyka, T. Grudniewski, J. Nowicka (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część 1* (s. 123-140). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103199_7
5. Chodyka, M., Dalba-Gołaszewska, A. (2025). Database security in the face of contemporary threats. Przegląd Naukowo-Metodyczny. *Edukacja dla Bezpieczeństwa, 18*(4/69), 29-44.
6. Chodyka, M., Wojciechowska-Filipek, S., Ciekanowski, Z., Chrząszcz, A. E., Żurawski, S. (2026). The effectiveness of security management systems in public organizations: A cybersecurity perspective. *European Research Studies Journal, 29*(1), 478-489. https://doi.org/10.35808/ersj/4323
7. Chodyka, M., Żurawski, S., Wojciechowska-Filipek, S., Ciekanowski, Z., Mazur, S. (2025). Critical infrastructure security management in the era of cyber threats. *European Research Studies Journal, 28*(2), 610-621. https://doi.org/10.35808/ersj/4000
8. Ciekanowski, M., Chodyka, M., Żurawski, S., Parczewska, W. (2025). Bezpieczeństwo teleinformatyczne w zarządzaniu kryzysowym. W: D. Brążkiewicz, M. Chodyka, T. Grudniewski, S. Żurawski (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część 2* (s. 159-174). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103205_8
9. Ciekanowski, Z., Wojciechowska-Filipek, S. (2019). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: Jednostki – organizacji – państwa*. CeDeWu.
10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. (2022). Dz.Urz. UE L 333 z 27.12.2022, s. 80-152.
11. ENISA. (2024). *Cyber Europe 2024: After Action Report. European Union Agency for Cybersecurity*. Pobrane z: https://www.enisa.europa.eu/publications/cyber-europe-2024-after-action-report
12. ISO. (2019). *ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements*. International Organization for Standardization.

13. Kitler, W. (2011). *Bezpieczeństwo narodowe RP: Podstawowe kategorie, uwarunkowania, system*. Akademia Obrony Narodowej.
14. Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung Forum: Qualitative Social Research, 1*(2). https://doi.org/10.17169/fqs-1.2.1089
15. NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
16. Nelson, A., Rekhi, S., Souppaya, M., Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
17. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694. (2025). Dz.Urz. UE L 2025/38 z 15.01.2025.
18. Kancelaria Sejmu. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (t.j. Dz. U. z 2026 r. poz. 20, 252 z późn. zm.).
19. Wiśniewski, B. (2013). *System bezpieczeństwa państwa: Konteksty teoretyczne i praktyczne*. Wydawnictwo WSPol.
20. Wołejszo, J., Feltynowski, M. (2023). Efficiency of the control and command system in crisis management. *Polish Political Science Yearbook, 52*(3), 85-100. https://doi.org/10.15804/ppsy202381
21. Wołejszo, J., Malasiewicz, K., Prusiński, N. (red.). (2021). *Prakseologia w naukach o bezpieczeństwie: Sprawność działania w zarządzaniu kryzysowym*. Wydawnictwo Naukowe Akademii Kaliskiej im. Prezydenta Stanisława Wojciechowskiego.
22. Żurawski, S., Chrząszcz, A. E., Ciekanowski, Z., Pauliuchuk, Y., Pietrzyk, S., Wyrzykowska, B. (2025). Effectiveness of information security incident management systems: Identifying practices, challenges and development perspectives. *European Research Studies Journal, 28*(1), 575-588. https://doi.org/10.35808/ersj/3922