Kom. dr inż. Andrzej MACHNACZ
Komenda Główna Policji

METODY ROZPOZNAWANIA, WYZNACZANIA I PROJEKTOWANIA INFRASTRUKTURY KRYTYCZNEJ NA POTRZEBY OCHRONY LUDNOŚCI ORAZ ZAPEWNIENIA FUNKCJONOWANIA ORGANÓW ADMINISTRACJI

Streszczenie: W treści artykułu przedstawiono metodę wyznaczania elementów infrastruktury krytycznej, w tym definiowania środków zabezpieczeń i projektowania architektury rozwiązań w sposób zapewniający jej ochronę przed zagrożeniami. Omówiono kryteria i przykładowe progi pozwalające na identyfikowanie składowych infrastruktury krytycznej poprzez określenie rozmiaru strat wynikłych z ich zakłócenia lub zniszczenia.
Słowa kluczowe: infrastruktura krytyczna, zarządzanie kryzysowe, bezpieczeństwo organów administracji.

1. Wprowadzenie

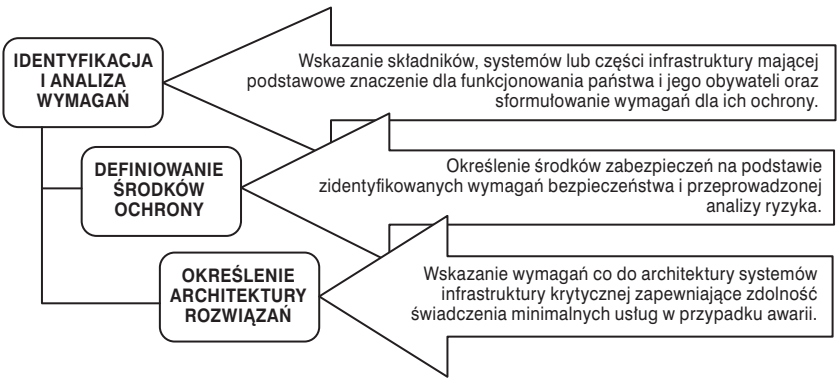
Rozwój cywilizacji, w tym intensywne zmiany technologiczne spowodowały, że utrzymanie niezbędnych funkcji społecznych, takich jak: zdrowie, bezpieczeństwo, ochrona, dobrobyt materialny lub społeczny ludności stało się zadaniem niezwykle trudnym. Niełatwo byłoby obecnie funkcjonować bez sprawnie działających systemów zaopatrzenia w energię, wodę i żywność, systemów łączności i sieci teleinformatycznych, systemów finansowych i transportowych, czy też ratowniczych i produkujących substancje chemiczne. Z punktu widzenia funkcjonowania państwa i życia obywateli naruszenie ciągłości działania administracji publicznej mogłoby wywołać destabilizację funkcjonowania jej organów. Wszystkie te elementy wpływają na bezpieczeństwo państwa i jego obywateli, w tym na skuteczność funkcjonowania organów władzy i administracji publicznej oraz instytucji i przedsiębiorców, przez co wchodzą w skład tzw. infrastruktury krytycznej, której ochrona powinna być jednym z podstawowych priorytetów każdego z państw[1]. Infrastruktura ta jest stosunkowo złożona i funkcjonalnie zależna, a jej prawidłowe działanie jest możliwe wyłącznie dzięki współdziałaniu wielu podmiotów sektora prywatnego i insty-

[1] A. Tyburska (red.), *Ochrona infrastruktury krytycznej*, WSPol Szczytno, 2010.

tucji administracji publicznej na rzecz przeciwdziałania zagrożeniom jej zniszczenia, uszkodzenia bądź zakłócenia funkcjonowania.

Z uwagi na wysokie koszty zabezpieczenia wszystkich obszarów związanych z funkcjonowaniem państwa i jego obywateli, niezwykle ważne jest właściwe rozpoznawanie, wyznaczanie i projektowanie infrastruktury krytycznej poprzez identyfikowanie poszczególnych elementów wchodzących w jej skład i analizę wymagań dotyczących ich ochrony, a także definiowanie środków zabezpieczeń oraz określanie architektury rozwiązań minimalizujących ryzyko utraty jej integralności.

Obszary wchodzące w skład infrastruktury krytycznej określono w art. 3 Ustawy[2]. Jednocześnie nie wskazano listy konkretnych użytkowanych systemów oraz wchodzących w ich skład powiązanych ze sobą funkcjonalnie obiektów, w tym urządzeń, instalacji, usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Wynika to z dynamicznego charakteru usług i związanych z nimi systemów, które mogą tworzyć tą infrastrukturę, a także z faktu, że lista elementów wchodzących w jej skład, jak i szczegółowe kryteria oraz przyjęte progi wyznaczania jej elementów należą do grupy szczególnie chronionych informacji, które w przypadku ujawnienia mogłyby zostać wykorzystane do zaplanowania i przeprowadzenia działań zmierzających do spowodowania zakłócenia lub zniszczenia urządzeń infrastruktury krytycznej.



Rys. 1. Etapy identyfikacji infrastruktury krytycznej i określania środków bezpieczeństwa.

[2] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. 2007, Nr 89, poz. 590 z późn. zm.).

W dalszej części opracowania przedstawiono propozycję rozpoznawania, wyznaczania i projektowania infrastruktury krytycznej poprzez określenie kryteriów i progów kwalifikowania do niej systemów oraz zdefiniowanie związanymi z nimi wymagań bezpieczeństwa, a także formułowanie na ich podstawie środków ochrony adekwatnych do przeprowadzanej analizy ryzyka.

2. Identyfikacja i analiza wymagań

Rozpoznawanie i wyznaczanie składników, systemów lub części infrastruktury mającej podstawowe znaczenie dla funkcjonowania państwa oraz jego obywateli z uwagi na swój charakter jest procesem ciągłym. Wynika to zarówno z naturalnego rozwoju społeczeństwa i gospodarki, jak i z wciąż pojawiających się nowych zagrożeń mogących zakłócić lub zniszczyć część infrastruktury niezbędnej do prawidłowego funkcjonowania organów administracji i życia obywateli.

Podstawowym instrumentem ułatwiającym rozpoznawanie i wyznaczanie określonych systemów, należących do poszczególnych sektorów, o których mowa w art. 3 ustawy[3], do kategorii infrastruktury krytycznej jest rozmiar strat wynikłych z ich zakłócenia lub zniszczenia. Opierając się na Dyrektywie[4] można sformułować pewne wymagania co do ww. strat pozwalające na kwalifikowanie poszczególnych systemów w sposób umożliwiający zaliczenie ich do części infrastruktury krytycznej. W grupie tych wymagań powinny się znaleźć następujące kryteria:

- OFIARY W LUDZIACH oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych;
- SKUTKI EKONOMICZNE oceniane w odniesieniu do wielkości strat ekonomicznych lub pogorszenia towarów lub usług, w tym potencjalnych skutków ekologicznych;
- KONSEKWENCJE SPOŁECZNE oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych i zakłócenia codziennego życia, w tym utraty podstawowych usług.

Dla poszczególnych kryteriów istotne jest zdefiniowanie **progów akceptacji** opartych na rozmiarze strat wynikłych z awarii danej infrastruktury należącej do określonego sektora, przy czym należy zaznaczyć, że czynnikiem decydującym

[3] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. 2007, Nr 89, poz. 590 z późn. zm.).

[4] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*.

o wyznaczeniu danego systemu do kategorii infrastruktury krytycznej nie musi być wymaganie łącznego spełnienia wszystkich wyżej wymienionych przesłanek.

W celu umożliwienia skwantyfikowania progów akceptacji dla ww. kryteriów przyjęto założenie, że:

- OFIARY W LUDZIACH będą stanowiły potencjalną liczbę ofiar lub rannych w wyniku jednego lub kilku zdarzeń o koincydencyjnym charakterze;
- STRATY EKONOMICZNE będą stanowiły wielkość przeliczoną w odniesieniu do Produktu Krajowego Brutto (PKB);
- KONSEKWENCJE SPOŁECZNE będą określane w odniesieniu do aglomeracji jako obszaru o intensywnej zabudowie, charakteryzującego się dużym zagęszczeniem ludności przebywającej na danym terenie okresowo lub stale oraz dużym przepływem osób i towarów, w tym znaczną wymianą usług.

Tabela 1. Przykładowe kryteria i progi wyznaczania infrastruktury krytycznej

Progi akceptacji	Kryteria		
	Ofiary w ludziach	**Skutki ekonomiczne**	**Konsekwencje społeczne**
Straty **duże**	Zagrożenie utraty życia lub zdrowia dla więcej niż 50 osób	Zagrożenie utraty więcej niż 0,0001% PKB	Zagrożenie awarii więcej niż 50% aglomeracji.
Straty **średnie**	Zagrożenie utraty życia lub zdrowia dla mniej niż 50 osób	Zagrożenie utraty mniej niż 0,0001% PKB	Zagrożenie awarii mniej niż 50% aglomeracji.
Straty **małe**	Zagrożenie utraty życia lub zdrowia dla mniej niż 20 osób	Zagrożenie straty w granicach 0,000001% PKB	Zagrożenie awarii mniej niż 20% aglomeracji.
Straty **znikome**	Zagrożenie utraty zdrowia.	Nieznaczne straty finansowe nie przekraczające 0,0000001% PKB	Potencjalne zagrożenie naruszenia struktury aglomeracji.

Przyjmując przedstawioną metodę jako wyznacznik infrastruktury krytycznej można założyć, że jeśli dany system i związane z nim zdarzenie spowodowane niezamierzonym lub celowym działaniem człowieka, czy też siłami natury mogłoby być przyczyną dużych lub średnich strat ekonomicznych, społecznych lub ofiar w ludziach, wówczas system ten należący do któregokolwiek z sektorów, takich jak np.: systemy zaopatrzenia w energię, systemy finansowe i sieci teleinformatyczne, może stanowić część infrastruktury krytycznej.

Dla wyznaczenia infrastruktury krytycznej można posłużyć się poniższym uogólnionym wzorem:

$$S \in IK \Longleftrightarrow \bigvee_{Z} Z \Rightarrow P \in \left\{ \left(\bigvee_{K1,\,K2,\,K3} P = SD \right) \cdot \left(\bigvee_{K1} P = SM \wedge \bigvee_{K2,\,K3} P = SD \right) \right\}$$

S – system ∈ {Systemy zaopatrzenia w energię, surowce energetyczne i paliwa; Systemy łączności; Sieci teleinformatyczne; Systemy finansowe; Systemy zaopatrzenia w żywność; Systemy zaopatrzenia w wodę; Systemy ochrony zdrowia; Systemy transportowe; Systemy ratownicze; Systemy zapewniające ciągłość działania administracji publicznej; Systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych};

IK – infrastruktura krytyczna;

K – kryteria wyznaczenia IK, gdzie K ∈ {K1, K2, K3}, tj.: **K1** – kryterium ofiar w ludziach, **K2** – kryterium skutków ekonomicznych, **K3** – kryterium konsekwencji społecznych;

P – progi akceptacji dla strat związanych z K, gdzie P ∈ {SD, SS, SM}, tj.: **SD** – straty duże, **SS** – straty średnie, **SM** – straty małe;

Z – zagrożenie dla S związane z niezamierzonym lub celowym działaniem człowieka, lub sił natury.

W zależności od potrzeb i charakteru danego systemu można przyjąć różne kryteria i progi akceptacji pozwalające zakwalifikować dany system do infrastruktury krytycznej. W zaproponowanym wzorze założono, że jeśli istnieje zagrożenie Z dla systemu S, które mogłoby spowodować duże straty (SD) w odniesieniu do wszystkich kryteriów (K1, K2, K3) lub małe straty (SM) w ludziach (K1) oraz duże straty (SD) ekonomiczne (K2) i społeczne (K3), wówczas dany system S zaliczono by do infrastruktury krytycznej. Nie oznacza to jednak, że system, dla którego określone zagrożenie mogłoby spowodować średnie straty (SM) w stosunku do ofiar w ludziach (K1) i kryterium społecznego (K3), nie mógłby zostać wskazany jako element infrastruktury krytycznej.

W momencie rozpoznania i wyznaczenia systemów należących do poszczególnych sektorów infrastruktury krytycznej niezbędne jest zdefiniowanie wymagań w zakresie ich ochrony obejmujących podstawowe atrybuty bezpieczeństwa, takie jak[5,6]:

---

[5] ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.

[6] PN-I-02000:2002 Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia.

- **Dostępność** rozumianą jako pewność, że funkcja określonego systemu wchodzącego w skład infrastruktury jest dostępna wtedy, kiedy jest potrzebna.
- **Integralność** rozumianą jako zapewnienie dokładności i kompletności realizowanych funkcji systemu wchodzącego w skład infrastruktury, zgodnie z oczekiwaniami użytkownika.
- **Poufność** rozumianą jako pewność, że funkcje określonego systemu wchodzącego w skład infrastruktury są dostępne wyłącznie dla uprawnionych osób, podmiotów i procesów.

W zależności od sektora stanowiącego część infrastruktury krytycznej należy określić wymagania bezpieczeństwa w odniesieniu do każdego z ww. atrybutów, co pozwoli docelowo, po przeprowadzeniu analizy ryzyka, sformułować odpowiednie środki ochrony.

Właściwe rozpoznanie elementów wchodzących w skład infrastruktury krytycznej w ramach poszczególnych sektorów, a także sformułowanie wymagań bezpieczeństwa, co do ich ochrony pozwala na zaprojektowanie środków zabezpieczeń, które powinny być adekwatne do zidentyfikowanych zagrożeń i ryzyk. Należy przy tym pamiętać, że bezpieczeństwo całej infrastruktury związane jest z podejmowaniem wszelkich działań zmierzających do zapewnienia funkcjonalności, ciągłości działania i jej integralności, w celu zapobiegania zagrożeniom oraz ograniczenia i neutralizacji ich skutków.

3. Definiowanie środków ochorny

Po rozpoznaniu i wyznaczeniu systemów należących do infrastruktury krytycznej należy zdefiniować, na podstawie określonych wymagań bezpieczeństwa oraz przeprowadzonej analizy ryzyka, środki ochrony pozwalające na przeciwdziałanie zagrożeniom zniszczenia, uszkodzenia bądź zakłócenia ich funkcjonowania.

Zabezpieczenie infrastruktury krytycznej związane jest bezpośrednio z analizą ryzyka stanowiącą etap zarządzania ryzykiem polegający na stałym monitorowaniu jej elementów i zmniejszaniem możliwych dla nich niekorzystnych zdarzeń poprzez estymacje wartości ryzyka, odnoszącego się do stanu systemów infrastruktury krytycznej[7,8]. Ten całościowy proces identyfikacji, kontrolowania

[7] ISO 31000:2009 Risk Management – Principles and Guidelines.

[8] ISO/IEC 27005 Information technology – Security techniques – Information security risk management.

Tabela 2. Wymagania bezpieczeństwa dla elementów infrastruktury krytycznej

Sektor infrastruktury krytycznej[1]	Wymagania bezpieczeństwa (wybrane)		
	Dostępność	**Integralność**	**Poufność**
Systemy zaopatrzenia w energię, surowce energetyczne i paliwa	– Zapewnienie niezawodnej infrastruktury i urządzeń do wytwarzania i przesyłania energii elektrycznej. – Zagwarantowanie skutecznej produkcji, rafinacji, przetwarzania, magazynowania i przesyłania rurociągami ropy naftowej oraz gazociągami gazu. – Bezpieczne udostępnianie terminali skroplonego gazu ziemnego (LNG).	– Wdrożenie mechanizmów detekcji i korekcji błędów. – Wprowadzenie środków kontroli realizowanych funkcji pod względem zgodności ze specyfikacją. – Zapewnienie stałych i okresowych punktów kontrolnych w całym procesie produkcji, przechowywania i dystrybucji.	– Wprowadzenie kontrolowanego i rozliczanego dostępu do każdego elementu systemu. – Stałe monitorowanie stref o wysokim stopniu zagrożenia. – Zapewnienie wykrywania niepożądanych zdarzeń i osób w strefach bezpieczeństwa.
Systemy łączności	– Dostarczenie niezawodnych organizacyjno-technicznych usług telekomunikacyjnych.	– Wprowadzenie mechanizmów chroniących przed manipulacją osób nieuprawnionych.	– Zapewnienie ochrony kanałów łączności przed zniekształceniem i podsłuchem.
Sieci teleinformatyczne	– Zagwarantowanie niezawodnych kanałów teletransmisyjnych przeznaczonych do świadczenia usług.	– Wprowadzenie środków badania i sterowania jakością usług (Quality of Service).	– Wprowadzenie narodowych rozwiązań zabezpieczających m.in. w zakresie kryptografii.
Systemy finansowe	– Zagwarantowanie bezpiecznych systemów bankowych, finansowo-ubezpieczeniowych, finansowych podmiotów gospodarczych i ludności. – Zapewnienie niezawodnych mechanizmów regulujących funkcjonowanie budżetu państwa i jednostek samorządu terytorialnego.	– Zapewnienie pełnego sterowania obrotem środków finansowych. – Wdrożenie środków weryfikacji dokonywanych transakcji pod względem ich zgodności z prawem i specyfikacją systemu.	– Wprowadzenie kontroli mechanizmów finansowych. – Wdrożenie niezależnych instrumentów rozliczania zdarzeń i analizy przepływu środków finansowych.

Sektor infrastruktury krytycznej[1]	Wymagania bezpieczeństwa (wybrane)		
	Dostępność	**Integralność**	**Poufność**
Systemy zaopatrzenia w żywność	– Zapewnienie niezawodnego łańcucha żywnościowego obejmującego produkcję, przetwórstwo, dystrybucję, magazynowanie i postępowanie z żywnością oraz jej składnikami. – Wprowadzenie bezpiecznych kanałów dystrybucji.	– Wprowadzenie środków bezpieczeństwa w zakresie stosowanych substancji dodatkowych i aromatów, poziomów substancji zanieczyszczających, pozostałości pestycydów i warunków napromieniowania.	– Wprowadzenie kontroli jakości produktów i ich dostawców na zgodność z kryteriami programu HACCP.
Systemy zaopatrzenia w wodę	– Zapewnienie niezawodnej infrastruktury systemu wodociągowego, w tym systemu produkcji i dystrybucji wody ,dostarczania i dystrybucji wody. – Zaopatrzenie miast w wodę w wymaganej ilości i o określonej jakości w czasie wyznaczonym potrzebami odbiorców. – Zapewnienie monitorowania i sterowania operacyjnego systemem zaopatrzenia w wodę.	– Uzyskanie gwarancji spełniania przez wodę wymagań hydraulicznych, wymagań jakości fizycznej, chemicznej oraz bakteriologicznej. – Zagwarantowanie pełnego bezpiecznego cyklu hydrologicznego, w tym: ujmowania i transportu wody surowej, uzdatniania wody, dostarczania i dystrybucji wody uzdatnionej, użytkowania komunalnego i przemysłowego wody, odbioru i oczyszczania ścieków, odprowadzania ścieków oczyszczonych.	– Ograniczenie dostępu nieuprawnionych stron do zbiorczego systemu zaopatrzenia w wodę. – Zapewnienie mechanizmów dla utrzymywania bezpieczeństwa bakteriologicznego i toksykologicznego, w tym jakości wody i jej dostawy (ciśnienie, ilość). – Ochrona topologii i wyposażenia sieci, w tym struktury poboru wody.
Systemy ochrony zdrowia	– Dostarczenie sprawnych środków pozwalających zapewnić opiekę zdrowotną ludności.	– Zagwarantowanie pełnych usług na rzecz ochrony zdrowia.	– Kontrola dostępu do usług medycznych oraz ocena stosowanych technologii i źródeł finansowania.

Sektor infrastruktury krytycznej[1]	Wymagania bezpieczeństwa (wybrane)		
	Dostępność	**Integralność**	**Poufność**
Systemy transportowe	– Zagwarantowanie sprawności przetwarzania strumienia ładunków i pasażerów w ramach usług przewozowych.	– Zapewnienie pełnego układu komunikacyjnego wypełnionego zespołem inwestycji transportowych, obejmującego majątek trwały i obrotowy oraz czynnik ludzki.	– Wdrożenie mechanizmów kontroli ilościowych i jakościowych potrzeb przewozowych.
Systemy ratownicze	– Zagwarantowanie środków i metod ratowania życia ludzkiego i niesienia pomocy w warunkach zagrożenia, a także służących ratowaniu lub zabezpieczaniu sprzętu, pomieszczeń itd. – Zapewnienie systemu łączności, w tym programu szkoleniowego.	– Wprowadzenie zintegrowanego systemu ratownictwa w celu współdziałania wszystkich zaangażowanych podmiotów. – Utrzymywanie danych o krajowych ekspertach i grupach ratowniczych, w tym zespołów ds. rozpoznania i koordynacji.	– Wprowadzenie rozwiązań uniemożliwiających zakłócenie procesów niesienia pomocy i zabezpieczenia miejsca zdarzenia.
Systemy zapewniające ciągłość działania administracji publicznej	– Zapewnienie środków umożliwiających realizowanie zadań publicznych.	– Wdrożenie mechanizmów pozwalających na świadczenie podstawowych usług.	– Implementacja mechanizmów kontroli dostępu i rozliczania działań.
Systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	– Zagwarantowanie bezpiecznych mechanizmów przechowywania i przetwarzania substancji chemicznych i jądrowych.	– Wprowadzenie środków badania i sterowania jakością wytwarzanych chemikaliów.	– Wprowadzenie środków rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów.

[1] Art. 3 Ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. 2007, Nr 89, poz. 590 z późn. zm.).

i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia zdarzeń, które mogą mieć wpływ na poszczególne systemy infrastruktury krytycznej, wymaga zdyscyplinowanego, konsekwentnego i rzetelnego podejścia. Pozwoli to ostatecznie na unikanie ryzyka, podejmowanie działań prewencyjnych, czy też jego przenoszenie lub dywersyfikację. Działania te stanowią bazowe strategie przeciwdziałania ryzyku, przez co rezultaty analizy ryzyka w oparciu o zidentyfikowane zagrożenia i wymagania bezpieczeństwa wprost przekładają się na dobierane środki ochrony[9, 10, 11, 12].

Warto podkreślić, że zarządzanie ryzykiem jest procesem, składającym się ze ściśle określonych, następujących po sobie i wzajemnie się determinujących etapów, tworzących jednocześnie powtarzający się cykl, w którym istotnym elementem jest stałe komunikowanie wszelkich pojawiających się ryzyk. Efekty podjętych działań i wypracowanych materiałów w ramach jednego etapu stanowią źródło danych dla kolejnego kroku w cyklu zarządzania ryzykiem. Istotne jest, że wybrane procesy, takie jak identyfikacja i analiza ryzyka odbywają się w sposób ciągły.

Dla poszczególnych systemów wchodzących w skład infrastruktury krytycznej należy sformułować, odpowiednio do wyników analizy ryzyka, środki zabezpieczeń w obszarze organizacyjnym, technicznym i kontrolno-weryfikacyjnym w odniesieniu do każdego z atrybutów bezpieczeństwa, tj. dostępności, integralności i poufności.

Właściwe rozpoznanie zagrożeń i ocena związanego z nimi ryzyka zakłócenia lub zniszczenia systemów istotnych z punktu widzenia życia obywatela i działania organów administracji stanowi podstawę wdrożenia wybranych środków ochrony elementów infrastruktury krytycznej. Poszczególne rodzaje zabezpieczeń powinny być wzajemnie skorelowane w sposób umożliwiający skuteczne przeciwdziałanie zagrożeniom. Nie mniej ważne jest również odpowiednie konstruowanie systemów infrastruktury krytycznej w sposób pozwalający na świadczenie minimalnych usług nawet w przypadku poważanych awarii spowodowanych niezamierzonym lub celowym działaniem człowieka lub sił natury.

---

[9] PN-ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

[10] PN-EN 50133-1:2007 Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe.

[11] PN-E-08350-14: 2002 Systemy sygnalizacji pożarowej. Projektowanie, zakładanie, odbiór, eksploatacja i konserwacja instalacji.

[12] PN-EN 50133-7: 2002 Systemy alarmowe. Systemy kontroli dostępu stosowane w zabezpieczeniach. Część 7: Zasady stosowania.

Tabela 3. Środki ochrony elementów infrastruktury krytycznej

Wymaganie bezpieczeństwa	Środki ochrony (wybrane)		
	Organizacyjne	**Techniczne**	**Kontrolno-weryfikacyjne**
Dostępność	– Plany ciągłości działania, w tym plany współdziałania i organizacji dostaw w sytuacjach kryzysowych oraz procedury sygnalizowania zagrożeń i zarządzania kryzysowego. – Wdrożenie polityki bezpieczeństwa, w tym procedur kontroli dostępu. – Podnoszenie świadomości w obszarze zagrożeń i środków zabezpieczeń. – Doskonalenie wiedzy i praktycznych umiejętności m.in. w zakresie obsługi planów alarmowych. – Współpraca z służbami bezpieczeństwa i ratownictwa medycznego, w tym Siłami Zbrojnymi RP w zakresie zapobiegania i obsługi zdarzeń związanych z sytuacjami kryzysowymi. – Stosowanie rozwiązań zgodnych z powszechnie akceptowalnymi standardami w danej dziedzinie.	– Implementacja systemów sygnalizacji włamania i napadu. – Wdrożenie systemów telewizji dozorowej. – Instalacja systemów ochrony peryferyjnej wewnętrznej. – Wdrożenie systemów monitoringu i interwencji fizycznej. – Zastosowanie systemów monitoringu stref zastrzeżonych zewnętrznych. – Wdrożenie systemów monitoringu skażeń środowiska. – Stosowanie systemów sygnalizacji pożaru i oddymiania. – Implementacja systemów ewakuacyjnych i nagłośnieniowych. – Wdrażanie rozwiązań redundantnych i zapasowych.	– Prowadzenie regularnych testów podatności na uszkodzenia. – Badanie faktycznej wytrzymałości obiektów, konstrukcji urządzeń. – Okresowa kontrola adekwatności przyjętych zabezpieczeń w stosunku do nowych zagrożeń. – Bieżąca identyfikacja zagrożeń i analiza ryzyka z nimi związana. – Okresowa ocena poziomu wdrożonych zabezpieczeń. – Przegląd zasad zarządzania w sytuacji kryzysowej i procedur awaryjnych. – Sprawdzenie jakości dokumentacji systemu i wiedzy oraz umiejętności użytkowników. – Przegląd zabezpieczeń w celu weryfikacji istnienia i adekwatności planu awaryjnego zapewniającego kontynuację działania systemu w przypadku zakłóceń.

Wymaganie bezpieczeństwa	Środki ochrony (wybrane)		
	Organizacyjne	**Techniczne**	**Kontrolno-weryfikacyjne**
Integralność	– Wykorzystywanie znormalizowanych urządzeń zabezpieczenia mechanicznego ujętych w kategorie wytrzymałości mechanicznej (szyby, drzwi, ściany, stropy, kraty) pod względem czasu otwarcia lub wyłamania. – Stosowanie sprawdzonych rozwiązań konstrukcyjnych poszczególnych elementów urządzenia, obiektu i systemu.	– Dyslokacja elementów systemu. – Instalacja urządzeń wykrywających i zapobiegawczych. – Uruchomienie centrów zarządzania kryzysowego. – Wprowadzanie rezerwowych kanałów dystrybucji. – Dywersyfikacja rozwiązań zapewniających dostawy.	– Przegląd możliwości sprzętowych w zakresie wykrywania błędów związanych z nieprawidłowym działaniem systemu. – Wykorzystywanie rozwiązań w zakresie badania jakości i weryfikacji poprawności realizowanych procedur. – Okresowa walidacja realizowanych funkcji pod względem zgodności z przyjętą specyfikacją.
Poufność	– Utrzymywanie całodobowego dozoru lokalnego. – Wprowadzenie stref szczególnie chronionych (zastrzeżonych). – Wdrożenie procedur przeszukiwania osób, bagaży, pojazdów i przesyłek.	– Wdrożenie mechanicznych i elektronicznych systemów kontroli dostępu. – Instalacja systemów ochrony perymetrycznej obwodowej.	– Przegląd i okresowa weryfikacja adekwatności i efektywności wdrożonych zabezpieczeń. – Ocena mechanizmów kontroli pod względem zapewnienia ochrony przed stratami lub poważnymi błędami.

4. Określenie architektury rozwiązań

Rozpoznanie i wyznaczenie infrastruktury krytycznej, w celu zapewnienia utrzymania podstawowych atrybutów bezpieczeństwa wymaga wdrażania środków ochrony adekwatnych do postawionych wymagań i przeprowadzanej analizy ryzyka. Nie wyklucza to jednak takiego projektowania i budowania systemów stanowiących elementy tej infrastruktury, aby już sama ich konstrukcja uwzględniała stosowne zabezpieczenia odnoszące się do standardowych ryzyk dla określonego typu systemów należących do poszczególnych sektorów infrastruktury krytycznej. Odpowiednie zaprojektowanie architektury rozwiązań systemów oraz wchodzących w ich skład powiązanych ze sobą funkcjonalnie obiektów, w tym urządzeń, instalacji oraz kluczowych usług dla bezpieczeństwa państwa i jego obywateli bezpośrednio wpływa na koszt implementacji środków ochrony.

Biorąc pod uwagę różnorodność systemów stanowiących krytyczną infrastrukturę, w tym systemy produkcji i składowania substancji chemicznych, zaopatrzenia w wodę i transportowe, systemy energetyczne, ich konstrukcja w obszarze zabezpieczeń powinna uwzględniać nie tyle rozwiązania techniczne, co również fizyczne, zwłaszcza w zakresie ich geograficznej lokalizacji, a nawet rozproszenia poszczególnych komponentów. Podejście takie zapewni środki kompensujące zagrożenia związane z działaniem sił natury, czy nawet człowieka poprzez wprowadzenie utrudnień dotyczących zniszczenia lub unieruchomienia części infrastruktury.

W grupie charakterystycznych rozwiązań pozwalających na zapewnienie ciągłości działania systemów infrastruktury na skutek różnego typu awarii powinny znaleźć się mechanizmy tolerowania uszkodzeń, spowodowanych np. błędami konstrukcyjnymi i wadliwością stosowanych podzespołów. Pod uwagę powinny być brane również wszelkie inne metody, takie jak: systemy zapasowe i rozwiązania alternatywne, np. agregaty prądotwórcze w wypadku uszkodzenia systemów zasilania energetycznego, zapewniające świadczenie niezbędnych usług związanych z ochroną zdrowia i życia.

Wyznacznikiem dla procesu projektowania systemów, które mają być częścią infrastruktury krytycznej są wymagania bezpieczeństwa w odniesieniu do kryteriów oraz odpowiadających im progów akceptacji. W zależności od potrzeb w zakresie ochrony i potencjalnego rozmiaru strat wynikłych z zakłócenia lub zniszczenia danego systemu uwzględniane mogą być konkretne rozwiązania spełniające ww. wymagania w obszarze architektury pozwalające na minimalizowanie ryzyka związanego z jego prawidłowym funkcjonowaniem. Należy jednak pamiętać, że architektura systemu będącego częścią krytycznej infrastruktury będzie wypadkową ww. wymagań i kryteriów.

Tabela 4. Wymagania dla architektury systemu infrastruktury krytycznej

Wymaganie bezpieczeństwa	Kryterium	Próg akceptacji (straty)	Wymagania architektury systemu (wybrane)
Dostępność	Ofiary w ludziach	DUŻE	– Konstrukcja o wysokiej wytrzymałości z rozproszoną dyslokacją krytycznych funkcji. – Przestrzenie uniemożliwiające gromadzenie w jednym miejscu dużej liczby osób. – Konstrukcja z co najmniej dwoma niezależnymi urządzeniami wewnętrznej komunikacji pionowej.
		ŚREDNIE	– Wbudowane sprzęgła w strefach zagrożonych wybuchem. – Konstrukcja ułatwiająca projektowanie zewnętrznych i wewnętrznych stref bezpieczeństwa. – Konstrukcja o wysokiej wytrzymałości.
		MAŁE	– Struktura bez elementów redundancji umożliwiająca realizowanie funkcji systemu.
	Skutki ekonomiczne	DUŻE	– Zdublowanie krytycznych funkcji działających niezależnie. – Konstrukcja obiektu umożliwiająca instalację elementów systemów wczesnego ostrzegania (alarm, ppoż. itd.) połączonych kilkoma niezależnymi drogami.
		ŚREDNIE	– Implementacja elementów nadmiarowych niezależnie rozmieszonych. – Struktura pozwalająca na uruchamianie rozwiązań doraźnych.
		MAŁE	– Wbudowane mechanizmy świadczenia podstawowych usług.
	Konsekwencje społeczne	DUŻE	– Instalacje tolerujące uszkodzenia i wdrażające obejścia miejsca awarii.
		ŚREDNIE	– Instalacje pozwalające na wdrażanie obejść miejsca awarii.
		MAŁE	– Konstrukcje pozwalające na sprawne wdrożenie środków tymczasowych do czasu usunięcia awarii.
Integralność	Ofiary w ludziach	DUŻE	– Wkomponowane zróżnicowane instrumenty weryfikacji poprawności realizowanych funkcji i braku ingerencji czynników zewnętrznych.
		ŚREDNIE	– Wbudowane mechanizmy wykrywania i korekcji błędów.

Wymaganie bezpieczeństwa	Kryterium	Próg akceptacji (straty)	Wymagania architektury systemu (wybrane)
Integralność	Ofiary w ludziach	MAŁE	– Podstawowe instrumenty sprawdzania poprawności realizowanych funkcji.
	Skutki ekonomiczne	DUŻE	– Segmentacja pozwalająca izolować miejsce awarii od pozostałych części systemu.
		ŚREDNIE	– Konstrukcja ograniczająca rozszerzanie się awarii.
		MAŁE	– Podstawowe mechanizmy redukcji zakłóceń realizowanych funkcji.
	Konsekwencje społeczne	DUŻE	– Konstrukcja ograniczająca rozprzestrzenianie się awarii.
		ŚREDNIE	– Utrudnione mechanizmy nieuprawnionej manipulacji.
		MAŁE	– Struktura limitująca przystępność obiektów, urządzeń itd.
Poufność	Ofiary w ludziach	DUŻE	– Wbudowane narodowe rozwiązania w zakresie bezpieczeństwa. – Kompozycja obiektu, urządzenia itd. kamuflująca faktyczne funkcje systemu.
		ŚREDNIE	– Konstrukcja pozwalająca stosować kilka niezależnych systemów wczesnego ostrzegania, w tym kontroli dostępu.
		MAŁE	– Struktura uwzględniająca podstawowe mechanizmy ewakuacji.
	Skutki ekonomiczne	DUŻE	– Wbudowane możliwości instalacji ukrytych systemów wczesnego ostrzegania.
		ŚREDNIE	– Struktura pozwalająca ukryć faktyczną lokalizację i pojemność obiektu.
		MAŁE	– Konstrukcja uwzględniająca podstawowe wymagania w zakresie kontroli i rozliczania.
	Konsekwencje społeczne	DUŻE	– Segmentacja świadczonych usług pod względem ich ważności.
		ŚREDNIE	– Kompozycja uniemożliwiająca niewłaściwe użycie obiektu, urządzenia itp.
		MAŁE	– Wbudowane standardowe instalacje.

5. Podsumowanie

Wyznaczenie infrastruktury krytycznej jest zadaniem złożonym. Wymaga przede wszystkim wskazania takich składników i systemów, które mają podstawowe znaczenie dla funkcjonowania państwa i jego obywateli. Istotnym elementem jest tutaj konieczność określenia dla każdego z tych systemów wymagań bezpieczeństwa i tym samym, na ich podstawie oraz w wyniku przeprowadzonej analizy ryzyka, zdefiniowania środków zabezpieczeń. Bez wątpienia pomocnym elementem byłoby uwzględnienie środków ochrony już na etapie projektowania i budowania systemów infrastruktury krytycznej.

Ważnym elementem działań związanych z ochroną infrastruktury krytycznej nie powinno być wyłącznie zabezpieczenie jej elementów, ale również wypracowanie takich rozwiązań, dzięki którym ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu byłyby możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki. Istota tych zadań powinna także sprowadzać się nie tyle do zapewnienia ochrony infrastruktury przed zagrożeniami, ale również do ograniczania ich skutków oraz szybkiego jej odtworzenia na wypadek awarii, ataków oraz innych zdarzeń zakłócających prawidłowe funkcjonowanie organów państwa i jego obywateli. Proces projektowania i budowania systemów infrastruktury krytycznej i wdrażanie środków ochrony powinien uwzględniać konieczność zapewnienia funkcjonowania urządzeń i obiektów użyteczności publicznej oraz infrastruktury komunalnej w przypadku odbudowy infrastruktury sprawdzającej się do przywracania stanu sprzed sytuacji kryzysowej.

Nie można zapomnieć również o tym, że rozpoznanie i wyznaczenie określonego systemu jako część infrastruktury krytycznej nie ma permanentnego charakteru. Wynika to z faktu, że mogą zaistnieć takie okoliczności i zdarzenia, które spowodują, że dany system nie będzie już spełniał kryteriów i odpowiadających im progów pozwalających na zakwalifikowanie go do systemów niezbędnych dla zapewnienia bezpieczeństwa państwa i jego obywateli.

Projektując architekturę dla systemów infrastruktury krytycznej i definiując środki ochrony w odniesieniu do wymagań i określonych ryzyk należy mieć na uwadze, aby konstrukcja proponowanych rozwiązań była wykonalna i adekwatna względem rzeczywistych potrzeb, a tym samym aby zapewniała ich dostępność, integralność i poufność.