

# CYBERBEZPIECZEŃSTWO PRZEDSIĘBIORSTW W KLUCZOWYCH BRANŻACH GOSPODARKI



## **MGR INŻ. DOROTA BAŁACHOWSKA**

Kierownik Wydziału Certyfikacji  
Wiceprzewodnicząca Zespołu ds. Cyberbezpieczeństwa UDT  
Departament Certyfikacji i Oceny Zgodności  
Urząd Dozoru Technicznego

Współczesna gospodarka opiera się na wykorzystywaniu bardzo wielu różnorodnych technologii, które wykształciły specyficzne środowisko pracy. Obserwujemy nieodwracalny progres cywilizacyjny i technologiczny napędzany nieustannym dążeniem do innowacyjności. Konsekwencją tak dużego postępu gospodarczego jest ujawnienie się różnego rodzaju zagrożeń wywołanych działalnością człowieka. Bezpieczeństwo w przemyśle zależy nie tylko od właściwego prowadzenia procesów i eliminacji narażenia ludzi na skutki zagrożeń, ale polega również na zapobieganiu atakom zewnętrznym, w tym cyberatakam.



Jest to zadanie dla Urzędu Dozoru Technicznego, które realizujemy zgodnie z obowiązującą wizją: **Lider innowacyjności w obszarze bezpieczeństwa publicznego, w tym również w obszarze cyberbezpieczeństwa.**

Zagrożenia związane z atakami w sieci można ograniczyć, stosując określone procedury.

Urząd Dozoru Technicznego opracował innowacyjną metodykę, która pomaga firmom w przeprowadzeniu audytu cyberbezpieczeństwa na zgodność z obowiązującymi przepisami.

## BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Systemy komputerowe stosowane w przemyśle powinny być zintegrowane w obszarze *security* oraz *safety*. Wyróżnia się dwa rodzaje systemów komputerowych z uwzględnieniem wymienionych obszarów, tj. systemy komputerowe odpowiedzialne za przetwarzanie, przechowywanie i przesyłanie informacji oraz systemy komputerowe odpowiedzialne za sterowanie, które reagują na zdarzenia zachodzące w ich środowisku poprzez wysyłanie do nich informacji sterującej. Przy budowaniu programu cyberbezpieczeństwa w organizacji należy uwzględnić integralność obu systemów.

**Zapewnianie bezpieczeństwa to działania UDT, które jako organizacja zaufania publicznego realizujemy od ponad 100 lat.**

Dobrze opracowany i skutecznie wdrożony program cyberbezpieczeństwa powinien umożliwić organizacji efektywne zarządzanie ryzykiem również poprzez odpowiednie wykorzystanie zasobów w obszarze cyberbezpieczeństwa. Organizacja musi zapewnić skuteczną ochronę przed istniejącymi i potencjalnymi zagrożeniami, wykrywać luki w systemie, podejmować niezbędne działania naprawcze oraz chronić aktywa informacyjne stanowiące wymierną wartość organizacji. Nieodłącznym aspektem należy opracowanego i skutecznie wdrożonego programu cyberbezpieczeństwa jest zadbanie o ochronę marki i reputacji organizacji oraz zapewnienie przewagi konkurencyjnej, m.in. poprzez elastyczne dostosowywanie się do otaczających zmian biznesowych.



Rys. 1. Pięć zasad cyberbezpieczeństwa

## KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

W skład Krajowego Systemu Cyberbezpieczeństwa (KSC) wchodzi m.in. instytucje administracji rządowej i samorządowej oraz najwięksi przedsiębiorcy z kluczowych sektorów gospodarki.

„Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.” [1]

W ustawie o krajowym systemie cyberbezpieczeństwa [1] określono objęte nią podmioty. Wśród nich można wymienić:

- **operatorów usług kluczowych (OUK), którymi są m.in. największe banki, firmy z sektora energetycznego, przewoźnicy lotniczy i kolejowi, armatorzy, szpitale,**
- **dostawców usług kluczowych (DUC), czyli m.in. internetowe platformy handlowe, organy właściwe (OW), czyli instytucje publiczne, w których kompetencjach znajdzie się nadzór nad danym sektorem istotnym dla gospodarki.**

W ramach KSC powstały Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. Utworzono je w trzech instytucjach: Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (CSIRT NASK) oraz Ministerstwie Obrony Narodowej (CSIRT MON).

Ustawa o KSC nakłada na operatorów usług kluczowych liczne obowiązki. Jednym z nich jest obowiązek przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej. Pierwszy audyt powinien być przeprowadzony w ciągu roku od momentu powołania na Operatora Usługi Kluczowej. Warto podkreślić, że za niewykonanie przez OUK obowiązków wynikających z ustawy przewidziano zastosowanie kar finansowych (rozdział 14 UoKSC).

**Urząd Dozoru Technicznego na potrzeby przeprowadzania audytu cyberbezpieczeństwa na zgodność z wymaganiami zawartymi w ustawie o Krajowym Systemie Cyberbezpieczeństwa opracował innowacyjną metodykę Framework UDTCyber tj. strukturę ramową systemu oceny cyberbezpieczeństwa w organizacji, stanowiącą jednocześnie podstawę do budowania programu cyberbezpieczeństwa.**



**Wydanie 2 Framework UDTCyber** jest odpowiedzią na zmiany w obowiązujących przepisach, jak również aktualizacje norm będących podstawą merytoryczną opracowania.

Dokument oparty jest na międzynarodowych metodykach, takich jak NIST Cybersecurity Framework [2], wymaganiach i wytycznych norm serii ISO/IEC 27000 [3, 8], IEC 62443 [4] oraz ISO 22301 [5], a także na wymaganiach ustawy o Krajowym Systemie Cyberbezpieczeństwa – UoKSC (Dz.U. z 2023 r. poz. 913) [1].

## WYMAGANIA PRAWNE – DYREKTYWA NIS 2 ORAZ DYREKTYWA CER

Aktualnie obowiązującym aktem prawnym dotyczącym ogólnego poziomu cyberbezpieczeństwa na terenie Rzeczypospolitej Polskiej jest ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r., Dz.U. z 2023 r. poz. 913 [1].

Ustawa KSC [1] (podrozdział 4.2) wraz z aktami wykonawczymi (podrozdział 4.3) implementuje postanowienia dyrektywy NIS 2016/1148/UE (ang. Network and Information Systems Directive) z 2016 r. (podrozdział 4.1).

Tymczasem w Dzienniku Urzędowym UE L333/80 z 27 grudnia 2022 r. została opublikowana dyrektywa NIS 2 2022/2555 [6] – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS).

Co ważne, wraz z publikacją NIS 2 w tym samym Dzienniku Urzędowym UE opublikowana została również dyrektywa CER 2022/2557 [7] – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.

**Dyrektywa CER wraz z dyrektywą NIS 2 tworzą całościowo spójne i zharmonizowane ramy prawne w zakresie zapewniania ciągłości świadczenia usług kluczowych dla państwa, kreując przy tym odporność podmiotów świadczących te usługi na zagrożenia fizyczne i incydenty cyberbezpieczeństwa.**

Z uwagi na powiązanie między bezpieczeństwem fizycznym a cyberbezpieczeństwem podmiotów krytycznych obydwa akty prawne wzajemnie się uzupełniają, przy czym dyrektywy CER nie stosuje się do kwestii objętych dyrektywą NIS 2. Dyrektywy weszły w życie 16 stycznia 2023 r., a państwa członkowskie zostały zobowiązane do implementacji wymagań unijnych do prawa krajowego do 17 października 2024 r. W chwili obecnej wymagania dyrektyw NIS 2 oraz CER nie zostały jeszcze wdrożone do prawa polskiego.

### Dyrektywa NIS 2 [6] określa:

- obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT),
- środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach kluczowych i ważnych, o których mowa w załączniku I lub II dyrektywy, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy CER,
- zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie,
- obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

### Dyrektywa NIS 2 [6] definiuje:

podmioty kluczowe (sektory kluczowe – Załącznik I dyrektywy NIS 2),  
podmioty ważne (sektory ważne – Załącznik II dyrektywy NIS 2).





Tabela 1. Zmiany sektorowe w dyrektywie NIS 2 w stosunku do dyrektywy NIS (**kolor czerwony – zmiany w stosunku do dyrektywy NIS, kolor zielony – brak zmian w stosunku do dyrektywy NIS**)

SEKTORY PODMIOTÓW KLUCZOWYCH	SEKTORY PODMIOTÓW WAŻNYCH
Energetyka (energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór)	Usługi pocztowe i kurierskie
Transport (lotniczy, kolejowy, wodny, drogowy)	Gospodarowanie odpadami
Bankowość	Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne; sprzęt elektryczny; maszyny i urządzenia; pojazdy samochodowe, przyczepy i naczepy; pozostały sprzęt transportowy)
Infrastruktura rynków finansowych	Produkcja, wytwarzanie i dystrybucja chemikaliów
Opieka zdrowotna	Produkcja, przetwarzanie i dystrybucja żywności
Woda pitna	Dostawcy usług cyfrowych
Ścieki	Badania naukowe
Infrastruktura cyfrowa	
Zarządzanie usługami ICT (między przedsiębiorstwami)	
Podmioty administracji publicznej	
Przestrzeń kosmiczna	

Reasumując, dyrektywa NIS 2 rozszerza znacznie zakres pierwszej dyrektywy NIS, zaostrza wymogi w zakresie bezpieczeństwa i sprawozdawczości dla przedsiębiorstw, wprowadza bardziej rygorystyczne środki nadzoru dla organów krajowych i surowsze wymogi w zakresie egzekwowania przepisów oraz poprawia wymianę informacji i współpracę między organami państw członkowskich.

## AUDYT BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO

Urząd Dozoru Technicznego przeprowadza audyty cyberbezpieczeństwa (audyt trzeciej strony) według kryteriów i obszarów zdefiniowanych w ramach Framework UDTCyber.

UDT jest jednostką akredytowaną w ramach norm:

- PN-EN ISO/IEC 27001. Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania [3],
  - PN-EN ISO 22301 – Systemy zarządzania ciągłością działania [5]
- oraz zatrudnia wykwalifikowanych audytorów posiadających odpowiednie kompetencje.

Zespół audytorów UDT dysponuje zarazem możliwościami technicznymi do przeprowadzania audytów cyberbezpieczeństwa i niezbędną wiedzą w wymaganym obszarze. Audyt jest szczególnym rodzajem oceny wykonywanym przez stronę niezależną.

### Niezależność strony wykonującej audyt musi być zachowana w stosunku do:

- organizacji i zespołu projektowego lub np.
- budującego system zabezpieczeń,
- dostawców sprzętu i oprogramowania,
- organizacji podlegającej przeglądom\*.

**Każda odpowiedzialna organizacja ma wydzielony oddzielny zespół/departament odpowiedzialny za cyberbezpieczeństwo, niebędący w strukturach IT.**

\* W skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt.

Dokumentacja wyników audytu powinna składać się z:

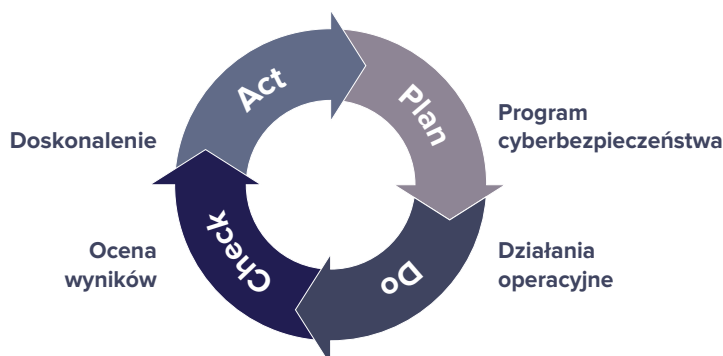
- raportu z audytu, zawierającego specyfikację celu audytu, opis realizacji przedsięwzięcia audytowego, podsumowanie wyników dla kadry kierowniczej (często wyodrębniane jako osobny dokument), specyfikację punktów sprawdzeń wraz z wynikami, zalecenia poaudytowe;
- wyników badań technicznych (tzw. dowodów audytowych) zawierających: przeglądy konfiguracji, analizę wyników testów penetracyjnych przeprowadzonych przez organizację bądź inny podmiot na zlecenie organizacji itp.

**Audyt może być przeprowadzany w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych, a więc np. audyt systemu zarządzania bezpieczeństwem informacji (27001) i zarządzania ciągłością działania (22301).**

## FRAMEWORK UDTCYBER

Metodyka UDTCyber zbudowana jest w systemie 7/7. Podział uwzględnia 7 modułów oraz 7 zdefiniowanych obszarów stanowiących zakres oceny. Framework UDTCyber jest metodyką, którą łatwo dostosować do potrzeb każdej organizacji oraz do potrzeb operatorów usług kluczowych.

**Budowa programu cyberbezpieczeństwa na podstawie niniejszej metodyki opiera się na cyklu Deminga (cykl PDCA) przebiegającym w czterech następujących po sobie etapach: planowanie – wykonanie – sprawdzenie – poprawienie (ang. Plan – Do – Check – Act).**

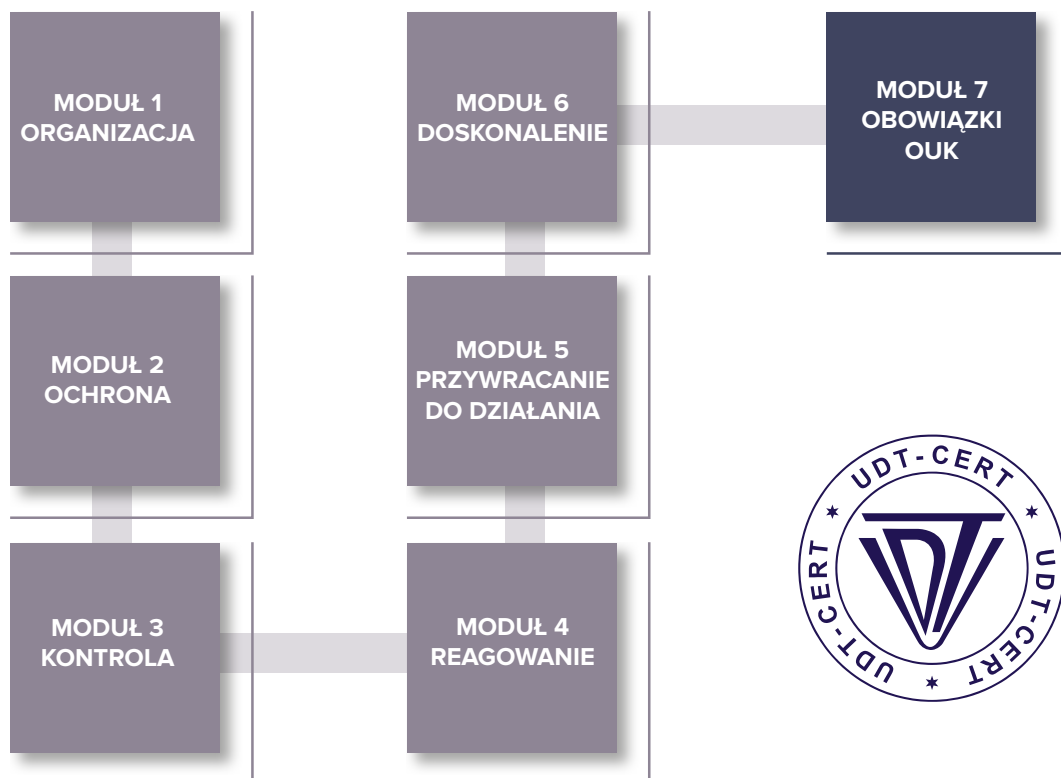


Rys. 2. Budowa programu cyberbezpieczeństwa na podstawie cyklu PDCA

Urząd Dozoru Technicznego tworząc innowacyjną metodykę budowania programu cyberbezpieczeństwa i oceny organizacji w ramach audytu cyberbezpieczeństwa, zastosował wybrane międzynarodowe metodyki: wymagania ISO/IEC 27001 [3] wraz z wytycznymi ISO/IEC 27002 [8], NIST Cybersecurity Framework [2], wymagania ISO 22301 [5], IEC 62443 [4] oraz wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa [1].



## FRAMEWORK **UDT** CYBER



Rys. 3. Framework UDTCyber – struktura

**Framework UDTCyber obejmuje następujące moduły (1-7) i obszary (M(1-7).1-7)**

**PRZYKŁAD**

Moduł 1 Organizacja - zawiera siedem obszarów od M1.1 do M1.7

Moduł 4 Reagowanie - zawiera siedem obszarów od M4.1 do M4.7.

M1.1. Struktura organizacyjna i otoczenie

M1.2. Zasoby ludzkie

M1.3. Zarządzanie i odpowiedzialność

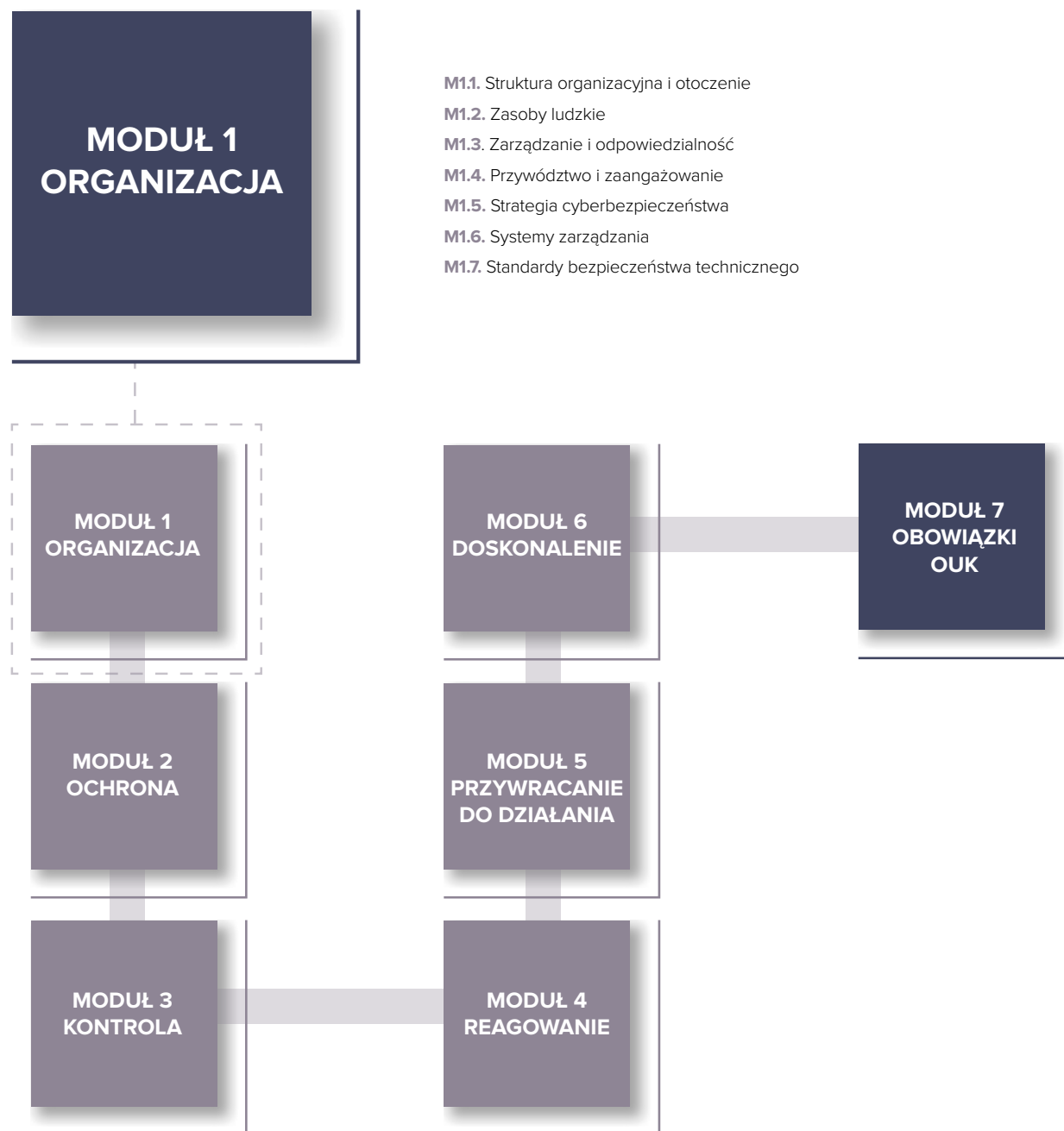
M1.4. Przywództwo i zaangażowanie

M1.5. Strategia cyberbezpieczeństwa

M1.6. Systemy zarządzania

M1.7. Standardy bezpieczeństwa technicznego

## FRAMEWORK UDT CYBER



Rys. 4. Moduł 1 Framework UDTCyber: ORGANIZACJA



## STANDARZY IEC 62443

Nowym elementem opracowania **Framework UDTCyber – wydanie 2** jest rozszerzenie o serię standardów **IEC 62443 [4]** (pierwotnie ISA-99) – Bezpieczeństwo w systemach sterowania i automatyki przemysłowej (ang. Security for Industrial Automation and Control Systems) / Przemysłowe sieci komunikacyjne - Bezpieczeństwo sieci i systemów (ang. Industrial communication networks – Network and system security).

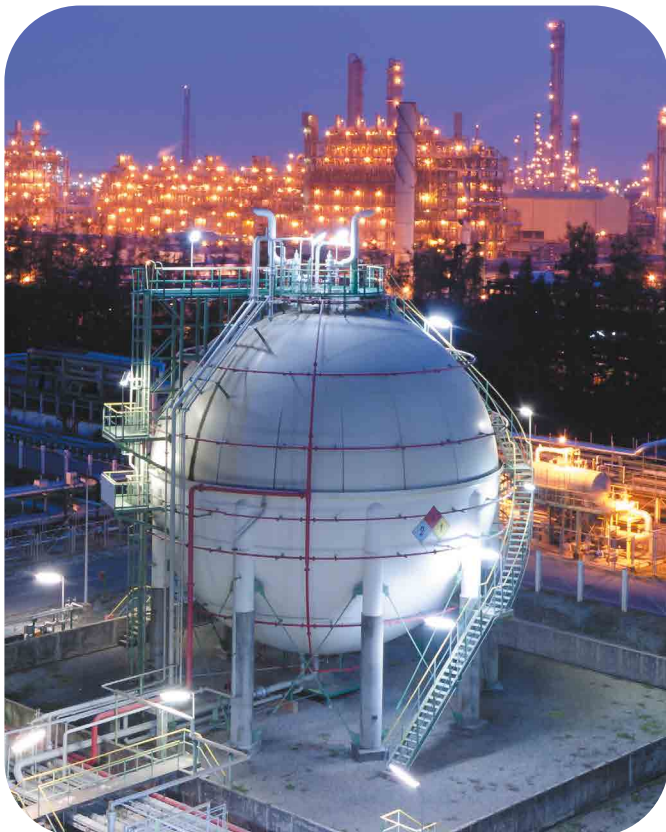
Seria norm będzie składać się docelowo z 15 arkuszy (kilka arkuszy jest aktualnie w opracowaniu), publikowanych historycznie jako ISA (ang. ISA – International Society of Automation, US), ANSI/ISA (ang. ANSI – American National Standards Institute), IEC (ang. IEC – International Electrotechnical Commission) oraz PN-EN IEC, dotyczących bezpieczeństwa w automatyce przemysłowej i systemach sterowania IACS (ang. Industrial Automation and Control Systems) oraz w przemysłowych sieciach komunikacyjnych (ang. Industrial communication networks).

Arkusze z pierwszej części normy wprowadzają do kluczowych terminów, pojęć i modeli używanych w całej serii norm IEC 62443 oraz ułatwiają zrozumienie specyficznej terminologii związanej z cyberbezpieczeństwem w kontekście systemów sterowania przemysłowego. Składają się na tę część cztery arkusze opisujące koncepcje cyberbezpieczeństwa, słownik terminów, definicji, metodologia opracowywania wskaźników ilościowych pochodzących z procesu i wymagań technicznych zawartych w normach, określenie podstawowego cyklu życia zabezpieczeń IACS, a także kilka przypadków użycia.

Druga część normy zawiera dokumenty, które skupiają się na politykach i procedurach związanych z bezpieczeństwem IACS. W skład tej części wchodzi pięć arkuszy określających wymagania co do zdefiniowania i wdrożenia efektywnego systemu zarządzania cyberbezpieczeństwem IACS, metodologię oceny poziomu ochrony, wytyczne dotyczące zarządzania poprawkami dla IACS, wymagania dla dostawców oraz informację, co jest wymagane do prowadzenia skutecznego programu cyberbezpieczeństwa IACS.

Trzecia część opisuje wymagania na poziomie systemowym zawarte w trzech arkuszach. Opisują one zastosowanie różnych technologii bezpieczeństwa w środowisku IACS, ocenę ryzyka cyberbezpieczeństwa i projektowania (model Zone and Conduit) oraz wymagania dla systemu IACS na podstawie poziomu bezpieczeństwa.

Czwarta i ostatnia grupa obejmuje dokumenty, które dostarczają informacji dotyczących bardziej konkretnych i szczegółowych wymagań związanych z rozwojem produktów IACS. W skład tej części wchodzi dwa arkusze opisujące cykl życia rozwoju zabezpieczeń oraz wymagania dotyczące komponentów IACS na podstawie poziomu bezpieczeństwa. Składniki obejmują urządzenia wbudowane, urządzenia hosta, urządzenia sieciowe i aplikacje.



## 1. WSTĘP

## 2. ZASADY I PROCEDURY

## 3. WYMAGANIA SYSTEMOWE

## 4. WYMAGANIA DOTYCZĄCE KOMPONENTÓW

- 1-1: Terminologia, koncepcje i modele
- 1-2: Główny słownik terminów i definicji
- 1-3: Wskaźniki zgodności zabezpieczeń systemu
- 1-4: Cykl życia i przypadki użycia zabezpieczeń IACS
- 2-1: Stworzenie programu bezpieczeństwa IACS
- 2-2: Oceny programów bezpieczeństwa IACS
- 2-3: Zarządzanie poprawkami w środowisku IACS
- 2-4: Wymagania programu bezpieczeństwa dla dostawców usług IACS
- 2-5: Wskazówki dotyczące wdrożenia dla właścicieli aktywów IACS
- 3-1: Technologie zabezpieczeń dla systemu IACS
- 3-2: Ocena ryzyka bezpieczeństwa dla projektu systemu
- 3-3: Wymagania i poziomy bezpieczeństwa systemu
- 4-1: Wymagania dotyczące cyklu życia rozwoju bezpieczeństwa produktu
- 4-2: Techniczne wymagania dotyczące bezpieczeństwa komponentów (IACS)

Rys. 5. Budowa standardu IEC 62443 [4]

Adresaci serii norm IEC 62443, w zależności od arkusza

- właściciele instalacji/systemów IACS
- dostawcy usług serwisowych/przegładowych
- integratorzy systemów IACS/dostawcy usług integracyjnych
- dostawcy produktów automatyki/komponentów systemów IACS

## WSPÓLPRACA W OBSZARZE CYBERBEZPIECZEŃSTWA

Aby zbudować i wdrożyć w organizacji program cyberbezpieczeństwa, należy zapewnić:

1. wsparcie ze strony najwyższego kierownictwa,
2. odpowiedni poziom finansowania,
3. wystarczające zasoby kadrowe.

U podstaw problemów z bezpieczeństwem leży brak wiedzy dotyczącej cyberzagrożeń, a programy podnoszenia świadomości i wiedzy w zakresie bezpieczeństwa są najlepszym sposobem na wzrost odporności organizacji na cyberataki.

**Urząd Dozoru Technicznego w obszarze cyberbezpieczeństwa działa dla wszystkich organizacji, które korzystają z systemów teleinformatycznych i/lub przetwarzają dane osobowe, a w szczególności dla operatorów usług kluczowych.**

**1. Audyt cyberbezpieczeństwa** w myśl ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. z 2018 r. poz. 1560) [1]

### 2. Certyfikacja

- systemów zarządzania bezpieczeństwem informacji – PN-EN ISO/IEC 27001 [3]
- systemów zarządzania ciągłością działania – PN-EN ISO 22301 [5]
- systemów zarządzania bezpieczeństwem funkcjonalnym (ang. Functional Safety Management – FSM) – PN-EN 61508 [9], PN-EN 61511 [10]

### 3. Szkolenia

Szkolenia UDT związane z audytem, certyfikacją oraz analizą zagrożeń w obszarze cyberbezpieczeństwa kierowane są zarówno do kadry zarządzającej, specjalistów odpowiedzialnych za cyberbezpieczeństwo, jak i pozostałych pracowników w organizacji.

Cyberbezpieczeństwo jest niezbędne w obszarze bezpieczeństwa publicznego, dlatego powinno być postrzegane jako celowy i zasadny wydatek. Cyberbezpieczeństwo to inwestycja. Krajowy System Cyberbezpieczeństwa nie może rozwijać się bez aktywnego zaangażowania UDT. Urząd Dozoru Technicznego posiada wykwalifikowaną kadrę, potencjał i możliwości realizacji zadań z tego obszaru. Przygotowany Framework UDT Cyber stanowi podstawę do wdrożenia strategii cyberbezpieczeństwa, która wraz z odpowiednimi mechanizmami współpracy z Operatorami Usług Kluczowych wspiera rozwój obszaru cyberbezpieczeństwa. Jest to zadanie dla UDT.

Każdy z procesów i zadań prowadzonych przez Urząd Dozoru Technicznego to powierzona jednostce sprawa ludzi, która jest realizowana z zachowaniem terminów, bezstronnie i obiektywnie, do czego między innymi zobowiązuje nas uczestnictwo w programie TIC Council, a także z poszanowaniem przepisów prawa oraz z najwyższą starannością. Poczucie misji i sensu wspierania cyberbezpieczeństwa czyni otaczający nas świat bezpieczniejszym.

#### Literatura:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 poz. 913)  
<https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230000913/U/D20230913Lj.pdf>
2. National Institute of Standards Technology, NIST Cybersecurity Framework  
<https://www.nist.gov/cyberframework>, NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
3. PN-EN ISO/IEC 27001:2023-01 - Bezpieczeństwo Informacji, cyberbezpieczeństwo i ochrona prywatności - Zabezpieczanie informacji
4. IEC 62443 - Security for Industrial Automation and Control Systems - Bezpieczeństwo w systemach sterowania i automatyki przemysłowej. Przemysłowe sieci komunikacyjne
5. PN-EN ISO 22301:2020-04 - Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania
6. Dyrektywa NIS 2 2022/2555 Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii  
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555>
7. Dyrektywa CER 2022/2557 Parlamentu Europejskiego i Rady (UE) z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych  
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2557>
8. PN-EN ISO/IEC 27002:2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Zabezpieczanie informacji
9. PN-EN 61508-1:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem -- Część 1: Wymagania ogólne
10. PN-EN 61511-1:2017-07 Bezpieczeństwo funkcjonalne -- Przynajmniej systemy bezpieczeństwa do sektora przemysłu procesowego -- Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania

