Problematyka planowanych zmian w polskim porządku prawnym w związku z wdrożeniem Dyrektywy NIS 2 w stosunku do uczelni wyższych.

Executive Summary

Kontekst i cel opracowania

Celem niniejszego raportu jest syntetyczna i realna ocena wpływu projektowanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC 2026) na funkcjonowanie uczelni wyższych w Polsce, w szczególności w kontekście zgodności z dyrektywą NIS2 oraz projektowanymi europejskimi ramami certyfikacji cyberbezpieczeństwa (CSA 2.0). Analiza obejmuje aspekty regulacyjne, organizacyjne, techniczne oraz kosztowe, ze szczególnym uwzględnieniem realiów środowiska akademickiego.

Kluczowe ustalenia

1. **Rozbieżność filozofii regulacyjnej**

   Dyrektywa NIS2 opiera się na zasadzie proporcjonalności, skalowalności i podejścia opartego na ryzyku, umożliwiając warunkowe lub dobrowolne objęcie regulacją podmiotów, których działalność ma rzeczywiste znaczenie systemowe (np. badania o charakterze odkrywczym lub strategicznym). Projekt KSC 2026 przyjmuje natomiast podejście sektorowe i administracyjne, które w praktyce prowadzi do automatycznego włączania uczelni wyższych do katalogu podmiotów „ważnych", niezależnie od ich faktycznej roli w krajowym systemie cyberodporności.

2. **Ryzyko nadregulacji („gold plating")**

Projekt KSC w wielu obszarach wykracza poza minimalne wymogi NIS2, wprowadzając dodatkowe obowiązki formalne, dokumentacyjne i operacyjne. Dotyczy to w szczególności governance, dokumentowania zgodności, zarządzania incydentami, ciągłości działania oraz relacji z dostawcami ICT. Nadregulacja ta zwiększa obciążenia administracyjne i finansowe uczelni bez proporcjonalnego wzrostu ich realnej odporności cybernetycznej.

3. **Pozorna zgodność zamiast odporności operacyjnej**

Analiza organizacyjna i techniczna (AS-IS) wskazuje, że wiele uczelni może funkcjonować obecnie w modelu reaktywnym, z fragmentarycznym zarządzaniem ryzykiem, ograniczonym monitoringiem, niespójnym zarządzaniem tożsamością IAM oraz nieprzetestowanymi planami ciągłości działania. W takim środowisku presja regulacyjna KSC sprzyja budowaniu zgodności formalnej („papierowej") zamiast inwestycjom w mierzalne zdolności wykrywania, reagowania i odtwarzania usług.

4. **Istotne i trwałe koszty wdrożeniowe**

Pełne wdrożenie wymogów KSC w aktualnie projektowanej formie oznacza dla uczelni konieczność poniesienia wysokich kosztów stałych i jednorazowych, obejmujących m.in.:

- budowę lub zakup usług SOC/SIEM/EDR,
- centralizację IAM i wdrożenie MFA/PAM,
- stałe audyty, testy bezpieczeństwa i ćwiczenia BCP/DR,

- utrzymanie „żywej” dokumentacji i dowodów operacyjnych,
- wzmocnienie zespołów cyberbezpieczeństwa lub outsourcing (vCISO). Skala tych kosztów jest porównywalna z obciążeniami sektora infrastruktury krytycznej, co jest trudne do uzasadnienia w odniesieniu do większości uczelni dydaktycznych.

5. **Niespójność z kierunkiem europejskim (CSA 2.0)**

Projektowane europejskie ramy CSA 2.0 zmierzają do harmonizacji wymagań, centralnej certyfikacji oraz ograniczenia fragmentacji regulacyjnej w UE. Krajowe rozwiązania KSC, w szczególności w zakresie łańcucha dostaw ICT i decyzji administracyjnych o charakterze natychmiastowym, mogą prowadzić do konfliktu z przyszłymi mechanizmami unijnymi i osłabienia konkurencyjności polskiego sektora nauki i technologii.

Wnioski strategiczne

- Uczelnie wyższe **nie są systemowo przygotowane** do funkcjonowania w KSC jako podmioty „ważne” w rozumieniu projektowanej ustawy, bez istotnego ryzyka nadmiernych kosztów i obciążeń organizacyjnych.
- Objęcie uczelni reżimem KSC powinno mieć **charakter fakultatywny**, zgodny z NIS2, i dotyczyć wyłącznie jednostek prowadzących badania o znaczeniu odkrywczym, eksperymentalnym lub posiadających status uczelni badawczej.
- Skuteczna poprawa cyberodporności sektora szkolnictwa wyższego wymaga **instrumentów wsparcia państwowego** (ramy referencyjne, wspólne usługi SOC, centralne wytyczne techniczne, programy kompetencyjne), a nie wyłącznie rozszerzania obowiązków ustawowych.

Konkluzja

W obecnym kształcie projekt ustawy KSC 2026 niesie istotne ryzyko nadregulacji sektora szkolnictwa wyższego. Zamiast wzmacniać realną odporność cybernetyczną, może on utrwalić model kosztownej, formalnej zgodności, nieadekwatnej do charakteru i misji uczelni. Z perspektywy strategicznej zasadne jest dostosowanie krajowych przepisów do ducha NIS2 i CSA 2.0, z zachowaniem zasady proporcjonalności, dobrowolności oraz oparcia regulacji na rzeczywistym ryzyku i dojrzałości organizacyjnej.

Problematyka planowanych zmian w polskim porządku prawnym w związku z wdrożeniem Dyrektywy NIS 2 w stosunku do uczelni wyższych.

1. Stan legislacyjny na dzień 30 stycznia 2026 r.

Celem niniejszego raportu jest szczegółowa analiza implikacji projektu nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), stanowiącej implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), dla sektora szkolnictwa wyższego i nauki w Polsce. Dokument koncentruje się na ocenie potencjalnych skutków operacyjnych i finansowych, jakie nowe przepisy niosą dla publicznych uczelni wyższych oraz instytutów badawczych. Analiza ta obejmuje swoim zakresem również elementy związane z procedowaniem samej ustawy oraz zaproponowanych rozwiązań administracyjnych, które mogą mieć znaczenie dla uczelni wyższych, gdyż zidentyfikowane w projekcie ustawy tendencje do nadregulacji wykraczają poza minimalne wymogi Dyrektywy NIS2, co grozi nałożeniem paraliżujących obciążeń na kluczowy dla innowacyjności i rozwoju Polski sektor nauki.

1.1. Aktualny status projektu ustawy:

Obecnie projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[1] (dalej: ustawa o zmianie ustawy o KSC lub nowelizacja KSC) został przekazany Prezydentowi Rzeczypospolitej Polskiej do podpisu. Treść nowelizacji KSC uległa zmianie w trakcie prac w Sejmie, natomiast Senat przyjął ostateczną wersję przepisów nowelizujących ustawę o krajowym systemie cyberbezpieczeństwa bez wnoszenia uchwalonych przez Sejm zmian na posiedzeniu w dniu 28 stycznia 2026 r.

Analizując projekt ustawy o zmianie ustawy o KSC należy podnieść na wstępie kilka istotnych kwestii prawnych związanych z procedowanymi zmianami, z uwzględnieniem również kwestii samych uczelni.

[1] druk sejmowy 1955 - https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1955

1.2. Przygotowanie nowej ustawy w zakresie KSC:

Sam projekt ustawy o zmianie ustawy o KSC wniesiony do Sejmu miał objętość 155 stron (bez uwzględnienia uzasadnienia, OSR oraz uwag do projektu), podczas gdy sama ustawa o KSC wraz z załącznikami ma obecnie objętość ok. 78 stron. Sama obszerność projektu o zmianie ustawy o KSC wskazuje, że powinna być przygotowana całkowicie nowa ustawa, a nie nowelizacja starej ustawy w myśl § 84 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2022 r. w sprawie „zasad techniki prawodawczej" na co zwracano uwagę w toku prowadzonych prac nad ustawą.[2]

Natomiast objęcie wszystkich uczelni wyższych wykracza znacznie poza ramy Dyrektywy NIS 2, która z góry nie klasyfikuje ich do żadnego z ustanowionych sektorów: czy to kluczowych, czy też ważnych. Ewentualne objęcie przepisami instytucji edukacyjnych uzależnione jest w szczególności od prowadzenia przez te podmioty działalności badawczej o krytycznym znaczeniu.

2. Ramy ustawy o Krajowym Systemie Cyberbezpieczeństwa w kontekście uczelni wyższych:

Zrozumienie nowych ram prawnych ma strategiczne znaczenie dla wszystkich podmiotów objętych regulacją. Projektowana nowelizacja KSC wprowadza fundamentalne zmiany w krajowym podejściu do cyberbezpieczeństwa, zastępując dotychczasowy model nową, dwustopniową kategoryzacją podmiotów oraz znacząco rozszerzając katalog nałożonych na nie obowiązków. Zmiany te mają na celu podniesienie ogólnego poziomu odporności na cyberzagrożenia, jednak ich skala i charakter wymagają dogłębnej oceny potencjalnych konsekwencji i realnego wpływu na funkcjonowanie sektorów objętych ustawą.

Podkreślenia wymaga, że w **obecnej treści rozdziału 5 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC)** uregulowano podstawowe obowiązki podmiotów publicznych. Dzięki temu podmioty publiczne, **w tym uczelnie wyższe**, zostały włączone do Krajowego Systemu Cyberbezpieczeństwa, którego głównym założeniem jest zapewnienie cyberbezpieczeństwa w kraju. Jednakże **zadania wskazane w podlegającej nowelizacji ustawie o KSC dotychczas skupiały się**

[2] Opinia do ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Biuro Legislacyjne, Kancelaria Senatu

głównie na udostępnianiu informacji o ew. incydentach do właściwego podmiotu tj. CSIRT MON, CSIRT NASK lub CSIRT GOV. Innymi słowy objęcie wszystkich uczelni wyższych bez żadnych wyjątków i zakwalifikowanie ich do sektora ważnego stanowi znaczą nadregulację Dyrektywy NIS 2 tj. wykraczającą swym zakresem ponad regulacje UE (tzw. „gold plating").

2.1. Udział uczelni wyższych w ustawie o Krajowym Systemie Cyberbezpieczeństwa:

Przechodząc do treści ustawy o zmianie ustawy o KSC należy wskazać dwa kluczowe obszary zmian, które obejmują uczelnie wyższe są to: obowiązki wynikające z konieczności dostosowania się do wymogów cyberbezpieczeństwa (w związku z zakwalifikowaniem uczelni wyższych jako podmioty ważne) oraz możliwe orzekanie przez organy administracji państwowej w zakresie zmiany klasyfikacji podmiotu z ważnego na kluczowy, co implikuje rozszerzenie nałożonych obowiązków w zakresie cyberbezpieczeństwa.

Pojawienie się uczelni wyższych w załączniku nr 2 ustawy o zmianie ustawy o KSC jest istotnym rozszerzeniem załącznika nr 2 do Dyrektywy NIS 2. Polski ustawodawca skorzystał z możliwości takiego rozszerzenia wskazanego w art. 2 ust 5 Dyrektywy NIS 2[3]. Zatem ujęcie wszystkich uczelni wyższych w załączniku nr 2 do ustawy o zmianie ustawy o KSC na pierwszy „rzut oka" wydaje się legalnym, lecz bardzo istotnym rozszerzeniem podmiotów objętych regulacjami Dyrektywy NIS 2. Podkreślenia wymaga, że treść załącznika nr 2 do Dyrektywy NIS 2 wskazuje, że jest ona ograniczona podmiotowo do organizacji badawczych, których definicja nie obejmuje w istocie wszystkich uczelni wyższych. Zgodnie z definicją w Dyrektywie NIS 2 "organizacja badawcza" oznacza podmiot, którego głównym celem jest prowadzenie badań stosowanych lub eksperymentalnych prac rozwojowych z myślą o wykorzystaniu wyników tych badań do celów komercyjnych, z wyłączeniem instytucji edukacyjnych[4]. Tym nie mniej polski ustawodawca postanowił skorzystać z przepisu art. 2 ust. 5 Dyrektywy NIS 2, który pozwala na zastosowanie regulacji w zakresie instytucji edukacyjnych, **zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu.** Jednakże polski ustawodawca zaproponował

[3]art. 2 ust. 5 Dyrektywy NIS 2:
„Państwa członkowskie mogą postanowić, że niniejsza dyrektywa ma zastosowanie do:
a) podmiotów administracji publicznej na poziomie lokalnym;
*b) **instytucji edukacyjnych**, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu."*
[4] Art. 6 pkt 41 Dyrektywy NIS 2

rozwiązanie, w którym bezwzględnie zobowiązał wszystkie uczelnie wyższe, bez względu na ich działalność oraz wielkość, do stosowania uregulowań związanych z przypisaniem ich do kategorii podmiotów ważnych (sektora ważnego). Ustawodawca nie badał w zasadzie jaki to ma wpływ na obowiązki i procedury, które od czasu wejścia w życie przepisów powinny być przestrzegane w uczelniach wyższych wobec objęcia ich dodatkowymi regulacjami. Nadmienić należy, że zgodnie z treścią projektowanych zmian w ustawie o krajowym systemie cyberbezpieczeństwa zostanie usunięty rozdział 5 tejże ustawy pt. „obowiązki podmiotów publicznych”[5].

Nie bez znaczenia są przepisy z art. 11 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, które wskazują, że co do zasady podstawowymi zadaniami uczelni są: prowadzenie kształcenia na studiach; prowadzenie kształcenia na studiach podyplomowych lub innych form kształcenia; prowadzenie działalności naukowej, świadczenie usług badawczych oraz transfer wiedzy i technologii do gospodarki; prowadzenie kształcenia doktorantów; kształcenie i promowanie kadr uczelni; stwarzanie osobom niepełnosprawnym warunków do pełnego udziału w: procesie przyjmowania na uczelnię w celu odbywania kształcenia, kształceniu, prowadzeniu działalności naukowej; wychowywanie studentów w poczuciu odpowiedzialności za państwo polskie, tradycję narodową, umacnianie zasad demokracji i poszanowanie praw człowieka; stwarzanie warunków do rozwoju kultury fizycznej studentów; upowszechnianie i pomnażanie osiągnięć nauki i kultury, w tym przez gromadzenie i udostępnianie zbiorów bibliotecznych, informacyjnych i archiwalnych; działanie na rzecz społeczności lokalnych i regionalnych. **W związku z tym należy wskazać, że główne zadania uczelni koncentrują się na kształceniu a nie działalności badawczej.** Zatem ustawodawca powinien mieć na uwadze przepisy Dyrektywy NIS 2 w zakresie możliwości rozszerzenia podmiotów objętych regulacjami wskazanym w art. 5, a nie traktować wszystkie podmioty jednakowo i zmuszać je do stosowania tych samych standardów bezpieczeństwa bez względu na ich wielkość, liczbę zatrudnionych osób oraz skalę działalności.

Innymi słowy jednolite potraktowanie wszystkich uczelni i instytutów jako podmiotów ważnych rażąco narusza fundamentalną zasadę proporcjonalności, prowadząc do niewspółmiernych obciążeń finansowych. Sytuacja dużego uniwersytetu technicznego, prowadzącego badania o znaczeniu strategicznym, jest

[5] art. 1 ust. 27 ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw „uchyla się rozdział 4 i 5”

nieporównywalna z sytuacją małej uczelni artystycznej, humanistycznej czy pedagogicznej. Profil ryzyka cyberbezpieczeństwa tych podmiotów, a także ich możliwości finansowe i organizacyjne, są drastycznie różne. Takie podejście legislacyjne prowadzi do obligatoryjnej, nieefektywnej alokacji ograniczonych zasobów publicznych w sektorze nauki i szkolnictwa wyższego, a w skrajnych przypadkach nawet do ograniczenia potencjału rozwojowego mniejszych, lecz wartościowych instytucji.

2.2. Kwalifikacja podmiotu jako kluczowy w ramach decyzji organu administracji:

Należy również zwrócić uwagę na możliwość zakwalifikowania uczelni wyższych, poprzez decyzję organu administracji, jako podmiot kluczowy zgodnie z proponowaną zmianą ustawy o KSC[6]. W razie wydania takiego orzeczenia administracyjnego podmiot określony jako kluczowy będzie musiał się niezwłocznie dostosować do dokonanej zmiany, bowiem z mocy prawa rozstrzygnięciu administracyjnemu jest nadawany rygor natychmiastowej wykonalności. Zatem nawet skorzystanie ze ścieżki zaskarżenia, tj. próby podważenia prawidłowości wydanej decyzji administracyjnej w przedmiocie uznania podmiotu jako kluczowy, a nie np. ważny, nie wstrzyma w czasie już nałożonych obowiązków wynikających ze zmiany klasyfikacji podmiotu z ważnego na kluczowy. Również ew. złożenie skargi do sądu administracyjnego nie sprawi, iż takiej decyzji nie będzie można wykonać. Zatem może dojść do sytuacji, w której decyzja administracyjna kwalifikująca dany podmiot jako kluczowy posiadająca rygor natychmiastowej wykonalności, po kilku miesiącach lub nawet latach zostanie uchylona, co oznaczać będzie powrót do stanu sprzed wydania takiej decyzji. Wskazana sekwencja zdarzeń może to rodzić odpowiedzialność odszkodowawczą Skarbu Państwa, bowiem zobowiązany podmiot uznany jako kluczowy może dokonać już znacznych nakładów pieniężnych związanych z dostosowaniem się do wymogów.

2.3. Niedoszacowanie kosztów KSC dla sektora badań naukowych:

Należy również zwrócić uwagę, że projekt nowej ustawy o KSC zawiera mało szczegółowe odniesienie się do kosztów jakie muszą ponieść podmioty zobowiązane do zastosowania zmian w związku z wprowadzeniem zaproponowanych treści

[6] treść art. 7l proponowanego w ustawie o zmianie ustawy o KSC.

regulacji[7]. Zabezpieczenie kosztów w zakresie szkolnictwa wyższego i nauki zostało ustalone na 2026 r. w wysokości 5 754 tys. zł[8]. Jednakże nie przedstawiono żadnych szczegółowych analiz w zakresie ustalenia powyższych kosztów i w jaki sposób stwierdzono, że taka kwota jest adekwatna do realizacji nowych zadań nałożonych na szkolnictwo wyższe[9].

2.4. Realna kontrola i audytowanie uczelni zgodne z KSC:

Ponadto mając na uwadze liczbę podmiotów podlegających nowym regulacjom w tym uczelni wyższych, których obecnie jest ok 350 w Polsce, trudno będzie kontrolować i sprawdzać wdrożenie nowych przepisów w życie przez organy kontroli (tj. Ministra ds. Cyfryzacji). Sprawdzenie przez organy państwowe nawet części podmiotów, w tym uczelni wyższych, w zakresie spełnienia nowych wymogów wprowadzonych nowelizacją ustawy o KSC jest bardzo trudne lub wręcz niemożliwe do wykonania w rozsądnym czasookresie. Sprawi to, że przepisy będą uchwalone ale ich stosowanie będzie ograniczone i zależne od wiedzy i chęci po stronie podmiotów, które do tych regulacji mają się stosować.

[7] pkt 1.6 uzasadnienia do ustawy o zmianie ustawy o KSC.
[8] treść art. 46 ust. 5 zaproponowany w ustawie o zmianie ustawy o KSC
[9] na przedmiotową kwestię również zwracała uwagę Konfederacja Rektorów Akademickich Szkół Polskich w piśmie z dnia 2 lipca 2025 r. skierowanym do Zastępcy Szefa Kancelarii Sejmu Dariusza Salamończyka

2.5. Porównanie KSC vs NIS2 w kontekście obowiązków sektora uczelni wyższych.

Obszar oceny	KSC – charakter nadregulacji (projekt 2026)	NIS2 – podejście regulacyjne	Skutki i obciążenia dla uczelni wyższych	Wnioski krytyczne (perspektywa uczelni)
Zakres podmiotowy i kategoryzacja	Rozszerzenie zakresu podmiotowego w sposób nieprecyzyjny; brak jednoznacznego rozróżnienia uczelni dydaktycznych, badawczych i projektowych; ryzyko automatycznego włączenia do kategorii „podmiotów ważnych".	Zakres sektorowy jasno określony; uczelnie objęte wyłącznie w kontekście działalności badawczej o znaczeniu krytycznym (art. 2 ust. 5 lit. b).	Wzrost obowiązków regulacyjnych bez adekwatnej analizy proporcjonalności i realnego znaczenia systemowego.	KSC narusza zasadę proporcjonalności i wykracza poza minimalną implementację NIS2 („gold plating").
Governance / odpowiedzialność kierownictwa	Formalna odpowiedzialność kierownika jednostki bez powiązania z mechanizmami realnego nadzoru, budżetowania i odpowiedzialności osobistej; nacisk na wyznaczenie „osoby odpowiedzialnej".	Wyraźne przypisanie odpowiedzialności najwyższemu kierownictwu + sankcje finansowe i obowiązek nadzoru.	Ryzyko delegowania odpowiedzialności na IT, pełnomocników lub kierowników średniego szczebla bez realnej decyzyjności.	KSC rozmywa odpowiedzialność strategiczną zamiast ją wzmacniać.

Obszar oceny	KSC – charakter nadregulacji (projekt 2026)	NIS2 – podejście regulacyjne	Skutki i obciążenia dla uczelni wyższych	Wnioski krytyczne (perspektywa uczelni)
Zarządzanie ryzykiem	Obowiązek ustawowy o charakterze ogólnym; brak wymogu ciągłości, mierzalności i integracji z decyzjami strategicznymi; nacisk na „posiadanie analizy”.	Ciągły proces risk management + ocena skuteczności środków (art. 21).	Analiza ryzyka prowadzona pod zgodność formalną, nie jako narzędzie decyzyjne.	KSC sprzyja pozornej zgodności zamiast realnego zarządzania ryzykiem.
Środki techniczne i organizacyjne	Wymogi opisowe i ogólne; szeroki margines interpretacyjny organów nadzorczych; ryzyko arbitralnej oceny.	Precyzyjny katalog obszarów środków zarządzania ryzykiem (art. 21).	Trudność w projektowaniu architektury bezpieczeństwa „pod audyt”; brak przewidywalności wymagań.	KSC utrudnia porównywalność i standaryzację wdrożeń.
Obsługa incydentów (IR)	Brak jasno zdefiniowanych mierników jakości procesu; nacisk na zgłoszenia i obowiązki formalne.	Ścisłe wymagania proceduralne + dowody działań i terminy raportowania.	Konieczność profesjonalizacji IR bez jasnych kryteriów dojrzałości.	KSC reguluje „co zgłosić”, ale nie „jak skutecznie reagować”.
Monitoring i detekcja	Brak jednoznacznego wymogu mierzalności i	Wymóg wykazywalnej odporności	Presja na kosztowne wdrożenia SIEM/EDR/MDR	KSC nie nadąża za współczesnym modelem zagrożeń opartych

Obszar oceny	KSC – charakter nadregulacji (projekt 2026)	NIS2 – podejście regulacyjne	Skutki i obciążenia dla uczelni wyższych	Wnioski krytyczne (perspektywa uczelni)
	ciągłego monitoringu; interpretacja zależna od organu.	operacyjnej i dowodów detekcji.	bez jasnej mapy proporcjonalności.	na tożsamości i lateral movement.
Ciągłość działania (BCP/DR)	Ogólny obowiązek zapewnienia ciągłości, bez obowiązku testów i ćwiczeń.	Wyraźny nacisk na BIA, RTO/RPO, testy i zarządzanie kryzysowe.	Znaczne koszty wdrożeniowe bez jednoznacznych kryteriów minimalnych.	KSC pozostaje deklaratywny i niespójny z podejściem odpornościowym UE.
Łańcuch dostaw ICT	Brak spójnych, precyzyjnych wymagań; ryzyko decyzji administracyjnych dot. dostawców.	Wyraźne uwzględnienie ryzyk dostawców i usług ICT w zarządzaniu ryzykiem.	Konieczność renegocjacji umów i wymiany infrastruktury bez harmonizacji unijnej.	KSC może prowadzić do fragmentacji rynku i ryzyk prawnych (PZP).
Świadomość i szkolenia	Wymóg działań organizacyjnych bez obowiązku oceny skuteczności.	Szkolenia i kompetencje jako pełnoprawny środek redukcji ryzyka.	Stałe programy szkoleniowe i obciążenie organizacyjne.	KSC nie tworzy mechanizmu trwałej zmiany kultury bezpieczeństwa.
Audyt i testowanie	Brak jednoznacznego obowiązku regularnych testów technicznych.	Testowanie i weryfikacja skuteczności jako standard.	Konieczność budżetowania testów i kompetencji zewnętrznych.	KSC sprzyja stagnacji technicznej i reaktywności.

Obszar oceny	KSC – charakter nadregulacji (projekt 2026)	NIS2 – podejście regulacyjne	Skutki i obciążenia dla uczelni wyższych	Wnioski krytyczne (perspektywa uczelni)
Dokumentacja i dowody zgodności	Dominacja dokumentów formalnych; ryzyko „papierowej zgodności".	Wymóg wykazania skuteczności i nadzoru (dowody operacyjne).	Znaczny wzrost prac administracyjnych i operacyjnych.	KSC promuje zgodność formalną kosztem odporności operacyjnej.

W kontekście powyższych wyznaczników należy zauważyć, że ramy regulacyjne dyrektywy NIS2 zostały zaprojektowane w celu zapewnienia **proporcjonalnego i skalowalnego podejścia do cyberbezpieczeństwa**, opartego na analizie dojrzałości organizacyjnej i technicznej podmiotu oraz rzeczywistej ocenie luk w zakresie usług informatycznych. Kluczowy nacisk położony jest na **ciągłe zarządzanie ryzykiem**, racjonalne podejście do **łańcucha dostaw ICT** oraz **skuteczność mechanizmów wykrywania, reagowania i testowania odporności** na incydenty cyberbezpieczeństwa, przy jednoczesnym uwzględnieniu wielkości, charakteru i znaczenia danego podmiotu.
Projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC 2026) przyjmuje natomiast odmienną logikę regulacyjną, w której **pierwszoplanową rolę odgrywa włączenie sektorowe oraz spełnienie obowiązków o charakterze formalno-administracyjnym**, a nie ocena realnej dojrzałości i odporności operacyjnej organizacji. W praktyce oznacza to, że objęcie uczelni wyższych reżimem KSC skutkuje **nałożeniem szerokiego katalogu obowiązków ustawowych**, niezależnie od faktycznego poziomu krytyczności ich usług informatycznych z perspektywy systemowej odporności państwa.
W konsekwencji krajowe prawodawstwo **traktuje uczelnie jako element infrastruktury o znaczeniu strategicznym dla bezpieczeństwa narodowego**, wymuszając ich realny i stały udział w realizacji celów KSC, bez pozostawienia mechanizmu samodzielnej, proporcjonalnej kwalifikacji do systemu – mechanizmu, który wprost przewiduje dyrektywa NIS2. Zakres krajowych obowiązków wynikających z KSC jest tym samym **istotnie szerszy** niż zakres wymagań, jakie mogłyby zostać nałożone w przypadku **dobrowolnej lub warunkowej kwalifikacji uczelni jako podmiotu ważnego**, zgodnie z kryteriami określonymi w NIS2

(w szczególności w odniesieniu do działalności badawczej o znaczeniu odkrywczym, eksperymentalnym lub strategicznym).
Tym samym analiza porównawcza potwierdza, że projekt ustawy KSC wprowadza elementy **nadregulacji („gold plating")**, które wykraczają poza minimalne wymogi prawa unijnego i prowadzą do zwiększenia obciążeń organizacyjnych, operacyjnych i kosztowych uczelni wyższych, bez jednoznacznego dowodu proporcjonalnego wzrostu ich realnej odporności cybernetycznej.

3. CSA 2.0 jako nowy standard europejskiej certyfikacji cyberbezpieczeństwa a niespójność z podejściem KSC:

W kontekście dynamicznych zmian w europejskim otoczeniu regulacyjnym w obszarze cyberbezpieczeństwa należy zwrócić szczególną uwagę na inicjatywę określaną jako CSA 2.0, stanowiącą rozwinięcie i istotne wzmocnienie dotychczasowych ram certyfikacji cyberbezpieczeństwa Unii Europejskiej. Proponowane rozwiązania zmierzają do stworzenia spójnego, jednolitego i obligatoryjnego systemu certyfikacji produktów, usług oraz procesów ICT wykorzystywanych na rynku europejskim[10]. W tym kontekście istnieje realne ryzyko, że część przepisów przyjmowanych w ramach krajowej ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) stanie się w krótkim horyzoncie czasowym regulacyjnie niespójna lub praktycznie niewykonalna.
Projekt CSA 2.0 zakłada szczegółowe określenie obszarów funkcjonowania cyberbezpieczeństwa na poziomie Unii Europejskiej, w tym ujednolicenie podejścia do oceny ryzyka, stosowania środków prewencyjnych, prowadzenia audytów oraz testów podatności[11]. Istotnym elementem tego podejścia jest oparcie decyzji regulacyjnych na wiedzy eksperckiej oraz doświadczeniach podmiotów odpowiedzialnych za operacyjne utrzymanie cyberbezpieczeństwa, co pozostaje w ścisłym związku z wymaganiami dyrektywy NIS2[12]. W rezultacie CSA 2.0 należy postrzegać jako narzędzie praktycznej realizacji NIS2, a nie jako odrębny, konkurencyjny akt normatywny.

---

[10] European Commission, *Proposal for a Regulation amending Regulation (EU) 2019/881 as regards managed security services (Cybersecurity Act 2.0)*, COM(2023) 209 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209
[11] European Commission, *Impact Assessment accompanying the proposal for CSA 2.0*, 2023, https://digital-strategy.ec.europa.eu
[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Na tle tych zmian obowiązujące oraz projektowane rozwiązania krajowe w ramach KSC należy ocenić krytycznie jako nadmiernie rozbudowane pod względem formalno-administracyjnym, a jednocześnie niedostosowane do rzeczywistych potrzeb wynikających z harmonizowanego prawa unijnego. KSC koncentruje się na krajowych mechanizmach decyzyjnych i administracyjnych, podczas gdy CSA 2.0 zmierza do centralizacji i unifikacji kluczowych procesów certyfikacyjnych na poziomie Unii Europejskiej. Ma to szczególne znaczenie dla sektora szkolnictwa wyższego, który zgodnie z dyrektywą NIS2 co do zasady nie jest kwalifikowany jako sektor objęty obowiązkami regulacyjnymi, z wyjątkiem instytucji prowadzących działalność badawczą o istotnym znaczeniu strategicznym[13].

CSA 2.0 wprowadza jakościową zmianę w podejściu do certyfikacji cyberbezpieczeństwa, przechodząc od dobrowolnych schematów certyfikacyjnych do modelu obligatoryjnego, obejmującego centralnie zarządzaną certyfikację produktów, usług i procesów ICT[14]. Kluczową rolę w tym systemie odgrywać ma Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), której kompetencje zostaną rozszerzone w zakresie koordynacji, nadzoru oraz wsparcia państw członkowskich[15]. Docelowo CSA 2.0 ma doprowadzić do powstania jednego, spójnego punktu odniesienia dla standardów, procedur oraz monitorowania cyberbezpieczeństwa w Unii Europejskiej, przy jednoczesnym zapewnieniu elastyczności umożliwiającej dostosowanie wymagań do dynamicznego rozwoju technologii, w szczególności w obszarach chmury obliczeniowej, sztucznej inteligencji oraz Internetu Rzeczy.

Wprowadzenie CSA 2.0 ma również na celu ograniczenie fragmentacji regulacyjnej, która obecnie wynika z nakładania się wielu aktów sektorowych oraz krajowych, prowadzących do powielania audytów, obowiązków sprawozdawczych i kosztów administracyjnych. Nowe podejście zakłada przejście do modelu zgodności opartego na certyfikacji, który ma być bardziej przejrzysty, proporcjonalny i mniej obciążający dla podmiotów objętych regulacją[16]. W tym kontekście utrzymywanie rozwiązań krajowych odbiegających od wspólnych ram europejskich może prowadzić do osłabienia konkurencyjności rynku krajowego oraz ograniczenia integracji z jednolitym rynkiem cyfrowym UE.

---

[13] Tamże, art. 2 us. 5 lit. b.
[14] European Union Agency for Cybersecurity (ENISA), *European Cybersecurity Certification Framework*, https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework
[15] European Union Agency for Cybersecurity (ENISA), *ENISA's role under the Cybersecurity Act*, https://www.enisa.europa.eu/about-enisa/regulatory-framework/legislation
[16] European Commission, *Digital Single Market – reducing regulatory fragmentation*, https://digital-strategy.ec.europa.eu

Istotnym elementem CSA 2.0 jest również nowe podejście do zarządzania ryzykiem w łańcuchu dostaw ICT. Regulacja ta rezygnuje z uproszczonych, krajowych klasyfikacji dostawców wysokiego ryzyka na rzecz skoordynowanych ocen prowadzonych na poziomie Unii Europejskiej[17]. Zgodnie z projektem CSA 2.0 inicjatywa oceny ryzyka może zostać podjęta przez Komisję Europejską lub grupę co najmniej trzech państw członkowskich i obejmować kompleksową analizę aktywów krytycznych, zagrożeń, podatności oraz scenariuszy ataku. Dopiero na tej podstawie możliwe jest zaproponowanie proporcjonalnych środków ograniczających ryzyko oraz ewentualne wprowadzenie ograniczeń w dostępie do rynku europejskiego.
W tym kontekście krajowe rozwiązania przewidziane w ustawie o KSC, oparte na jednostronnych decyzjach administracyjnych podejmowanych na poziomie państwa członkowskiego, bez spójnych procedur unijnych i jednoznacznych mechanizmów odwoławczych, należy uznać za potencjalnie sprzeczne z kierunkiem rozwoju europejskiego prawa cyberbezpieczeństwa. Takie podejście może w przyszłości prowadzić do konfliktów kompetencyjnych oraz problemów z hierarchią źródeł prawa, w szczególności w zakresie nadrzędności prawa Unii Europejskiej nad regulacjami krajowymi.
W dłuższej perspektywie utrzymywanie rozwiązań krajowych niezgodnych z CSA 2.0 może skutkować ograniczeniem współpracy polskich podmiotów z rynkiem europejskim, zmniejszeniem dostępności certyfikowanych rozwiązań ICT oraz osłabieniem konkurencyjności krajowego sektora technologicznego. Z punktu widzenia uczelni wyższych oraz instytucji badawczych oznacza to ryzyko funkcjonowania w otoczeniu regulacyjnym, które nie tylko nie wspiera realnego podnoszenia poziomu cyberbezpieczeństwa, lecz również utrudnia integrację z europejskim ekosystemem cyfrowym.

[17] European Commission, *Secure and resilient ICT supply chains*, 2023, https://digital-strategy.ec.europa.eu

4. Specyfika cyberzagrożeń w szkolnictwie wyższym

4.1. Charakter środowiska akademickiego i wpływ na realnie możliwe wdrożenie koniecznych obowiązków wynikających z sektora ważnego.

(otwartość, autonomia, rotacja użytkowników)

Środowisko akademickie charakteryzuje się wysokim stopniem otwartości informacyjnej, znaczną autonomią jednostek organizacyjnych – w tym instytutów naukowych oraz zespołów badawczych funkcjonujących w strukturach uczelni – a także dużą rotacją użytkowników. Dodatkowo uczelnie wyższe, poza działalnością dydaktyczną i badawczą, utrzymują rozbudowaną administrację niezbędną do bieżącego funkcjonowania instytucji. Zestaw tych cech w sposób istotny zwiększa poziom ryzyka cyberbezpieczeństwa oraz złożoność zarządzania bezpieczeństwem informacji. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że organizacje o rozproszonych strukturach decyzyjnych i dużej liczbie użytkowników są szczególnie podatne na incydenty cybernetyczne, zwłaszcza te oparte na socjotechnice oraz nadużyciach uprawnień[18].

Jednocześnie obowiązujące regulacje w ramach Krajowego Systemu Cyberbezpieczeństwa nie uwzględniają w wystarczającym stopniu specyfiki środowiska akademickiego, w którym autonomia wydziałów i zespołów badawczych sprzyja decentralizacji decyzji technologicznych. Brak mechanizmów wymuszających rzeczywisty, centralny nadzór nad infrastrukturą IT oraz jednoznaczne przypisanie odpowiedzialności za bezpieczeństwo informacji prowadzi do utrwalania niejednolitych standardów ochrony oraz znacząco utrudnia skuteczne reagowanie na incydenty. Najwyższa Izba Kontroli w wynikach kontroli jednostek sektora publicznego wskazuje, że rozproszona odpowiedzialność oraz brak spójnego nadzoru nad systemami informatycznymi istotnie ograniczają skuteczność działań w obszarze cyberbezpieczeństwa[19]. W praktyce podejście KSC okazuje się niedostosowane do realiów uczelni wyższych, przerzucając ciężar odpowiedzialności na struktury

[18] European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/
[19] Najwyższa Izba Kontroli,NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

organizacyjne, które nie posiadają adekwatnych narzędzi ani kompetencji decyzyjnych.

Dodatkowym czynnikiem pogłębiającym tę lukę regulacyjną jest wysoka rotacja studentów oraz pracowników czasowych, która znacząco utrudnia zarządzanie tożsamościami, kontrolę uprawnień oraz budowanie trwałej kultury bezpieczeństwa. Czynniki te, wskazywane w raportach zespołów reagowania na incydenty jako istotne źródło ryzyka, nie znajdują odpowiedniego odzwierciedlenia w wymaganiach KSC, co sprzyja utrzymywaniu jedynie formalnej, a nie operacyjnej zgodności z regulacją[20].

4.2. Typowe aktywa i dane przetwarzane w uczelni wyższej

(dane osobowe, dane badawcze, systemy krytyczne)

Uczelnie wyższe przetwarzają znaczne ilości danych osobowych oraz danych o wysokiej wartości naukowej i strategicznej, których charakter oraz skala istotnie odróżniają je od wielu innych podmiotów sektora publicznego. Obejmują one zarówno dane studentów i pracowników, jak i dane badawcze, często unikatowe, objęte zobowiązaniami kontraktowymi, grantowymi lub międzynarodowymi. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że instytucje edukacyjne należą do grupy organizacji szczególnie narażonych na incydenty skutkujące utratą poufności i dostępności danych, zwłaszcza w wyniku ataków ukierunkowanych na przejęcie tożsamości oraz dostęp do systemów informatycznych[21].
Jednocześnie regulacje w ramach Krajowego Systemu Cyberbezpieczeństwa traktują ochronę danych i aktywów informacyjnych uczelni w sposób uogólniony, nie różnicując poziomu wrażliwości danych badawczych, danych osobowych ani systemów wspierających kluczowe procesy dydaktyczne i naukowe. Brak precyzyjnego odniesienia do specyfiki aktywów przetwarzanych w środowisku akademickim powoduje, że wymagania KSC nie odzwierciedlają rzeczywistego profilu ryzyka uczelni wyższych, ograniczając się do minimalnych standardów o charakterze formalnym.
CERT Polska podkreśla, że dane osobowe użytkowników w tym np. studentów i pracowników uczelni są częstym celem ataków phishingowych oraz prób przejęcia

[20] CERT Polska, *Raport roczny o stanie cyberbezpieczeństwa w Polsce*, CERT Polska, 2024, https://cert.pl/posts/2025/04/raport-roczny-2024/

[21] European Union Agency for Cybersecurity (ENISA), *Cybersecurity for the education sector*, ENISA, 2023,https://www.enisa.europa.eu/topics/cybersecurity-education

kont, które stanowią punkt wyjścia do dalszej eskalacji ataków wewnątrz organizacji[22]. Pomimo skali tego zagrożenia KSC nie wprowadza mechanizmów wymuszających wdrażanie zaawansowanych środków ochrony tożsamości ani centralnego zarządzania dostępem, pozostawiając te decyzje w gestii poszczególnych jednostek organizacyjnych uczelni.
Szczególną kategorię aktywów stanowią systemy krytyczne w znaczeniu uczelni, takie jak systemy rekrutacyjne, dziekanatowe czy platformy e-learningowe, których dostępność warunkuje ciągłość realizacji podstawowych zadań uczelni. Najwyższa Izba Kontroli wskazuje, że niedostępność tego typu systemów w jednostkach sektora publicznego może prowadzić do paraliżu kluczowych procesów organizacyjnych[23]. W kontekście uczelni wyższych brak precyzyjnych wymagań KSC dotyczących odporności i odtwarzania systemów krytycznych skutkuje sytuacją, w której ochrona tych zasobów pozostaje niewystarczająca i niespójna, a zapewnienie ich ciągłości działania ma charakter deklaratywny, a nie operacyjny.

4.3. Dominujące wektory ataku w uczelniach wyższych

(phishing, ransomware, podatności, błędy konfiguracji)

Analiza incydentów cyberbezpieczeństwa jednoznacznie wskazuje, że dominującymi wektorami ataku w środowisku akademickim pozostają phishing oraz ransomware. CERT Polska regularnie identyfikuje phishing jako najczęściej zgłaszany typ incydentu w instytucjach publicznych, w tym w uczelniach wyższych, co bezpośrednio wynika z dużej liczby użytkowników, wysokiej rotacji oraz intensywnej komunikacji elektronicznej[24]. Charakter tych zagrożeń ma w przeważającej mierze wymiar organizacyjno-ludzki, a nie wyłącznie techniczny.
Jednocześnie regulacje w ramach Krajowego Systemu Cyberbezpieczeństwa koncentrują się w większym stopniu na spełnieniu formalnych obowiązków proceduralnych niż na adresowaniu rzeczywistych wektorów ataku dominujących w uczelniach wyższych. KSC nie różnicuje w wystarczającym stopniu wymagań w zależności od profilu zagrożeń, co w praktyce prowadzi do nadregulacji

[22] CERT Polska, *Raport roczny o stanie cyberbezpieczeństwa w Polsce*, CERT Polska, 2024, https://cert.pl/posts/2025/04/raport-roczny-2024/

[23] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf .
[24] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025, https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

dokumentacyjnej przy jednoczesnym niedoszacowaniu działań prewencyjnych, takich jak zarządzanie tożsamością, szkolenia użytkowników czy centralna detekcja zdarzeń bezpieczeństwa.
Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że ransomware stanowi jedno z najpoważniejszych zagrożeń dla organizacji silnie zależnych od dostępności systemów IT, a sektor edukacji jest szczególnie narażony ze względu na rozproszenie infrastruktury oraz ograniczone zasoby techniczne i kadrowe[25]. Pomimo tej diagnozy KSC nie wprowadza precyzyjnych, egzekwowalnych wymagań dotyczących odporności na ransomware, testowania mechanizmów odtwarzania ani mierzalnych parametrów ciągłości działania, pozostawiając te kwestie w sferze ogólnych zaleceń.
Dodatkowym, istotnym źródłem zagrożeń są znane podatności oraz błędy konfiguracji systemów informatycznych, które – jak wskazuje Najwyższa Izba Kontroli – często wynikają z braku systematycznych aktualizacji, niedoborów kadrowych oraz fragmentarycznego zarządzania infrastrukturą IT w jednostkach sektora publicznego[26]. W tym kontekście KSC nakłada na uczelnie obowiązki o charakterze szerokim i sformalizowanym, nie zapewniając jednocześnie mechanizmów wsparcia ani realnych narzędzi umożliwiających skuteczne ograniczanie podatności technicznych. Skutkuje to sytuacją, w której uczelnie obciążone są nadmiernymi wymaganiami regulacyjnymi, podczas gdy kluczowe źródła ryzyka pozostają niewystarczająco adresowane.

4.4. Zjawisko „shadow IT" i jego konsekwencje regulacyjne w kontekście KSC:

Zjawisko określane mianem „shadow IT" zostało zidentyfikowane przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) jako istotny czynnik zwiększający ryzyko cyberbezpieczeństwa w organizacjach o zdecentralizowanej strukturze decyzyjnej, do których zaliczają się uczelnie wyższe[27]. Wykorzystywanie przez wydziały i zespoły badawcze nieautoryzowanych narzędzi informatycznych oraz usług chmurowych prowadzi do utraty kontroli nad danymi, fragmentaryzacji środowiska IT oraz ograniczenia zdolności do skutecznego zarządzania bezpieczeństwem informacji.

---

[25] ENISA Threat Landscape for Ransomware Attacks (2022), https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
[26] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf .
[27] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2021, ENISA, 2021, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf.

Jednocześnie regulacje w ramach Krajowego Systemu Cyberbezpieczeństwa nie odnoszą się w sposób adekwatny do zjawiska shadow IT, traktując je pośrednio jako problem organizacyjny, bez wskazania konkretnych mechanizmów jego ograniczania. W praktyce KSC koncentruje się na spełnieniu formalnych wymagań proceduralnych, nie uwzględniając realiów środowiska akademickiego, w którym decentralizacja decyzji technologicznych jest elementem strukturalnym, a nie odstępstwem od zasad. Taka konstrukcja regulacyjna prowadzi do sytuacji, w której uczelnie ponoszą odpowiedzialność za obszary pozostające poza faktyczną kontrolą centralnych struktur IT.

Publikacje CERT Polska za 2024 r. opisują rekordową skalę incydentów i rosnącą złożoność krajobrazu zagrożeń (m.in. oszustwa, wycieki, ransomware), co podnosi wymagania dla reagowania na incydenty i widoczności środowiska IT; raport nie używa pojęcia *shadow IT*, ale kontekst operacyjny (liczba i różnorodność zdarzeń) wzmacnia wagę pełnej inwentaryzacji zasobów i przepływów danych w organizacjach publicznych i akademickich[28]. **ENISA** w swoich materiałach i wytycznych wdrożeniowych do NIS2 **wprost** rekomenduje utrzymywanie inwentaryzacji aktywów (sprzętu, oprogramowania i danych), kontrolę usług chmurowych oraz zarządzanie ryzykiem łańcucha dostaw i „nieautoryzowanych" rozwiązań — co jest kluczowe dla skutecznego **incident response** i ograniczania ryzyka *shadow IT*[29]. Jednocześnie **ustawa o krajowym systemie cyberbezpieczeństwa (KSC)** nakłada ogólny obowiązek zarządzania ryzykiem i reagowania na incydenty, ale **nie wprowadza literalnych, szczegółowych wymogów** prowadzenia inwentaryzacji zasobów IT lub centralnej kontroli usług chmurowych — co w praktyce przerzuca na podmioty (w tym uczelnie) ciężar zdefiniowania i wdrożenia tych mechanizmów organizacyjnych[30]. W efekcie, w uczelniach **brak pełnej widoczności zasobów i usług (shadow IT)** utrudnia klasyfikację zdarzeń, priorytetyzację incydentów i odtwarzanie zdolności działania, a konsekwencje obejmują nie tylko koszty techniczne, lecz także

[28] CERT Polska, *Raport roczny z działalności CERT Polska w 2024 roku*, NASK – Państwowy Instytut Badawczy, Warszawa 2025. [ops.pl]
[29] ENISA, *Technical Implementation Guidance on NIS2 Cybersecurity Risk-Management Measures*, Version 1.0, June 2025. [enisa.europa.eu]
ENISA, *Incident management* (strona tematyczna). [enisa.europa.eu]
ENISA, *Cloud Security Guide for SMEs* (2015). [enisa.europa.eu]

[30] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, **tekst jednolity**: Dz.U. 2026 poz. 20 / Dz.U. 2024 poz. 1077. [infor.pl], [api.sejm.gov.pl]

koszty organizacyjne i reputacyjne (np. opóźnienia w projektach, ryzyko utraty partnerów i finansowania), co jest spójne z trendami ryzyka opisywanymi w raportach ENISA o zagrożeniach i ich wpływie na sektor publiczny[31].

W konsekwencji KSC, zamiast wspierać redukcję ryzyka wynikającego z niekontrolowanego wykorzystania technologii informatycznych, przyczynia się do utrwalenia luki pomiędzy formalną zgodnością regulacyjną a rzeczywistym poziomem bezpieczeństwa operacyjnego w uczelniach wyższych.

4.5. Konsekwencje incydentów cyberbezpieczeństwa dla misji uczelni:

(dydaktyka, badania, reputacja, finanse)

Incydenty cyberbezpieczeństwa mogą prowadzić do istotnych i długotrwałych zakłóceń w realizacji podstawowej misji uczelni wyższych, obejmującej działalność dydaktyczną, badawczą oraz funkcje administracyjne. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że współczesne cyberataki — zwłaszcza ransomware oraz ataki na dostępność charakteryzują się wysokim wpływem prowadząc do poważnych zakłóceń działania organizacji, naruszeń integralności danych oraz ograniczenia dostępności usług, a ich skutki mogą być długotrwałe, o charakterze „high impact, low recovery", ze względu na rosnącą destrukcyjność i relatywnie niską zdolność organizacji szczególnie w obszarze edukacyjnym do szybkiego powrotu do stanu sprzed incydentu, wpływając jednocześnie na dostępność systemów, integralność danych oraz zaufanie interesariuszy[32].
W tym kontekście podejście przyjęte w Krajowym Systemie Cyberbezpieczeństwa należy ocenić krytycznie, gdyż regulacja ta koncentruje się głównie na nałożeniu obowiązków formalnych po stronie podmiotów objętych systemem, nie oferując jednocześnie adekwatnych mechanizmów wsparcia dla instytucji realizujących zadania o charakterze publicznym i misyjnym, takich jak uczelnie wyższe. KSC nie uwzględnia specyfiki skutków incydentów cyberbezpieczeństwa dla procesów dydaktycznych i badawczych, traktując je w sposób porównywalny z innymi

[31] ENISA, *Threat Landscape – strona tematyczna (ETL 2024/2025)*. [enisa.europa.eu]
[32] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, ENISA, 2022,

usługami publicznymi, mimo że ich zakłócenie może prowadzić do nieodwracalnych strat naukowych, opóźnień projektów badawczych oraz utraty pozycji konkurencyjnej uczelni.

Najwyższa Izba Kontroli wskazuje, że niewystarczające przygotowanie jednostek sektora publicznego do reagowania na incydenty cyberbezpieczeństwa może prowadzić do istotnych zakłóceń organizacyjnych, w tym przerw w realizacji zadań publicznych oraz obniżenia skuteczności działania instytucji. W dłuższej perspektywie konsekwencje te mogą pośrednio wpływać na sytuację finansową jednostek oraz ich postrzeganie przez interesariuszy[33]. W przypadku uczelni wyższych skutki te mogą obejmować spadek zainteresowania kandydatów, utratę partnerów naukowych oraz ograniczenie możliwości pozyskiwania środków zewnętrznych.

Z perspektywy systemowej brak w KSC instrumentów wspierających odporność operacyjną uczelni należy uznać za istotną lukę regulacyjną. Alternatywą dla obecnego podejścia mogłoby być wprowadzenie przez państwo komplementarnych środków organizacyjnych, takich jak dedykowane programy wsparcia finansowego dla sektora szkolnictwa wyższego w obszarze cyberbezpieczeństwa, centralne usługi bezpieczeństwa (np. sektorowe centra monitoringu lub reagowania na incydenty), a także mechanizmy doradcze i szkoleniowe adresowane do kadry zarządzającej uczelniami. Rozwiązania tego typu, rekomendowane w dokumentach ENISA oraz częściowo implementowane w ramach dyrektywy NIS2, pozwalałyby na realne ograniczenie skutków incydentów cyberbezpieczeństwa, zamiast przerzucania pełnej odpowiedzialności na instytucje, które nie dysponują porównywalnymi zasobami do podmiotów komercyjnych.

[33] Najwyższa Izba Kontroli, https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/cyberbezpieczenstwo-w-samorzadach-2025.html

4.6. Mapowanie zagrożeń na ryzyka cyberbezpieczeństwa dla uczelni wyższych.

(Tabela integrująca analizę jakościową z analizą ryzyka – element metodologiczny pracy)

Zagrożenie	**Źródło zagrożenia**	**Aktywa narażone**	**Ryzyko**	**Potencjalny wpływ**	**Przykładowa kategoria ryzyka**
Phishing	Czynniki ludzkie, socjotechnika	Konta użytkowników, poczta	Przejęcie tożsamości, eskalacja uprawnień	Dostęp nieautoryzowany, wycieki danych	Operacyjne / informacyjne
Ransomware	Złośliwe oprogramowanie	Systemy krytyczne, dane	Niedostępność systemów	Paraliż dydaktyki i administracji	Ciągłość działania
Niezałatane podatności	Brak aktualizacji	Serwery, aplikacje	Nieautoryzowany dostęp	Naruszenie poufności i integralności	Techniczne
Błędy konfiguracji	Brak standardów	Systemy chmurowe, sieci	Ekspozycja usług	Wycieki danych, dostęp zewnętrzny	Techniczne
Shadow IT	Autonomia jednostek	Dane badawcze, dane osobowe	Brak kontroli nad danymi	Naruszenia regulacyjne	Organizacyjne / prawne
Brak świadomości użytkowników	Niedostateczne szkolenia	Wszystkie aktywa	Eskalacja incydentów	Zwiększona skuteczność ataków	Organizacyjne
Brak monitoringu	Niedojrzałość techniczna	Infrastruktura IT	Opóźnione wykrycie incydentu	Wzrost skali szkód	Operacyjne

Powyższa tabela stanowi pomost pomiędzy analizą jakościową zagrożeń a analizą ryzyka cyberbezpieczeństwa. Pozwala ona na systematyczne przełożenie identyfikowanych zagrożeń na konkretne ryzyka, które następnie mogą zostać ocenione pod względem prawdopodobieństwa i wpływu.

5. Analiza stanu obecnego (AS-IS) cyberbezpieczeństwa w uczelniach wyższych – ujęcie organizacyjne i zarządcze

5.1. Rola governance w systemie cyberbezpieczeństwa uczelni wyższej:

Zarządzanie cyberbezpieczeństwem w uczelniach wyższych powinno być analizowane w kontekście koncepcji *cybersecurity governance*, rozumianej jako zbiór struktur organizacyjnych, procesów decyzyjnych oraz mechanizmów nadzoru zapewniających, że ryzyka cybernetyczne są identyfikowane, oceniane i zarządzane na poziomie adekwatnym do ich wpływu na realizację misji instytucji. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że brak jednoznacznego umocowania cyberbezpieczeństwa w strukturach zarządczych stanowi jedną z głównych przyczyn niskiej dojrzałości systemów bezpieczeństwa w sektorze publicznym, w tym w instytucjach edukacyjnych, które podlegają tym samym wyzwaniom organizacyjnym [34].

W tym kontekście podejście przyjęte w Krajowym Systemie Cyberbezpieczeństwa należy ocenić krytycznie. Regulacja ta formalnie przypisuje obowiązki w obszarze cyberbezpieczeństwa kierownikowi jednostki, jednak nie wprowadza skutecznych mechanizmów wymuszających rzeczywiste zaangażowanie najwyższego kierownictwa w proces zarządzania ryzykiem cyberbezpieczeństwa. W praktyce KSC sprzyja utrzymaniu modelu, w którym cyberbezpieczeństwo pozostaje zagadnieniem technicznym, delegowanym do działów IT, bez systematycznego nadzoru strategicznego oraz bez integracji z ogólnym systemem zarządzania uczelnią.

Taki stan rzeczy pozostaje w wyraźnej sprzeczności z podejściem przyjętym w dyrektywie NIS2, która jednoznacznie akcentuje odpowiedzialność najwyższego kierownictwa za nadzór nad cyberbezpieczeństwem, w tym obowiązek zatwierdzania

[34] European Union Agency for Cybersecurity (ENISA), *Cybersecurity governance*, ENISA, 2023, https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies

środków zarządzania ryzykiem, monitorowania ich skuteczności oraz ponoszenia konsekwencji w przypadku zaniedbań[35]. NIS2, w przeciwieństwie do KSC, przesuwa ciężar odpowiedzialności z poziomu operacyjnego na poziom strategiczny, wzmacniając rolę governance jako kluczowego elementu odporności organizacyjnej.
Analogiczne podejście prezentowane jest w normie ISO/IEC 27001, która wymaga aktywnego zaangażowania najwyższego kierownictwa w ustanawianie polityki bezpieczeństwa informacji, zapewnienie zasobów oraz nadzór nad funkcjonowaniem systemu zarządzania bezpieczeństwem informacji[36]. Brak zbieżności pomiędzy wymaganiami KSC a standardami międzynarodowymi i regulacjami unijnymi prowadzi do sytuacji, w której uczelnie wyższe funkcjonują w stanie formalnej zgodności z przepisami krajowymi, nie osiągając jednocześnie poziomu dojrzałości governance niezbędnego do skutecznego zarządzania ryzykiem cyberbezpieczeństwa.

5.2. Odpowiedzialność kierownictwa uczelni za cyberbezpieczeństwo – ograniczona skuteczność podejścia KSC:

Zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa odpowiedzialność za realizację obowiązków w zakresie cyberbezpieczeństwa została formalnie przypisana kierownikowi jednostki, obejmując zapewnienie środków organizacyjnych i technicznych oraz nadzór nad ich funkcjonowaniem[37]. Konstrukcja ta ma jednak w przeważającej mierze charakter deklaratywny i nie jest poparta mechanizmami egzekwowania, które realnie wymuszałyby zaangażowanie najwyższego kierownictwa uczelni w zarządzanie ryzykiem cyberbezpieczeństwa.
Najwyższa Izba Kontroli wskazuje, że w wielu jednostkach sektora publicznego decyzje dotyczące bezpieczeństwa informatycznego podejmowane są na poziomie operacyjnym, bez udziału kierownictwa najwyższego szczebla, co prowadzi do

[35] 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 (NIS2), art. 20–21, https://eur-lex.europa.eu/eli/dir/2022/2555/oj .
[36] ISO/IEC 27001:2022, *Information Security Management Systems – Requirements*, International Organization for Standardization, 2022, https://www.iso.org/standard/27001

[37] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560 z późn. zm., https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

fragmentarycznego i reaktywnego podejścia do cyberbezpieczeństwa[38]. W praktyce oznacza to, że obowiązek przypisany kierownikowi jednostki w KSC rzadko przekłada się na rzeczywiste działania strategiczne, a cyberbezpieczeństwo nie jest traktowane jako ryzyko porównywalne z ryzykiem finansowym, prawnym czy reputacyjnym.

Ograniczona skuteczność Krajowego Systemu Cyberbezpieczeństwa w obszarze odpowiedzialności kierownictwa nie wynika z niskiego poziomu sankcji, lecz z ich konstrukcji oraz oderwania od realnego modelu zarządzania cyberbezpieczeństwem. W aktualnych i projektowanych przepisach KSC przewidziano kary administracyjne, które w wielu przypadkach są **surowsze niż sankcje wynikające z dyrektywy NIS2**, zarówno pod względem maksymalnej wysokości, jak i zakresu podmiotowego ich stosowania. Kary te mogą być nakładane bezpośrednio na podmioty publiczne, w tym uczelnie wyższe, a także na osoby pełniące funkcje kierownicze, co formalnie tworzy jeden z najbardziej restrykcyjnych reżimów sankcyjnych w obszarze cyberbezpieczeństwa w Unii Europejskiej.

Paradoksalnie jednak, mimo wysokiego poziomu sankcji, KSC nie buduje spójnego i dojrzałego modelu odpowiedzialności zarządczej. Sankcje mają charakter **represyjny i administracyjny**, a nie systemowy, i nie są powiązane z jasno zdefiniowanymi obowiązkami governance, mierzalnymi kryteriami należytej staranności ani obowiązkiem zatwierdzania i nadzorowania strategii zarządzania ryzykiem cyberbezpieczeństwa na poziomie kierownictwa. W rezultacie wysokie kary funkcjonują w oderwaniu od mechanizmów decyzyjnych, które umożliwiałyby kierownictwu uczelni realne i świadome zarządzanie ryzykiem.

Dla porównania dyrektywa NIS2, mimo że w wielu przypadkach przewiduje **niższe maksymalne progi sankcji finansowych**, wprowadza zasadniczo odmienną logikę odpowiedzialności. NIS2 jednoznacznie wiąże odpowiedzialność kierownictwa z obowiązkiem zatwierdzania środków zarządzania ryzykiem cyberbezpieczeństwa, zapewnienia zasobów oraz sprawowania stałego nadzoru nad skutecznością wdrożonych rozwiązań. Sankcje w NIS2 pełnią funkcję wtórną wobec modelu governance, którego celem jest wymuszenie strategicznego, a nie reaktywnego podejścia do cyberbezpieczeństwa.

W konsekwencji w środowisku uczelni wyższych KSC prowadzi do sytuacji, w której kierownictwo formalnie ponosi wysoką odpowiedzialność sankcyjną, nie dysponując jednocześnie jasnymi ramami decyzyjnymi, wskaźnikami skuteczności ani

[38] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf .

systemowym wsparciem organizacyjnym. Taki model zwiększa ryzyko odpowiedzialności prawnej bez proporcjonalnej możliwości jej realnego zarządzania, co odróżnia KSC od podejścia przyjętego w NIS2, gdzie ciężar regulacyjny przesunięty jest z sankcji na **dojrzałość procesów, odpowiedzialność zarządczą i udokumentowaną należytą staranność**.

5.3. Struktura organizacyjna cyberbezpieczeństwa w uczelni wyższej – ograniczenia podejścia KSC:

Analiza stanu obecnego funkcjonowania uczelni wyższych wskazuje, że struktura organizacyjna cyberbezpieczeństwa jest w tym sektorze silnie zróżnicowana. Część uczelni posiada wyodrębnione role lub komórki odpowiedzialne za bezpieczeństwo informacji, jednak w wielu przypadkach zadania te realizowane są w sposób rozproszony i niesformalizowany, najczęściej przez działy IT, administratorów systemów informatycznych oraz inspektorów ochrony danych. Taki model organizacyjny nie musi wynikać z zaniedbań po stronie uczelni, lecz jest często konsekwencją braku jednoznacznych wymagań strukturalnych w obowiązujących regulacjach krajowych.
W tym kontekście podejście przyjęte w Krajowym Systemie Cyberbezpieczeństwa należy ocenić krytycznie. KSC nakłada na kierownika jednostki szeroką odpowiedzialność za realizację obowiązków w obszarze cyberbezpieczeństwa, nie definiując jednak minimalnych wymogów dotyczących struktury organizacyjnej, ról decyzyjnych ani relacji kompetencyjnych pomiędzy funkcjami technicznymi, prawnymi i zarządczymi. W praktyce pozostawia to uczelniom znaczną swobodę interpretacyjną, która sprzyja utrwalaniu modeli fragmentarycznych, opartych na doraźnym podziale zadań, zamiast na systemowym zarządzaniu ryzykiem.
Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) wskazuje, że skuteczne zarządzanie cyberbezpieczeństwem wymaga **jasno zdefiniowanych ról organizacyjnych i kompetencyjnych**, obejmujących m.in. **właścicieli ryzyka, funkcję koordynacyjną w obszarze cyberbezpieczeństwa oraz wyspecjalizowane zespoły reagowania na incydenty**, które powinny być **trwale osadzone w strukturach decyzyjnych organizacji oraz powiązane z procesami zarządzania ryzykiem i nadzoru**[39]. Brak takich ról prowadzi do rozmycia odpowiedzialności, konfliktów kompetencyjnych oraz trudności w podejmowaniu decyzji o charakterze strategicznym, zwłaszcza w sytuacjach kryzysowych.

[39] European Union Agency for Cybersecurity (ENISA), European Cybersecurity Skills Framework – Role Profiles, ENISA, 2022, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Pomimo tej diagnozy KSC nie wprowadza mechanizmów, które wymuszałyby budowę spójnych struktur cyberbezpieczeństwa w uczelniach wyższych. Regulacja koncentruje się na obowiązkach formalnych i sprawozdawczych, nie adresując wprost problemu rozproszenia odpowiedzialności organizacyjnej. W rezultacie nawet uczelnie podejmujące działania w zakresie cyberbezpieczeństwa mogą funkcjonować w modelu, w którym odpowiedzialność operacyjna, decyzyjna i nadzorcza pozostaje niejednoznaczna.
Konsekwencją takiego podejścia jest dominacja działań reaktywnych nad planowymi, ograniczona zdolność do długofalowego zarządzania ryzykiem oraz utrudniona integracja cyberbezpieczeństwa z procesami zarządczymi uczelni. W tym sensie KSC, zamiast wspierać profesjonalizację struktur cyberbezpieczeństwa w szkolnictwie wyższym, utrwala stan organizacyjnej niejednorodności, który stoi w sprzeczności z rekomendacjami ENISA oraz kierunkiem rozwoju regulacji unijnych, w szczególności dyrektywy NIS2.

5.4. Zarządzanie ryzykiem cyberbezpieczeństwa – podejście organizacyjne a praktyka KSC:

Zarządzanie ryzykiem cyberbezpieczeństwa stanowi fundament skutecznego systemu ochrony informacji i powinno mieć charakter ciągły, udokumentowany oraz powiązany z celami organizacyjnymi. Norma ISO/IEC 27005 wskazuje, że proces zarządzania ryzykiem powinien obejmować regularną identyfikację zagrożeń, ocenę ich wpływu oraz dostosowywanie środków ochrony do zmieniającego się otoczenia ryzyka[40]. W ujęciu normatywnym ryzyko cyberbezpieczeństwa stanowi element systemowego zarządzania organizacją, a nie jednorazowe ćwiczenie dokumentacyjne. W praktyce uczelni wyższych oraz innych podmiotów sektora publicznego proces analizy ryzyka cyberbezpieczeństwa bywa jednak realizowany głównie w celu spełnienia wymogów formalnych wynikających z obowiązujących regulacji, w tym Krajowego Systemu Cyberbezpieczeństwa. KSC nie precyzuje w sposób jednoznaczny wymagań dotyczących cykliczności, metodologii ani integracji analizy ryzyka z procesami decyzyjnymi i budżetowymi. W efekcie analiza ryzyka może być prowadzona jednorazowo lub okresowo wyłącznie na potrzeby wykazania formalnej zgodności z przepisami, bez realnego wpływu na dobór środków technicznych i organizacyjnych.

[40] ISO/IEC 27005:2022, *Information security risk management*, International Organization for Standardization, https://www.iso.org/standard/80585.html .

CERT Polska, analizując rosnącą złożoność i dynamikę incydentów cyberbezpieczeństwa, podkreśla konieczność dostosowywania mechanizmów ochronnych do stale ewoluujących technik ataków oraz zmieniającego się środowiska zagrożeń[41]. W przypadku uczelni wyższych wyzwanie to jest szczególnie istotne ze względu na wysoki poziom rozproszenia organizacyjnego oraz dynamiczne, hybrydowe środowisko IT, które wymagają podejścia opartego na ciągłym monitorowaniu ryzyka, podatności i procesów bezpieczeństwa, a nie na statycznych dokumentach czy jednorazowej ocenie ryzyka
Organizacyjnie skutkiem administracyjno-proceduralnego podejścia do zarządzania ryzykiem, utrwalanego przez konstrukcję KSC, jest brak powiązania ryzyka cyberbezpieczeństwa z kluczowymi procesami zarządczymi uczelni, w szczególności z planowaniem inwestycji, alokacją zasobów oraz ustalaniem priorytetów strategicznych. Ryzyko cybernetyczne funkcjonuje wówczas jako odrębny byt dokumentacyjny, a nie jako czynnik wpływający na decyzje kierownictwa.
W tym sensie KSC sprzyja utrzymywaniu modelu zgodności formalnej, w którym głównym celem jest posiadanie wymaganej dokumentacji, a nie realne zarządzanie ryzykiem. Model ten pozostaje w sprzeczności zarówno z podejściem normatywnym ISO/IEC 27005, jak i z kierunkiem wyznaczonym przez dyrektywę NIS2, która jednoznacznie akcentuje konieczność ciągłego, mierzalnego i zintegrowanego zarządzania ryzykiem cyberbezpieczeństwa na poziomie organizacyjnym.

5.5. Zarządzanie zasobami ludzkimi i kompetencjami – kosztowe konsekwencje wdrożenia KSC w uczelniach wyższych:

Kompetencje personelu stanowią jeden z kluczowych czynników determinujących poziom cyberbezpieczeństwa organizacji. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że niedobór wykwalifikowanych specjalistów oraz brak systematycznych szkoleń użytkowników końcowych istotnie zwiększają skuteczność ataków socjotechnicznych i obniżają zdolność organizacji do reagowania na incydenty[42]. Problem ten ma charakter strukturalny i dotyczy w szczególności sektora publicznego oraz instytucji edukacyjnych.

[41] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025,

https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

[42] European Union Agency for Cybersecurity (ENISA), 2024 Report on the State of Cybersecurity in the Union, ENISA, 3 Dec 2024,

W uczelniach wyższych niedobory kompetencyjne są dodatkowo potęgowane przez ograniczenia budżetowe oraz silną konkurencję ze strony sektora komercyjnego, który oferuje znacznie wyższe wynagrodzenia dla specjalistów ds. cyberbezpieczeństwa. W rezultacie bezpieczeństwo systemów informatycznych uczelni bywa uzależnione od wiedzy i dostępności pojedynczych administratorów, przy jednoczesnym braku planów sukcesji kompetencyjnej oraz formalnych ścieżek rozwoju kadr w obszarze cyberbezpieczeństwa.

Wprowadzenie i egzekwowanie wymagań Krajowego Systemu Cyberbezpieczeństwa w aktualnym kształcie istotnie zwiększa presję na budowę wewnętrznych struktur kadrowych, niezależnie od rzeczywistej skali ryzyka i specyfiki działalności uczelni. KSC nie przewiduje elastycznych modeli spełniania wymagań kompetencyjnych, co w praktyce oznacza konieczność zatrudnienia dedykowanego zespołu cyberbezpieczeństwa, obejmującego co najmniej pełnomocnika ds. cyberbezpieczeństwa (CISO lub równoważną funkcję), specjalistów ds. bezpieczeństwa operacyjnego oraz osoby odpowiedzialne za zgodność i raportowanie.

Szacunkowy koszt utrzymania minimalnego, wewnętrznego zespołu cyberbezpieczeństwa w uczelni wyższej można określić na poziomie:

- **pełnomocnik ds. cyberbezpieczeństwa (CISO / Pełnomocnik KSC)**: 18–25 tys. PLN brutto miesięcznie (216–300 tys. PLN rocznie),
- **2–3 specjalistów ds. cyberbezpieczeństwa / bezpieczeństwa IT**: 12–18 tys. PLN brutto miesięcznie każdy (łącznie ok. 300–600 tys. PLN rocznie),
- **koszty pośrednie (szkolenia, certyfikacje, absencje, rotacja, zastępstwa)**: ok. 20–30% kosztów osobowych.

Łączny roczny koszt takiego podstawowego zespołu kształtuje się na poziomie **700 tys. – 1,1 mln PLN**, przy czym są to koszty stałe, niezależne od faktycznej liczby incydentów czy skali zagrożeń. Dla wielu uczelni publicznych oznacza to istotne i długoterminowe obciążenie budżetowe, które konkuruje bezpośrednio z finansowaniem działalności dydaktycznej i badawczej.

Alternatywą dla modelu etatowego jest wykorzystanie usług zewnętrznych, takich jak **vCISO (Virtual CISO)** oraz zarządzane usługi cyberbezpieczeństwa. Koszt takiego rozwiązania, obejmującego dostęp do doświadczonego eksperta, wsparcie w obszarze governance, zarządzania ryzykiem, zgodności regulacyjnej oraz koordynacji reagowania na incydenty, szacowany jest na poziomie **150–300 tys. PLN rocznie**,

https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

w zależności od zakresu usług i wielkości organizacji. Model ten pozwala na elastyczne dostosowanie poziomu wsparcia do rzeczywistych potrzeb uczelni, bez konieczności ponoszenia pełnych kosztów zatrudnienia specjalistów na etat.
W aktualnym kształcie KSC nie promuje jednak proporcjonalnego i ryzyko -zorientowanego podejścia do zarządzania kompetencjami, preferując rozwiązania organizacyjne oparte na stałych strukturach i formalnym przypisaniu odpowiedzialności. Skutkuje to sytuacją, w której uczelnie wyższe zmuszone są ponosić wysokie, stałe koszty kadrowe, nie zawsze przekładające się na adekwatny wzrost poziomu cyberbezpieczeństwa. Taki model należy ocenić krytycznie, zwłaszcza w kontekście kierunku wyznaczanego przez regulacje unijne, które coraz wyraźniej akcentują proporcjonalność, zarządzanie ryzykiem oraz możliwość korzystania z usług wspólnych i zewnętrznych zamiast rozbudowywania kosztownych struktur wewnętrznych.

5.6. Polityki, procedury i dokumentacja bezpieczeństwa – koszt i skutki nadregulacji KSC:

Formalne dokumenty bezpieczeństwa, takie jak polityki, regulaminy oraz procedury, stanowią istotny element systemu zarządzania cyberbezpieczeństwem. Norma ISO/IEC 27001 jednoznacznie wskazuje jednak, że dokumentacja powinna odzwierciedlać rzeczywiste procesy organizacyjne oraz być wspierana przez ich faktyczne wdrożenie, egzekwowanie i cykliczną aktualizację[43]. Dokumentacja bezpieczeństwa nie powinna zatem pełnić wyłącznie funkcji deklaratywnej, lecz stanowić element „żywego" systemu zarządzania.
Najwyższa Izba Kontroli zwraca uwagę, że w wielu jednostkach sektora publicznego dokumentacja bezpieczeństwa ma charakter formalny i nie znajduje realnego odzwierciedlenia w praktyce operacyjnej[44]. Zjawisko to jest w dużej mierze konsekwencją regulacyjnego nacisku na posiadanie dokumentów, a nie na mierzalną skutecznością wdrożonych mechanizmów ochronnych.
W kontekście Krajowego Systemu Cyberbezpieczeństwa problem ten ulega istotnemu pogłębieniu w przypadku uczelni wyższych, które – ze względu na prowadzoną działalność badawczą – mogłyby zostać zakwalifikowane jako podmioty ważne. W takim scenariuszu uczelnia byłaby zobowiązana do utrzymywania rozbudowanej, aktualnej i audytowalnej dokumentacji obejmującej cały cykl życia bezpieczeństwa

[43] ISO/IEC 27001:2022, *Information Security Management Systems – Documentation requirements*, International Organization for Standardization, https://www.iso.org/standard/27001
[44] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

informacji: od zarządzania ryzykiem, przez ciągłość działania, obsługę incydentów, zarządzanie dostawcami, aż po szkolenia i świadomość użytkowników. Dokumentacja ta musiałaby być nie tylko opracowana, lecz również stale aktualizowana, wersjonowana i powiązana z dowodami operacyjnymi.
Utrzymanie tzw. „żywej dokumentacji" w reżimie KSC oznacza w praktyce przyspieszenie i sformalizowanie procesów w całej organizacji. Każdy proces biznesowy i techniczny musi mieć przypisanego właściciela, jasno określone role, mierniki skuteczności oraz powiązanie z analizą ryzyka. Dodatkowo konieczne staje się wdrożenie narzędzi wspierających zarządzanie dokumentacją, zgodnością i audytami, umożliwiających bieżące monitorowanie realizacji obowiązków oraz przygotowanie organizacji do cyklicznych kontroli.
Szacunkowy roczny koszt utrzymania takiego zakresu dokumentacji i zgodności w uczelni wyższej, przy założeniu obowiązkowych audytów zgodności KSC, obejmuje:

- **zasoby kadrowe (koordynacja, właściciele procesów, wsparcie prawne i IT)**: 250–400 tys. PLN,
- **narzędzia GRC / compliance / zarządzania dokumentacją**: 80–150 tys. PLN,
- **audyty zewnętrzne, testy zgodności, przygotowanie do kontroli**: 120–250 tys. PLN,
- **szkolenia, warsztaty, aktualizacja procedur i materiałów**: 50–100 tys. PLN.

Łączny koszt roczny utrzymania „żywej" dokumentacji w reżimie KSC można zatem oszacować na poziomie **500–900 tys. PLN**, przy czym są to koszty stałe, niezależne od rzeczywistej liczby incydentów czy skali zagrożeń.
Dla porównania podejście wynikające z dyrektywy NIS2, choć również wymaga dokumentowania działań, ma charakter bardziej deklaratywny i proporcjonalny, kładąc nacisk na wykazanie skuteczności zarządzania ryzykiem, a nie na szczegółową rozbudowę dokumentacji procesowej. NIS2 dopuszcza większą elastyczność w doborze formy i zakresu dokumentacji, co pozwala organizacjom – w tym uczelniom wyższym – dostosować poziom formalizacji do rzeczywistej skali ryzyka.
W konsekwencji KSC, w aktualnym kształcie, prowadzi do istotnego wzrostu kosztów organizacyjnych i administracyjnych po stronie uczelni wyższych, nieproporcjonalnego do osiąganych efektów w zakresie realnego podniesienia poziomu cyberbezpieczeństwa. Nadmierna koncentracja na dokumentacji i audytowalności sprzyja spełnianiu wymogów formalnych, jednocześnie ograniczając elastyczność organizacyjną oraz zdolność uczelni do reagowania na dynamicznie zmieniające się zagrożenia.

5.7. Zarządzanie dostawcami i usługami ICT – konsekwencje nadregulacji KSC dla uczelni wyższych:

Współczesne uczelnie wyższe w coraz większym stopniu opierają realizację kluczowych procesów dydaktycznych, badawczych i administracyjnych na zewnętrznych dostawcach usług ICT, w tym na usługach chmurowych, rozwiązaniach sieciowych, platformach e-learningowych oraz specjalistycznym oprogramowaniu badawczym. Europejska Agencja ds. Cyberbezpieczeństwa wskazuje, że ryzyko łańcucha dostaw stanowi jedno z kluczowych wyzwań współczesnego cyberbezpieczeństwa, wymagające podejścia opartego na analizie ryzyka, proporcjonalności oraz przejrzystych kryteriach oceny dostawców[45].
W praktyce uczelni wyższych zarządzanie ryzykiem dostawców ICT bywa jednak ograniczone do zapisów umownych o charakterze ogólnym, bez precyzyjnych wymagań dotyczących bezpieczeństwa, obsługi incydentów, audytów czy odpowiedzialności za naruszenia. Problem ten nie wynika wyłącznie z zaniedbań po stronie uczelni, lecz również z braku jednoznacznych, proporcjonalnych i stabilnych ram regulacyjnych dostosowanych do realiów sektora publicznego i akademickiego.
W tym kontekście podejście przyjęte w Krajowym Systemie Cyberbezpieczeństwa należy ocenić krytycznie. KSC wprowadza mechanizmy administracyjne umożliwiające kwestionowanie lub wykluczanie określonych rozwiązań, technologii lub dostawców ICT, bez równoległego zapewnienia jasnych, technicznie mierzalnych kryteriów oceny ryzyka oraz realnych okresów przejściowych umożliwiających bezpieczne dostosowanie infrastruktury. W skrajnym scenariuszu decyzja administracyjna, opatrzona rygorem natychmiastowej wykonalności, może wymusić na uczelni konieczność szybkiej wymiany kluczowych elementów infrastruktury ICT. Potencjalny zakres takiej wymiany może obejmować:

- **warstwę sieciową** (urządzenia aktywne, zapory sieciowe, przełączniki),
- **infrastrukturę serwerową i macierzową**,
- **systemy automatyki i infrastruktury technicznej budynków**,
- **oprogramowanie systemowe i aplikacyjne**, w tym rozwiązania specjalistyczne wykorzystywane w badaniach naukowych.

Szacunkowy jednorazowy koszt wymiany infrastruktury ICT w średniej lub dużej uczelni wyższej, w zależności od skali i stopnia uzależnienia od danego dostawcy, może wynosić:

- **warstwa sieciowa**: 1,5–4 mln PLN,

[45] European Union Agency for Cybersecurity (ENISA), Good practices for supply chain cybersecurity, ENISA, 13 Jun 2023, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

- **serwery, pamięci masowe, wirtualizacja**: 2–6 mln PLN,
- **automatyka i systemy techniczne**: 0,5–2 mln PLN,
- **licencje, migracje, wdrożenia aplikacyjne**: 1–3 mln PLN.

Łącznie oznacza to **koszt jednorazowy rzędu 5–15 mln PLN**, nie uwzględniając kosztów pośrednich, takich jak przestoje, ryzyko utraty danych, konieczność szkoleń personelu czy czasowe ograniczenie dostępności usług dydaktycznych i badawczych. Dodatkowym, istotnym problemem jest kolizja mechanizmów KSC z przepisami ustawy prawo zamówień publicznych. Uczelnie wyższe, jako jednostki sektora finansów publicznych, zobowiązane są do prowadzenia sformalizowanych postępowań zakupowych, których harmonogram liczony jest w miesiącach, a nie tygodniach. Decyzja administracyjna wymagająca natychmiastowej wykonalności, następnie wymiany infrastruktury ICT, zakazu nabywania sprzętu tej samej klasy do utrzymania aktualnie działających usług pozostaje w oczywistej sprzeczności z realnymi możliwościami uwzględnienia takich zmian w zakresie budżetowym danego roku np. uniwersyteckiego, przygotowania i przeprowadzenia zgodnego z prawem postępowania przetargowego, pozyskania środków finansowych na wymianę sprzętu, co generuje istotne ryzyko prawne i operacyjne.
W rezultacie uczelnie wyższe mogą znaleźć się w sytuacji, w której wykonanie decyzji administracyjnej zgodnie z KSC jest niemożliwe bez naruszenia przepisów PZP lub bez zastosowania nadzwyczajnych trybów zakupowych, które same w sobie zwiększają ryzyko organizacyjne i finansowe. Taki model regulacyjny należy uznać za nieproporcjonalny, zwłaszcza w zestawieniu z podejściem unijnym, które coraz wyraźniej akcentuje potrzebę skoordynowanych ocen ryzyka na poziomie UE, realnych okresów przejściowych oraz mechanizmów ograniczania ryzyka zamiast administracyjnego wykluczania technologii na poziomie krajowym.
W konsekwencji KSC, zamiast wspierać racjonalne zarządzanie ryzykiem łańcucha dostaw ICT w uczelniach wyższych, generuje istotne ryzyka finansowe, prawne i operacyjne, które mogą bezpośrednio wpływać na ciągłość działalności dydaktycznej i badawczej oraz stabilność finansową instytucji.

5.8. Kultura organizacyjna i świadomość bezpieczeństwa – luka pomiędzy regulacją KSC a realnym ograniczaniem ryzyka (z uwzględnieniem kosztów):

Kultura organizacyjna oraz poziom świadomości użytkowników mają kluczowe znaczenie dla skuteczności systemu cyberbezpieczeństwa, zwłaszcza w organizacjach o dużej liczbie użytkowników i wysokiej rotacji, takich jak uczelnie wyższe. CERT Polska wskazuje, że niski poziom świadomości cyberzagrożeń wśród użytkowników

końcowych pozostaje jednym z głównych czynników umożliwiających skuteczne ataki phishingowe oraz dalszą eskalację incydentów wewnątrz organizacji[46]. Zjawisko to ma charakter systemowy i nie może być skutecznie ograniczane wyłącznie za pomocą środków technicznych.

W tym kontekście podejście przyjęte w Krajowym Systemie Cyberbezpieczeństwa należy ocenić jako niewystarczające. KSC koncentruje się przede wszystkim na spełnieniu obowiązków formalnych i dokumentacyjnych, nie nadając należytej rangi ciągłym programom budowania świadomości bezpieczeństwa. Brak wymogów dotyczących jakości, cykliczności oraz mierzalności działań uświadamiających sprzyja ich incydentalnemu charakterowi i realizacji wyłącznie na potrzeby wykazania zgodności regulacyjnej.

Z perspektywy organizacyjnej i finansowej wdrożenie realnie skutecznego programu budowania kultury bezpieczeństwa w uczelni wyższej wiąże się z istotnymi, stałymi kosztami, które nie są wprost uwzględnione ani wspierane przez mechanizmy KSC. Szacunkowy roczny koszt utrzymania takiego programu, obejmującego całą organizację, może wynosić:

- **platforma e-learningowa i testy phishingowe (licencje, konfiguracja)**: 50–120 tys. PLN,
- **szkolenia cykliczne dla pracowników i doktorantów (online + stacjonarne)**: 80–150 tys. PLN,
- **kampanie uświadamiające (materiały, komunikacja, symulacje)**: 30–70 tys. PLN,
- **czas pracy zespołu koordynującego (IT, HR, bezpieczeństwo, komunikacja)**: 40–80 tys. PLN.

Łączny koszt roczny utrzymania systematycznego programu podnoszenia świadomości bezpieczeństwa można zatem oszacować na poziomie **200–400 tys. PLN**, przy czym są to koszty powtarzalne, niezależne od liczby incydentów oraz stopnia formalnej zgodności z regulacjami.

Paradoksalnie KSC nie tworzy mechanizmów zachęcających do ponoszenia tych kosztów, nie wiążąc poziomu świadomości użytkowników z oceną skuteczności systemu cyberbezpieczeństwa ani z ograniczeniem odpowiedzialności regulacyjnej. W rezultacie uczelnie, działając racjonalnie z punktu widzenia zgodności prawnej, mogą ograniczać inwestycje w kulturę bezpieczeństwa, koncentrując się na spełnieniu wymogów formalnych, które są łatwiejsze do wykazania w trakcie kontroli.

[46] CERT Polska, *Świadomość cyberzagrożeń i phishing*, CERT Polska, 2024, https://cert.pl/posts/2025/04/raport-roczny-2024/

Skutkiem takiego podejścia jest utrzymywanie się wysokiego poziomu ryzyka operacyjnego, powtarzalność incydentów opartych na socjotechnice oraz wzrost kosztów obsługi naruszeń bezpieczeństwa. W dłuższej perspektywie oznacza to, że KSC – mimo zwiększania obciążeń administracyjnych – nie przekłada się proporcjonalnie na realne ograniczenie ryzyka, zwłaszcza w środowisku akademickim, gdzie czynnik ludzki pozostaje jednym z głównych wektorów ataku.

5.9. Porównanie kosztów TCO: budowa świadomości cyberbezpieczeństwa vs obsługa incydentów:

Z perspektywy całkowitego kosztu posiadania (TCO – *Total Cost of Ownership*) działania w obszarze budowy kultury bezpieczeństwa i świadomości użytkowników należy analizować w zestawieniu z kosztami obsługi incydentów cyberbezpieczeństwa, które wynikają z zaniedbań w tym obszarze. W środowisku uczelni wyższych, charakteryzującym się dużą liczbą użytkowników oraz wysoką rotacją, czynnik ludzki pozostaje jednym z dominujących wektorów ryzyka.

a) Roczny TCO inwestycji w świadomość cyberbezpieczeństwa (model prewencyjny)

Szacunkowy roczny koszt utrzymania systematycznego programu budowy świadomości bezpieczeństwa w średniej lub dużej uczelni wyższej obejmuje:

- platformę e-learningową i testy phishingowe: **50–120 tys. PLN**,
- cykliczne szkolenia pracowników i doktorantów: **80–150 tys. PLN**,
- kampanie uświadamiające i symulacje ataków: **30–70 tys. PLN**,
- koordynację organizacyjną (IT, HR, bezpieczeństwo): **40–80 tys. PLN**.

Łączny roczny TCO działań prewencyjnych: 200–400 tys. PLN

Koszt ten ma charakter **stały i przewidywalny**, a jego efektem jest stopniowe ograniczanie liczby incydentów, skrócenie czasu ich wykrycia oraz zmniejszenie skali eskalacji.

b) Roczny TCO obsługi incydentów cyberbezpieczeństwa (model reaktywny)

Koszty obsługi pojedynczego istotnego incydentu (np. phishing prowadzący do przejęcia kont, ransomware, wyciek danych) w uczelni wyższej obejmują:

- prace zespołów IT i bezpieczeństwa (analiza, odtwarzanie): **50–150 tys. PLN**,
- wsparcie zewnętrzne (IR, forensics, doradztwo prawne): **80–250 tys. PLN**,
- przestoje systemów dydaktycznych i administracyjnych: **50–200 tys. PLN**,
- koszty organizacyjne i komunikacyjne (obsługa interesariuszy, raportowanie): **20–80 tys. PLN**,
- potencjalne kary administracyjne i ryzyko odpowiedzialności kierownictwa: **trudne do oszacowania, lecz istotne**.

Łączny koszt pojedynczego poważnego incydentu: 200–600 tys. PLN
W przypadku wystąpienia **2–3 incydentów rocznie** (co w środowisku akademickim nie jest scenariuszem skrajnym), roczny TCO modelu reaktywnego może wynosić:
400 tys. – 1,2 mln PLN rocznie
Koszty te są **nieprzewidywalne, skokowe i trudne do zaplanowania budżetowo**, a dodatkowo wiążą się z ryzykiem reputacyjnym i prawnym.

c) Porównanie TCO – ujęcie syntetyczne:

Obszar	Model prewencyjny – świadomość	Model reaktywny – incydenty
Charakter kosztów	Stałe, możliwe do zaplanowania	Skokowe, nieprzewidywalne
Roczny TCO	200–400 tys. PLN	400 tys. – 1,2 mln PLN
Wpływ na ryzyko	Redukcja liczby i skali incydentów	Brak redukcji ryzyka źródłowego
Wpływ organizacyjny	Wzrost kultury bezpieczeństwa	Przestoje, chaos decyzyjny
Zgodność regulacyjna	Wspiera realną odporność	Często wyłącznie reagowanie i usuwanie incydentów

d) Wniosek kosztowo-regulacyjny w kontekście KSC:

Z punktu widzenia TCO inwestycje w budowę świadomości cyberbezpieczeństwa są **kilkukrotnie tańsze** niż długoterminowe koszty obsługi incydentów. Paradoksalnie jednak Krajowy System Cyberbezpieczeństwa nie tworzy mechanizmów premiujących taki model prewencyjny, koncentrując się na obowiązkach formalnych, dokumentacyjnych i sankcyjnych.
W efekcie uczelnie wyższe, działając racjonalnie w ramach nadregulacyjnego reżimu KSC, mogą ograniczać nakłady na świadomość i kulturę bezpieczeństwa, mimo że to właśnie ten obszar generuje **najlepszy stosunek koszt–efekt** w redukcji ryzyka cybernetycznego.

5.10. Wnioski z analizy organizacyjnej stanu AS-IS:

Analiza organizacyjna stanu AS-IS w obszarze cyberbezpieczeństwa uczelni wyższych wskazuje, że znaczna część instytucji może być nieprzygotowana do wdrożenia wymogów Krajowego Systemu Cyberbezpieczeństwa w aktualnym kształcie, nie tyle

ze względu na faktyczny poziom zagrożeń, ile z uwagi na skalę i charakter obciążeń regulacyjnych. Wymogi KSC wprowadzają rozbudowany model odpowiedzialności, dokumentacji, audytowalności oraz nadzoru administracyjnego, który wykracza poza dotychczasowe praktyki organizacyjne funkcjonujące w sektorze szkolnictwa wyższego.

Z perspektywy organizacyjnej problemem nie jest wyłącznie reaktywny charakter działań w obszarze cyberbezpieczeństwa, lecz przede wszystkim brak struktur, procesów i zasobów umożliwiających spełnienie formalnych wymagań KSC w sposób systemowy i trwały. Uczelnie, nawet te posiadające rozwinięte zaplecze techniczne, mogą nie dysponować odpowiednim poziomem governance, jasno zdefiniowanymi rolami decyzyjnymi ani mechanizmami integrującymi cyberbezpieczeństwo z procesami zarządczymi i budżetowymi, co znacząco utrudnia adaptację do nadregulacyjnego modelu KSC.

Należy podkreślić, że konstrukcja KSC wymusza przesunięcie ciężaru odpowiedzialności z poziomu operacyjnego na poziom formalno-zarządczy, przy jednoczesnym zwiększeniu ryzyka sankcyjnego. Dla uczelni wyższych oznacza to konieczność szybkiej transformacji organizacyjnej, obejmującej m.in. budowę struktur nadzorczych, utrzymanie „żywej" dokumentacji, zapewnienie ciągłości procesów audytowych oraz spełnienie wymogów raportowych. Taka transformacja, realizowana bez odpowiednich okresów przejściowych i wsparcia systemowego, może prowadzić do istotnych napięć organizacyjnych i finansowych.

W tym kontekście należy stwierdzić, że potencjalna niezgodność uczelni wyższych z wymogami KSC nie musi wynikać z braku świadomości zagrożeń czy zaniedbań operacyjnych, lecz z niedostosowania modelu regulacyjnego do specyfiki i możliwości organizacyjnych sektora akademickiego. Z perspektywy KSC i NIS2 oznacza to, że zamiast stopniowej transformacji w kierunku zarządzania ryzykiem na poziomie strategicznym, uczelnie mogą zostać zmuszone do realizacji kosztownych i administracyjnie złożonych działań dostosowawczych, których efektywność w zakresie realnego podniesienia poziomu cyberbezpieczeństwa pozostaje dyskusyjna.

Mapa możliwych problemów wynikających niespełnienia wymogów KSC:

Wymóg KSC	**Typowa luka organizacyjna (AS-IS)**	**Szacunkowy koszt dostosowania**	**Ryzyko pozostawienia luki**
Odpowiedzialność kierownika jednostki za cyberbezpieczeństwo	Brak formalnego governance; cyberbezpieczeństwo	Koszt pośredni: czas zarządu + wsparcie doradcze	Odpowiedzialność osobista kierownictwa, decyzje ad hoc, brak

Wymóg KSC	**Typowa luka organizacyjna (AS-IS)**	**Szacunkowy koszt dostosowania**	**Ryzyko pozostawienia luki**
	delegowane do IT bez mechanizmów decyzyjnych	**50–150 tys. PLN/rok**	obrony „należytej staranności”
Wyodrębnienie ról i struktur bezpieczeństwa	Brak CISO / pełnomocnika; konflikty IT–IOD–administracja	Zespół wewnętrzny: **700 tys.–1,1 mln PLN/rok** lub vCISO: **150–300 tys. PLN/rok**	Rozmycie odpowiedzialności, chaos decyzyjny w incydencie
Ciągłe zarządzanie ryzykiem	Analiza ryzyka jednorazowa lub „do teczki”	Warsztaty + narzędzia GRC: **120–250 tys. PLN/rok**	Niezgodność formalna + brak podstaw do decyzji inwestycyjnych
„Żywa” dokumentacja i audytowalność	Dokumentacja statyczna, brak ownerów procesów	Dokumentacja + narzędzia + audyty: **500–900 tys. PLN/rok**	Sankcje administracyjne, niezdolność do wykazania zgodności
Obsługa incydentów i raportowanie	Brak procedur IR, brak logów i playbooków	SOC/MDR + IR readiness: **200–500 tys. PLN/rok**	Eskalacja incydentów, chaos raportowy, ryzyko kar
Monitoring i detekcja	Brak SIEM/EDR, rozproszone logi	SIEM + EDR/MDR: **300–700 tys. PLN/rok**	Incydenty wykrywane z opóźnieniem lub przez osoby trzecie
Zarządzanie dostawcami ICT	Umowy bez klauzul cyberbezpieczeństwa; brak oceny ryzyka, brak certyfikacji dostawcy	Audyty dostawców + renegocjacje: **100–300 tys. PLN/rok**	Ryzyko łańcucha dostaw, odpowiedzialność za cudze błędy
Eliminacja „niekwalifikowanej” infrastruktury	Brak planów migracji, uzależnienie od jednego dostawcy	Wymiana infrastruktury: **5–15 mln PLN (jednorazowo)**	Paraliż operacyjny, konflikt z PZP, ryzyko prawne
Ciągłość działania (BCP/DR)	Brak RTO/RPO, brak testów	BCP/DR + testy: **150–400 tys. PLN/rok**	Długotrwałe przestoje, utrata danych i reputacji
Szkolenia i świadomość	Szkolenia incydentalne lub brak	Program świadomości: **200–400 tys. PLN/rok**	Phishing, powtarzalność incydentów, eskalacja kosztów

Analiza mapy możliwych problemów wynikających z KSC wskazuje, że potencjalna niezgodność uczelni wyższych z wymogami KSC wynika przede wszystkim z nadregulacyjnego charakteru przepisów, a nie z braku świadomości zagrożeń czy zaniedbań operacyjnych adekwatnych do możliwości uczelni. Skala wymaganych zmian organizacyjnych, kompetencyjnych i finansowych znacząco przekracza obecne modele funkcjonowania uczelni, prowadząc do ryzyka kosztowej i organizacyjnej nieadekwatności regulacji wobec rzeczywistych zagrożeń.

6. Analiza stanu obecnego (AS-IS) cyberbezpieczeństwa w uczelniach wyższych – ujęcie techniczne i operacyjne

6.1. Architektura infrastruktury IT i jej wpływ na poziom bezpieczeństwa:

Infrastruktura informatyczna uczelni wyższych charakteryzuje się znacznym stopniem złożoności oraz heterogeniczności, wynikającym z wieloletniego, ewolucyjnego rozwoju systemów informatycznych. W praktyce oznacza to współistnienie nowoczesnych rozwiązań informatycznych z systemami starszej generacji (tzw. *legacy systems*), które często nie spełniają aktualnych standardów bezpieczeństwa.
European Union Agency for Cybersecurity wskazuje, że brak spójnej architektury bezpieczeństwa oraz standaryzacji środowiska IT istotnie zwiększa powierzchnię ataku, utrudnia centralne zarządzanie zabezpieczeniami oraz ogranicza skuteczność procesów zarządzania ryzykiem cybernetycznym[47]. Problem ten dotyczy w szczególności organizacji o rozproszonej strukturze i długim cyklu życia systemów, do których zaliczają się uczelnie wyższe.
Analogiczne wnioski formułuje Najwyższa Izba Kontroli, wskazując, że w jednostkach sektora publicznego rozproszenie infrastruktury IT, brak centralnej inwentaryzacji zasobów oraz niejednolite standardy techniczne stanowią jedną z głównych barier skutecznego zabezpieczenia systemów informatycznych[48]. W konsekwencji utrudnione jest zarówno wykrywanie podatności, jak i skuteczne reagowanie na incydenty cyberbezpieczeństwa.

[47] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, ENISA, 2022,

[48] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024,
https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

6.2. Zarządzanie tożsamością i dostępem (IAM):

Zarządzanie tożsamością i dostępem (Identity and Access Management – IAM) stanowi jeden z najbardziej krytycznych filarów technicznego cyberbezpieczeństwa, ponieważ w praktyce **tożsamość użytkownika jest dziś główną „granicą" bezpieczeństwa** dla usług chmurowych, systemów dziekanatowych, poczty, narzędzi badawczych oraz zasobów sieciowych. W środowisku szkolnictwa wyższego obszar IAM jest szczególnie złożony ze względu na masową skalę populacji użytkowników, wysoką rotację (studenci, doktoranci, stażyści, pracownicy czasowi), wielość ról i wyjątków (goście, użytkownicy zewnętrzni, partnerzy konsorcjów), a także autonomię jednostek organizacyjnych i laboratoriów.
W praktyce najczęściej ujawniają się następujące problemy:

- brak centralnego systemu IAM lub jego częściowe, niespójne wdrożenie (lokalne katalogi, osobne bazy kont w systemach),
- zróżnicowane mechanizmy uwierzytelniania (w tym brak spójnego SSO),
- nadmiarowe uprawnienia i brak formalnego modelu ról (RBAC/ABAC),
- opóźnienia w dezaktywacji kont oraz brak automatyzacji cyklu życia tożsamości (Joiner–Mover–Leaver),
- niewystarczający nadzór nad kontami uprzywilejowanymi (administratorzy, konta serwisowe, konta aplikacyjne),
- niejednolite standardy MFA, zwłaszcza w systemach „legacy", laboratoriach i usługach specyficznych dla badań.

Z perspektywy dobrych praktyk bezpieczeństwa, norma ISO/IEC 27001 wymaga m.in. stosowania zasady minimalnych uprawnień, kontrolowania nadawania i odbierania dostępów oraz zarządzania cyklem życia kont użytkowników[49]. W obszarze operacyjnym oznacza to konieczność wdrożenia procesów i mechanizmów technicznych, które zapewniają, że:

- dostęp jest przyznawany wyłącznie na podstawie uzasadnionej potrzeby biznesowej,
- uprawnienia są regularnie przeglądane i recertyfikowane,
- konta są automatycznie dezaktywowane po ustaniu relacji z organizacją,
- konta uprzywilejowane są chronione dodatkowymi kontrolami (PAM, MFA, rejestrowanie sesji).

[49] ISO/IEC 27001:2022 – *Information Security Management Systems* (wymogi dotyczące m.in. kontroli dostępu i zarządzania uprawnieniami), https://www.iso.org/standard/27001

Jednocześnie dane operacyjne CSIRT pokazują, że przejęcie kont – najczęściej w wyniku phishingu lub kradzieży danych uwierzytelniających – stanowi jeden z dominujących punktów wejścia do środowisk organizacji publicznych, w tym uczelni. W konsekwencji skuteczny IAM (zwłaszcza MFA + szybkie wygaszanie kont + kontrola uprawnień) jest realnym „hamulcem" eskalacji incydentu[50].

Aspekty techniczne, które powinny zostać ujęte w architekturze IAM

Aby IAM pełnił funkcję realnego mechanizmu ograniczania ryzyka, a nie wyłącznie elementu formalnej zgodności, architektura powinna obejmować co najmniej:

- **centralną usługę tożsamości** (IdP) i katalog (np. AD/LDAP) jako „single source of truth",
- **federację tożsamości i SSO** (SAML/OIDC) dla usług uczelnianych i chmury,
- **MFA w modelu ryzyka** (risk-based / conditional access) przynajmniej dla poczty, VPN, paneli administracyjnych, aplikacji krytycznych i dostępu zewnętrznego,
- **proces Joiner–Mover–Leaver** z integracją z systemami kadrowymi i studenckimi (automatyzacja tworzenia kont, zmian ról, dezaktywacji),
- **PAM (Privileged Access Management)** dla kont uprzywilejowanych i kont serwisowych,
- **recertyfikację uprawnień** (np. kwartalną dla systemów krytycznych i danych badawczych),
- **logowanie zdarzeń IAM** (audyt logowań, zmian uprawnień, użycia kont uprzywilejowanych) i zasilanie tym SIEM.

Nadregulacja KSC (projekt 2026) a realne potrzeby IAM

Projekt nowej ustawy KSC (2026) – implementując NIS2 – wzmacnia oczekiwanie, że podmiot będzie w stanie **wykazać** (dowodowo) skuteczne mechanizmy kontroli dostępu, zarządzania ryzykiem i obsługi incydentów. Problem w realiach sektora publicznego polega na tym, że konstrukcja krajowa może w praktyce przesuwać ciężar z efektu bezpieczeństwa (np. skrócenie czasu dezaktywacji kont i ograniczenie skuteczności phishingu) na **audytowalność i formalną wykazywalność** procesu[51].

W obszarze IAM może to generować kilka ryzyk nadregulacyjnych:

a) **Presja na natychmiastową, pełną centralizację** ról i tożsamości w całej organizacji, również tam, gdzie procesy są rozproszone i „badawczo

[50] CERT Polska, Przegląd kampanii phishingowych z 2024 roku, CERT Polska, 02 Apr 2025, https://cert.pl/posts/2025/04/przeglad-kampanii-2024/

[51] Ustawa o KSC – tekst jednolity (ISAP) oraz kontekst projektowanych zmian implementujących NIS2 (projekt 2026), https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 https://www.gov.pl/web/cyfryzacja

-projektowe", a nie usługowe (laboratoria, konsorcja, środowiska eksperymentalne).

b) **Rozrost obowiązków dokumentacyjnych** (rejestry dostępów, uzasadnienia, protokoły recertyfikacji, procedury wyjątków) jako „dowodów" zgodności, nawet jeśli nie przekładają się one proporcjonalnie na poprawę bezpieczeństwa operacyjnego.

c) **Ryzyko sankcyjne i odpowiedzialności** przy jednoczesnej niejednoznaczności kryteriów jakości (np. „kiedy IAM jest wystarczająco centralny", „jaki poziom MFA jest wystarczający"), co może prowadzić do zachowań obronnych: formalizacja zamiast realnego podnoszenia odporności.

d) **Zwiększenie kosztów i czasu wdrożenia**: IAM w skali dużej organizacji publicznej wymaga nie tylko narzędzia, ale przebudowy procesów HR/Student/Grant/IT, mapowania ról, integracji systemów oraz cyklicznej recertyfikacji. W warunkach nadregulacji rośnie ryzyko, że wdrożenie stanie się projektem compliance, a nie projektem odporności.

Z punktu widzenia „realnych wymogów" NIS2, kluczowe jest, aby wymagania kontroli dostępu i tożsamości były wdrażane **proporcjonalnie do ryzyka** i krytyczności usług, a skuteczność była wykazywana poprzez mierzalne efekty (np. odsetek kont z MFA, czas dezaktywacji kont po zakończeniu relacji, liczba kont uprzywilejowanych, wyniki recertyfikacji), a nie wyłącznie poprzez rozbudowę dokumentacji procesowej[52]. Jeżeli krajowe podejście KSC (2026) będzie interpretowane zbyt „papierowo", istnieje ryzyko, że główne zasoby zostaną przesunięte na formalne procedury, zamiast na modernizację tożsamości (SSO/MFA/PAM) i automatyzację cyklu życia.

Wniosek operacyjny

W obszarze IAM priorytet powinien obejmować: (1) centralny IdP + federację i SSO, (2) MFA dla systemów krytycznych i zdalnych dostępów, (3) automatyzację Joiner–Mover–Leaver, (4) PAM dla kont uprzywilejowanych, (5) recertyfikacje i logowanie zdarzeń IAM. Dopiero na tej bazie uzasadnione jest rozwijanie warstwy formalnej (procedury, rejestry, dowody). W przeciwnym razie wdrożenie może stać się przykładem kosztownej zgodności formalnej, nieprzekładającej się na proporcjonalną poprawę odporności na realne incydenty oparte o przejęcie tożsamości.

[52] Dyrektywa (UE) 2022/2555 (NIS2) – obowiązek stosowania środków zarządzania ryzykiem i wykazywania ich skuteczności (art. 21), https://eur-lex.europa.eu/eli/dir/2022/2555/oj

6.3. Monitorowanie bezpieczeństwa i detekcja incydentów – konsekwencje nadregulacji KSC:

Efektywna detekcja incydentów cyberbezpieczeństwa wymaga centralnego monitorowania i korelacji zdarzeń generowanych przez systemy informatyczne, sieciowe oraz aplikacyjne. W środowisku uczelni wyższych zdolność ta bywa ograniczona lub fragmentaryczna, co wynika z rozproszonej architektury IT, heterogenicznych systemów oraz braku centralnych zespołów bezpieczeństwa. W praktyce brak centralnej korelacji zdarzeń skutkuje opóźnionym wykrywaniem incydentów, ograniczoną widocznością ataków wieloetapowych oraz trudnościami w przeprowadzaniu analizy przyczyn źródłowych.
Norma ISO/IEC 27002 wskazuje na konieczność prowadzenia ciągłego monitoringu bezpieczeństwa, gromadzenia logów oraz ich systematycznej analizy jako podstawowego mechanizmu wczesnego wykrywania zagrożeń[53]. Analogicznie CERT Polska podkreśla, że rosnąca skala, złożoność i trudności w identyfikacji incydentów powodują, iż znaczna część również w sektorze publicznym jest wykrywana dopiero po wystąpieniu widocznych skutków operacyjnych, co znacząco zwiększa skalę strat finansowych i organizacyjnych[54].
W kontekście Krajowego Systemu Cyberbezpieczeństwa problem ten ulega jednak istotnemu zaostrzeniu. KSC, poprzez rozbudowane obowiązki raportowe, audytowe oraz sankcyjne, w sposób pośredni wymusza wdrażanie zaawansowanych mechanizmów monitorowania, takich jak systemy SIEM, EDR/XDR oraz całodobowe centra operacyjne bezpieczeństwa (SOC). Jednocześnie regulacja nie definiuje minimalnych, proporcjonalnych poziomów dojrzałości detekcji ani nie uwzględnia specyfiki i skali działalności uczelni wyższych, co prowadzi do nadmiernego obciążenia organizacyjnego i finansowego.
Wdrożenie pełnego modelu monitorowania zgodnego z oczekiwaniami interpretacyjnymi KSC wiąże się z istotnymi kosztami. Szacunkowy roczny koszt utrzymania:

- **systemu SIEM (licencje, integracje, utrzymanie)**: 150–350 tys. PLN,
- **rozwiązań EDR/XDR dla stacji roboczych i serwerów**: 100–250 tys. PLN,
- **usług SOC / MDR (24/7 monitoring i reakcja)**: 200–500 tys. PLN.

---

[53] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*, International Organization for Standardization, https://www.iso.org/standard/75652.html
[54] CERT Polska, *Raport roczny o stanie cyberbezpieczeństwa w Polsce*, CERT Polska, 2024, https://cert.pl/posts/2025/04/raport-roczny-2024/

Łączny koszt roczny funkcjonowania modelu SOC/SIEM/EDR w uczelni wyższej może zatem wynosić **450–1 100 tys. PLN**, nie uwzględniając kosztów jednorazowych wdrożenia, integracji z systemami legacy oraz dodatkowych zasobów kadrowych po stronie uczelni. Są to koszty stałe, niezależne od liczby rzeczywistych incydentów, które wprost konkurują z finansowaniem działalności dydaktycznej i badawczej.
Dodatkowym problemem wynikającym z nadregulacji KSC jest ryzyko formalizacji detekcji kosztem jej skuteczności. Uczelnie mogą być zmuszone do wdrażania rozbudowanych narzędzi monitorujących przede wszystkim w celu wykazania zgodności audytowej, a nie w odpowiedzi na rzeczywiste potrzeby zarządzania ryzykiem. W efekcie monitoring bezpieczeństwa staje się kolejnym elementem spełniania wymogów formalnych, zamiast narzędziem realnie poprawiającym zdolność organizacji do wczesnego wykrywania i ograniczania skutków incydentów.
W porównaniu do podejścia promowanego w dyrektywie NIS2, która akcentuje proporcjonalność oraz skuteczność środków technicznych, KSC w aktualnym kształcie sprzyja wdrażaniu kosztownych i sztywnych rozwiązań detekcyjnych, bez jednoznacznego powiązania ich zakresu z profilem ryzyka uczelni. W konsekwencji monitoring bezpieczeństwa, zamiast wzmacniać odporność cybernetyczną sektora akademickiego, może stać się źródłem istotnych obciążeń finansowych i organizacyjnych.

6.4. Zarządzanie podatnościami i aktualizacjami – praktyka techniczna a wymogi KSC:

Zarządzanie podatnościami oraz proces aktualizacji systemów informatycznych stanowią jeden z kluczowych filarów technicznego cyberbezpieczeństwa. W środowisku uczelni wyższych proces ten może być realizowany z różnym stopniem dojrzałości, w zależności od skali infrastruktury, dostępnych zasobów kadrowych oraz krytyczności obsługiwanych systemów. W praktyce uczelnie często stosują podejście ostrożne, polegające na opóźnianiu instalacji poprawek bezpieczeństwa w systemach dydaktycznych i badawczych, w celu ograniczenia ryzyka zakłóceń ciągłości działania lub niekompatybilności z oprogramowaniem specjalistycznym.
European Union Agency for Cybersecurity wskazuje, że opóźnienia w instalowaniu poprawek bezpieczeństwa należą do najczęstszych przyczyn skutecznych ataków na infrastrukturę organizacji publicznych, szczególnie w środowiskach o dużej liczbie systemów legacy oraz ograniczonej automatyzacji procesów aktualizacyjnych[55].

[55] European Union Agency for Cybersecurity, *Vulnerability management*, ENISA, 2022, https://www.enisa.europa.eu/topics/threat-risk-management/vulnerability-management

Jednocześnie należy podkreślić, że w przypadku uczelni wyższych decyzje o przesunięciu aktualizacji nie zawsze wynikają z zaniedbań, lecz często są świadomym kompromisem pomiędzy bezpieczeństwem a stabilnością procesów dydaktycznych i badawczych.

Najwyższa Izba Kontroli zwraca uwagę, że brak systematycznego i udokumentowanego podejścia do zarządzania podatnościami stanowi istotną nieprawidłowość w jednostkach sektora publicznego[56]. W kontekście Krajowego Systemu Cyberbezpieczeństwa problem ten nabiera jednak nowego wymiaru. KSC akcentuje obowiązek zapewnienia „odpowiedniego" poziomu zabezpieczeń, nie precyzując jednocześnie, w jaki sposób organizacje powinny równoważyć wymagania bezpieczeństwa z potrzebą zapewnienia ciągłości i stabilności usług.

Nadregulacyjny charakter KSC powoduje, że zarządzanie podatnościami staje się nie tylko zagadnieniem technicznym, lecz również obszarem podwyższonego ryzyka formalnego. Uczelnie mogą zostać zmuszone do wdrażania sztywnych harmonogramów aktualizacji, rozbudowanej dokumentacji oraz audytowalnych procedur, niezależnie od specyfiki poszczególnych systemów. W przypadku środowisk dydaktycznych i badawczych, w których wykorzystywane są rozwiązania niszowe, autorskie lub rzadko aktualizowane przez producentów, takie podejście może prowadzić do zwiększenia ryzyka operacyjnego zamiast jego ograniczenia.

W praktyce oznacza to konieczność budowy dodatkowych mechanizmów kompensacyjnych, takich jak środowiska testowe, segmentacja sieci, tymczasowe środki ochrony czy rozszerzony monitoring, co generuje istotne koszty organizacyjne i techniczne. KSC nie przewiduje jednak elastycznych modeli oceny ryzyka, które pozwalałyby uznać takie środki alternatywne za równoważne z natychmiastową instalacją poprawek.

W porównaniu z podejściem promowanym w regulacjach unijnych oraz dobrych praktykach ENISA, które akcentują zarządzanie podatnościami w oparciu o analizę ryzyka i krytyczność zasobów, KSC w aktualnym kształcie sprzyja formalizacji i uniformizacji procesów. Dla uczelni wyższych oznacza to ryzyko nieproporcjonalnych obciążeń regulacyjnych, które nie zawsze przekładają się na realny wzrost poziomu cyberbezpieczeństwa, a w skrajnych przypadkach mogą prowadzić do destabilizacji kluczowych systemów dydaktycznych i badawczych.

[56] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024,https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

6.5. Zarządzanie podatnościami, aktualizacjami oraz testami regresji – implikacje kosztowe w reżimie KSC:

Zarządzanie podatnościami w środowisku uczelni wyższych nie ogranicza się wyłącznie do identyfikacji i instalowania poprawek bezpieczeństwa, lecz obejmuje również konieczność zapewnienia stabilności systemów dydaktycznych, badawczych i administracyjnych. W praktyce oznacza to potrzebę prowadzenia testów regresji, weryfikacji kompatybilności aktualizacji z oprogramowaniem specjalistycznym oraz planowania okien serwisowych w sposób minimalizujący wpływ na ciągłość działania uczelni.
W warunkach nadregulacyjnych Krajowego Systemu Cyberbezpieczeństwa proces ten ulega istotnemu sformalizowaniu. KSC, poprzez wymogi audytowalności, dokumentowania decyzji oraz odpowiedzialności kierownictwa, pośrednio wymusza wdrożenie powtarzalnych, udokumentowanych procedur patch managementu, obejmujących pełny cykl życia podatności: identyfikację, ocenę ryzyka, testowanie, wdrożenie oraz weryfikację skuteczności. Dla uczelni wyższych oznacza to znaczący wzrost kosztów operacyjnych, niezależny od faktycznej liczby krytycznych podatności.
Szacunkowy roczny koszt utrzymania dojrzałego procesu patch managementu w średniej lub dużej uczelni wyższej obejmuje:

- **narzędzia do skanowania podatności i zarządzania aktualizacjami**: 80–180 tys. PLN,
- **utrzymanie środowisk testowych (sprzęt, wirtualizacja, licencje)**: 100–250 tys. PLN,
- **prace zespołów IT i bezpieczeństwa (analiza podatności, planowanie, dokumentacja)**: 150–300 tys. PLN,
- **testy regresji systemów dydaktycznych i badawczych (wewnętrzne lub zewnętrzne)**: 100–200 tys. PLN.

Łączny roczny koszt utrzymania procesu zarządzania podatnościami i testów regresji można zatem oszacować na poziomie **430–930 tys. PLN**, przy czym są to koszty stałe, powtarzalne i w dużej mierze niezależne od faktycznego poziomu zagrożeń.
W kontekście KSC szczególnie problematyczne jest to, że regulacja nie przewiduje elastycznych mechanizmów uznawania decyzji opartych na analizie ryzyka, takich jak czasowe odroczenie aktualizacji przy jednoczesnym wdrożeniu środków kompensacyjnych (np. segmentacja sieci, ograniczenie uprawnień, rozszerzony monitoring). W efekcie uczelnie mogą być zmuszone do przeprowadzania kosztownych testów regresji i aktualizacji również w przypadkach, w których ryzyko techniczne jest relatywnie niskie, lecz ryzyko formalnej niezgodności – wysokie.

Dodatkowym obciążeniem jest konieczność dokumentowania każdego etapu procesu w sposób umożliwiający jego późniejszą weryfikację przez organy nadzorcze. Taki model sprzyja formalizacji i biurokratyzacji patch managementu, przesuwając ciężar działań z realnego ograniczania ryzyka na spełnianie wymogów audytowych. W skrajnych przypadkach może to prowadzić do sytuacji, w której decyzje techniczne są podejmowane nie na podstawie krytyczności podatności, lecz w celu minimalizacji ryzyka regulacyjnego.
W porównaniu z podejściem rekomendowanym przez europejskie instytucje eksperckie, które akcentują proporcjonalność oraz zarządzanie podatnościami w oparciu o kontekst ryzyka i krytyczność zasobów, KSC w aktualnym kształcie generuje istotne i trwałe koszty operacyjne. Dla uczelni wyższych oznacza to konieczność utrzymywania rozbudowanych procesów patch managementu i testów regresji, które nie zawsze przekładają się na adekwatny wzrost poziomu cyberbezpieczeństwa, a jednocześnie ograniczają elastyczność.

6.6. Kopie zapasowe i odporność na ransomware – skuteczność techniczna a wymogi KSC:

Mechanizmy tworzenia kopii zapasowych stanowią jeden z kluczowych elementów odporności organizacji na ataki typu ransomware. W uczelniach wyższych kopie zapasowe są co do zasady wykonywane, jednak w wielu przypadkach proces ten koncentruje się na samym tworzeniu backupów, bez regularnych testów procedur odtwarzania, weryfikacji spójności danych oraz symulacji scenariuszy kryzysowych. Taki model zapewnia jedynie pozorną odporność na ransomware, ograniczoną do poziomu deklaratywnego.
European Union Agency for Cybersecurity wskazuje, że brak regularnych testów odtworzeniowych istotnie obniża skuteczność systemów backupowych w sytuacji realnego incydentu ransomware, gdyż organizacje nie są w stanie przewidzieć rzeczywistego czasu odtworzenia ani zakresu utraty danych[57]. W praktyce oznacza to, że posiadanie kopii zapasowych nie jest równoznaczne z posiadaniem zdolności do szybkiego i kontrolowanego przywrócenia ciągłości działania.
Najwyższa Izba Kontroli podkreśla dodatkowo, że jednostki sektora publicznego często nie są w stanie wykazać faktycznej zdolności do odtworzenia danych po incydencie cyberbezpieczeństwa, a procedury odtworzeniowe istnieją głównie

[57] ENISA Threat Landscape for Ransomware Attacks (2022), https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

na poziomie dokumentacyjnym[58]. Problem ten ma charakter systemowy i wynika m.in. z braku testów, niedostosowania infrastruktury backupowej do skali środowiska produkcyjnego oraz niejasnych ról i odpowiedzialności w procesie przywracania systemów.

W kontekście Krajowego Systemu Cyberbezpieczeństwa zagadnienie kopii zapasowych nabiera dodatkowego wymiaru regulacyjnego. KSC akcentuje obowiązek zapewnienia ciągłości działania oraz odporności systemów informatycznych, jednocześnie koncentrując się na możliwości wykazania spełnienia tych wymogów w toku kontroli lub audytu. W efekcie uczelnie mogą być zmuszone do rozbudowy dokumentacji, procedur i harmonogramów testów backupów w sposób formalny, bez proporcjonalnego wsparcia organizacyjnego i finansowego dla faktycznego zwiększenia odporności technicznej.

Nadregulacyjny charakter KSC powoduje, że testy odtworzeniowe oraz architektura kopii zapasowych stają się elementem wysokiego ryzyka formalnego. Brak udokumentowanych testów lub nieosiągnięcie założonych parametrów RTO/RPO może być interpretowane jako niezgodność regulacyjna, niezależnie od rzeczywistego poziomu ryzyka operacyjnego. Skłania to organizacje do podejmowania działań nastawionych na spełnienie wymogów audytowych, a nie na optymalizację realnej odporności na ransomware.

W praktyce skutkuje to koniecznością inwestowania w kosztowne rozwiązania klasy enterprise, obejmujące separację środowisk backupowych, mechanizmy niezmienności danych (*immutable backups*), dodatkowe lokalizacje odtworzeniowe oraz cykliczne testy przywracania. Dla uczelni wyższych, funkcjonujących w reżimie finansów publicznych, oznacza to istotne i trwałe obciążenie budżetowe, które nie zawsze pozostaje proporcjonalne do rzeczywistego profilu ryzyka.

W porównaniu z podejściem rekomendowanym w ramach dobrych praktyk europejskich, które akcentują testowanie odporności w oparciu o analizę ryzyka i krytyczność usług, KSC w aktualnym kształcie sprzyja formalizacji i biurokratyzacji obszaru kopii zapasowych. W rezultacie uczelnie mogą spełniać wymogi regulacyjne dotyczące backupów, nie osiągając jednocześnie istotnego wzrostu zdolności do skutecznego reagowania na ataki ransomware.

[58] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

6.7. Obsługa incydentów cyberbezpieczeństwa – ujęcie techniczne w kontekście nadregulacji KSC:

Obsługa incydentów cyberbezpieczeństwa wymaga sformalizowanych procedur technicznych, jasno zdefiniowanych ról oraz narzędzi wspierających proces reagowania, takich jak systemy zgłoszeń, rejestry incydentów, mechanizmy zbierania dowodów oraz środowiska analityczne. W praktyce uczelni wyższych obsługa incydentów bywa realizowana z różnym stopniem dojrzałości – od ustrukturyzowanych procesów w większych jednostkach, po działania o charakterze ad hoc, oparte na wiedzy i doświadczeniu pojedynczych administratorów systemów informatycznych.

Norma **ISO/IEC 27035** jednoznacznie wskazuje na konieczność posiadania udokumentowanego procesu zarządzania incydentami, obejmującego ich identyfikację, klasyfikację, obsługę, analizę przyczyn źródłowych oraz wyciąganie wniosków na przyszłość[59]. W ujęciu normatywnym proces ten ma charakter ciągły i powinien być zintegrowany z zarządzaniem ryzykiem oraz mechanizmami doskonalenia systemu bezpieczeństwa informacji.

W kontekście Krajowego Systemu Cyberbezpieczeństwa obsługa incydentów nabiera jednak dodatkowego, silnie sformalizowanego wymiaru. KSC nie tylko wymaga zdolności technicznej do reagowania na incydenty, lecz również nakłada obowiązki dokumentacyjne, raportowe oraz sprawozdawcze, których niespełnienie może być interpretowane jako naruszenie obowiązków ustawowych. Brak udokumentowanych procedur, rejestrów incydentów lub jednoznacznych ścieżek decyzyjnych stanowi w tym ujęciu istotną lukę formalną, niezależnie od faktycznej skuteczności działań technicznych podejmowanych przez personel IT.

Nadregulacyjny charakter KSC powoduje, że proces reagowania na incydenty przestaje być wyłącznie zagadnieniem technicznym, a staje się obszarem podwyższonego ryzyka regulacyjnego. Uczelnie mogą być zmuszone do rozbudowy procedur, formularzy, klasyfikacji incydentów oraz mechanizmów raportowania, nawet w odniesieniu do zdarzeń o niskim wpływie operacyjnym. W efekcie zasoby techniczne i kadrowe są kierowane na obsługę wymogów formalnych, a nie na realne ograniczanie skutków incydentów.

Dodatkowym problemem jest konieczność zapewnienia spójności pomiędzy procedurami wewnętrznymi uczelni a wymaganiami raportowymi wobec właściwych CSIRT-ów. W środowisku akademickim, charakteryzującym się dużą liczbą zdarzeń

[59] ISO/IEC 27035-1:2016, *Information technology — Security techniques — Information security incident management*, International Organization for Standardization, https://www.iso.org/standard/60803.html

o niskiej krytyczności (np. próby phishingu, infekcje pojedynczych stacji roboczych), może to prowadzić do nadmiernej eskalacji zdarzeń oraz przeciążenia zespołów technicznych obowiązkami administracyjnymi.
Z perspektywy technicznej wdrożenie obsługi incydentów zgodnej z oczekiwaniami interpretacyjnymi KSC wymaga zastosowania narzędzi wspierających cały cykl życia incydentu, takich jak systemy ticketowe klasy enterprise, platformy SOAR, centralne repozytoria logów oraz mechanizmy gromadzenia dowodów cyfrowych. Rozwiązania te generują istotne koszty wdrożeniowe i operacyjne, które nie zawsze pozostają proporcjonalne do rzeczywistego profilu ryzyka uczelni.
W porównaniu z podejściem promowanym w normach ISO oraz w regulacjach unijnych, które kładą nacisk na skuteczność reagowania i uczenie się organizacji na podstawie incydentów, KSC w aktualnym kształcie sprzyja formalizacji procesu obsługi incydentów. W rezultacie uczelnie wyższe mogą spełniać wymogi dokumentacyjne i raportowe, nie osiągając jednocześnie istotnego wzrostu zdolności technicznych do szybkiego wykrywania, izolowania i neutralizowania zagrożeń.

6.8. Testowanie bezpieczeństwa i audyty techniczne – skuteczność techniczna a wymogi KSC:

Testowanie bezpieczeństwa systemów informatycznych, obejmujące testy podatności, testy penetracyjne oraz inne formy weryfikacji technicznej, stanowi istotny element oceny skuteczności wdrożonych zabezpieczeń. W środowisku uczelni wyższych działania te mogą być realizowane z różną regularnością, często incydentalnie lub reaktywnie, w odpowiedzi na wystąpienie incydentu lub istotnej zmiany w infrastrukturze IT.
European Union Agency for Cybersecurity (ENISA) wskazuje, że **brak systematycznego i planowego testowania bezpieczeństwa** znacząco ogranicza zdolność organizacji do **wczesnej identyfikacji podatności technicznych**, zanim zostaną one wykorzystane przez podmioty nieuprawnione. ENISA podkreśla jednocześnie, że **testy bezpieczeństwa (w tym testy podatności i testy penetracyjne) powinny stanowić integralny element ciągłego cyklu doskonalenia cyberbezpieczeństwa**, obejmującego ocenę ryzyka, wdrażanie środków ochronnych oraz weryfikację ich skuteczności[60]. W podejściu eksperckim testy te powinny być planowane w oparciu o analizę ryzyka, krytyczność zasobów oraz zmiany w architekturze systemów.

[60] European Union Agency for Cybersecurity (ENISA), Handbook for Cyber Stress Tests, ENISA, 2025, https://www.enisa.europa.eu/sites/default/files/2025-05/2025.04311_01_ms_v2.0_Handbook%20for%20Cyber%20Stress%20Tests_en.pdf

W kontekście Krajowego Systemu Cyberbezpieczeństwa zagadnienie testowania bezpieczeństwa ulega jednak znacznemu sformalizowaniu. KSC, poprzez obowiązki wykazania skuteczności stosowanych środków technicznych oraz gotowości do kontroli i audytów, w praktyce wymusza regularne i udokumentowane testy bezpieczeństwa, niezależnie od rzeczywistego profilu ryzyka uczelni. Brak dowodów przeprowadzonych testów może zostać zakwalifikowany jako luka w realizacji obowiązków ustawowych, nawet w sytuacji, gdy nie występują przesłanki podwyższonego ryzyka technicznego.
Nadregulacyjny charakter KSC powoduje, że testy podatności i testy penetracyjne stają się nie tylko narzędziem technicznym, lecz również elementem obciążenia formalno-audytowego. Uczelnie mogą być zmuszone do przeprowadzania testów w stałych cyklach czasowych lub po każdej istotniejszej zmianie infrastruktury, przy jednoczesnym obowiązku dokumentowania ich zakresu, wyników oraz działań naprawczych. W praktyce prowadzi to do sytuacji, w której celem testowania staje się spełnienie wymogów audytowych, a nie optymalizacja poziomu bezpieczeństwa.
Dodatkowym problemem jest konieczność zapewnienia niezależności i odpowiedniego poziomu kompetencji podmiotów realizujących testy bezpieczeństwa. W przypadku uczelni wyższych, które często korzystają z rozwiązań niszowych lub środowisk badawczych o podwyższonej wrażliwości, przeprowadzanie testów penetracyjnych wiąże się z ryzykiem zakłócenia ciągłości pracy dydaktycznej lub badawczej. KSC nie przewiduje jednak elastycznych mechanizmów uznawania alternatywnych form testowania (np. ograniczonych testów zakresowych, przeglądów architektury czy analiz konfiguracyjnych) jako równoważnych z pełnymi testami penetracyjnymi.
W porównaniu z podejściem promowanym przez ENISA oraz regulacje unijne, które akcentują proporcjonalność, zarządzanie ryzykiem i dostosowanie zakresu testów do krytyczności zasobów, KSC w aktualnym kształcie sprzyja uniformizacji i formalizacji procesu testowania bezpieczeństwa. Dla uczelni wyższych oznacza to istotne obciążenia organizacyjne i finansowe, które nie zawsze przekładają się na adekwatny wzrost realnej odporności cybernetycznej.

6.9. Wniosek AS-IS cyberbezpieczeństwa dla uczelni wyższych:

Analiza techniczna stanu AS-IS cyberbezpieczeństwa w uczelniach wyższych wskazuje, że środowisko IT tego sektora cechuje się wysoką złożonością oraz heterogenicznością wynikającą z wieloletniego, ewolucyjnego rozwoju infrastruktury. W praktyce oznacza to współistnienie systemów nowoczesnych z rozwiązaniami typu *legacy*, rozproszenie odpowiedzialności technicznej oraz ograniczoną standaryzację

konfiguracji i polityk bezpieczeństwa. W wielu uczelniach dominują działania o charakterze reaktywnym, a priorytety techniczne są kształtowane przez potrzeby dostępności usług dydaktycznych i badawczych, co może prowadzić do tolerowania ryzyk technicznych (np. opóźnionego patchowania, ograniczonej segmentacji, braku pełnej inwentaryzacji).

a) **Zdolność detekcji i reagowania jest kluczowym punktem krytycznym**

W licznych środowiskach akademickich zdolność centralnego monitorowania zdarzeń bezpieczeństwa (SIEM/log management), rozszerzonej telemetrii endpointów (EDR/XDR) oraz całodobowego nadzoru (SOC/MDR) bywa ograniczona lub fragmentaryczna. Skutkiem jest opóźnione wykrywanie incydentów, słaba widoczność ataków wieloetapowych oraz trudności w analizie przyczyn źródłowych. W reżimie KSC problem ten ma dodatkowy wymiar: brak „dowodów operacyjnych" (logów, rejestrów, ścieżek eskalacji, zapisów działań) może zostać oceniony jako luka w realizacji obowiązków, niezależnie od faktycznego poziomu ryzyka technicznego. W podejściu NIS2, choć nadal wymagane są środki zarządzania ryzykiem, nacisk przesuwa się na skuteczność i proporcjonalność mechanizmów, co sprzyja modelom „managed services" i mierzalnej odporności zamiast formalnej rozbudowy dokumentacji.

b) **Zarządzanie tożsamością i dostępem (IAM) jest niedojrzałe w relacji do skali środowiska**

Uczelnie, z uwagi na dużą liczbę kont (studenci, doktoranci, pracownicy, goście, współpracownicy z grantów) oraz wysoką rotację, są szczególnie wrażliwe na nadużycia tożsamości, phishing i przejęcia kont. W wielu przypadkach obserwuje się ograniczoną centralizację zarządzania dostępem (brak spójnych polityk MFA, segmentacji uprawnień, PAM dla kont uprzywilejowanych, cyklicznych przeglądów uprawnień). Z perspektywy KSC niedojrzałość IAM generuje zarówno ryzyko operacyjne (eskalacja ataku w sieci), jak i ryzyko formalne (trudność wykazania, że organizacja „zapewnia" adekwatne środki ochrony). NIS2 wprost wzmacnia logikę zarządzania ryzykiem i bezpieczeństwa dostępu jako elementu „cyklu bezpieczeństwa" (technika + proces + odpowiedzialność).

c) **Patch management i podatności – konflikt bezpieczeństwo vs stabilność usług**

W uczelniach często występuje napięcie pomiędzy wymaganiem szybkiego wdrażania poprawek bezpieczeństwa a potrzebą stabilności systemów dydaktycznych i badawczych, zwłaszcza w środowiskach z oprogramowaniem specjalistycznym, laboratoriami i systemami legacy. Braki w automatyzacji aktualizacji, ograniczone środowiska testowe oraz koszt testów regresji mogą skutkować opóźnieniami w patchowaniu. W reżimie KSC problem ten może być

wzmacniany przez formalizację procesu (procedury, dowody, audytowalność), co zwiększa koszty operacyjne i przesuwa uwagę z realnego ograniczania ryzyka na minimalizowanie ryzyka regulacyjnego. W ujęciu NIS2 nacisk kładzie się na proporcjonalność i skuteczność środków – organizacja powinna móc uzasadniać decyzje (np. odroczenie patcha) środkami kompensacyjnymi (segmentacja, monitoring, ograniczenie uprawnień), co jest podejściem bardziej „inżynierskim" niż formalno-administracyjnym.

e) Odporność na ransomware – backup bez testów nie stanowi odporności

W wielu organizacjach kopie zapasowe są wykonywane, lecz rzadziej testuje się odtwarzanie, weryfikuje integralność backupów oraz mierzy rzeczywiste parametry odtworzenia (RTO/RPO). Bez testów odtworzeniowych backup pozostaje mechanizmem deklaratywnym, a nie operacyjnym. W KSC ryzyko to może zostać wzmocnione przez wymóg „wykazania" zdolności ciągłości działania (dowody testów, protokoły, wyniki ćwiczeń), co w praktyce wymusza inwestycje w droższe architektury kopii (np. separacja, niezmienność danych, dodatkowe lokalizacje) i cykliczne ćwiczenia. NIS2 kierunkowo wspiera wymaganie realnej odporności i testowania, jednak logika wdrożenia jest bardziej oparta na zarządzaniu ryzykiem i mierzalności niż na samej procedurze.

f) Testowanie bezpieczeństwa i audyty techniczne – ryzyko „compliance -driven testing"

Testy podatności i testy penetracyjne są ważne, ale w środowiskach uczelni wyższych mogą być realizowane nieregularnie (koszty, obawy o zakłócenia działania, brak zasobów). W reżimie KSC istnieje ryzyko, że testowanie będzie napędzane przede wszystkim wymogiem audytowalności i kontroli, a nie optymalnym doborem działań do profilu ryzyka (np. testy ukierunkowane na krytyczne systemy, segmenty sieci i procesy). W podejściu NIS2 większy nacisk kładzie się na demonstrację skuteczności i zarządzanie ryzykiem, co w praktyce sprzyja bardziej selektywnemu i uzasadnionemu doborowi testów.

g) Największe ryzyko systemowe: brak spójnego modelu technicznego + brak dowodów operacyjnych

W ujęciu syntetycznym kluczowym problemem technicznym sektora uczelni wyższych nie jest brak pojedynczych narzędzi, lecz brak zintegrowanego modelu bezpieczeństwa obejmującego: IAM (MFA/PAM), monitoring (SIEM/EDR/SOC), patch management (z testami regresji), backup/DR (z testami odtworzeniowymi) oraz cykliczne testowanie bezpieczeństwa. Jednocześnie w KSC szczególnie dotkliwy staje się brak „dowodów operacyjnych" (logów, protokołów testów, rejestrów incydentów, wyników ćwiczeń), co może prowadzić do sytuacji, w której organizacja podejmuje

działania techniczne, ale nie jest w stanie wykazać ich weryfikowalności i skuteczności.

Wniosek końcowy AS IS: Z perspektywy KSC oraz dyrektywy NIS2 uczelnie wyższe, aby osiągnąć realną odporność cybernetyczną, muszą przejść od punktowych zabezpieczeń technicznych do zintegrowanego modelu cyberbezpieczeństwa opartego na ryzyku, mierzalnej skuteczności oraz dowodach działania. Jednocześnie w warunkach nadregulacji KSC ryzykiem staje się to, że transformacja będzie motywowana głównie wymogami formalnymi i sankcyjnymi, a nie optymalizacją bezpieczeństwa – co zwiększa koszty i utrudnia proporcjonalne wdrożenie środków technicznych adekwatnych do profilu uczelni.

7. Ocena zgodności uczelni wyższych z wymaganiami Krajowego Systemu Cyberbezpieczeństwa oraz analiza nadregulacji do dyrektywy NIS2:

7.1. Cel i metodologia oceny zgodności

Celem przeprowadzonej oceny było zbadanie stopnia zgodności organizacyjnej i technicznej uczelni wyższych z wymaganiami Krajowego Systemu Cyberbezpieczeństwa (KSC) oraz identyfikacja luki regulacyjnej i operacyjnej w odniesieniu do dyrektywy NIS2. Analiza została przeprowadzona w oparciu o podejście porównawcze, łączące metodologię compliance-based (zgodność formalna z przepisami) oraz risk-based (zarządzanie ryzykiem i skuteczność środków bezpieczeństwa).

Zastosowanie obu podejść było celowe i wynikało z istotnych różnic pomiędzy logiką regulacyjną KSC a kierunkiem wyznaczonym przez dyrektywę NIS2. KSC, jako akt prawa krajowego, koncentruje się na określeniu katalogu obowiązków formalnych, organizacyjnych i dokumentacyjnych, których spełnienie ma charakter minimalny i weryfikowalny administracyjnie. W praktyce prowadzi to do oceny zgodności w oparciu o istnienie procedur, dokumentów, struktur organizacyjnych oraz zdolność do wykazania ich wdrożenia w toku kontroli[61].

Jednocześnie konstrukcja KSC powoduje istotne ryzyko nadregulacji, polegające na przesunięciu ciężaru oceny cyberbezpieczeństwa z obszaru faktycznej odporności

[61] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity), ISAP, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

technicznej i organizacyjnej na obszar spełnienia wymogów formalnych. W takim modelu organizacja może zostać uznana za niezgodną z przepisami pomimo podejmowania racjonalnych, opartych na analizie ryzyka działań technicznych, jeśli działania te nie zostały ujęte w odpowiednio sformalizowanej i audytowalnej dokumentacji.

W przeciwieństwie do tego dyrektywa NIS2 podnosi próg oczekiwań wobec podmiotów objętych regulacją, kładąc nacisk na skuteczność zarządzania ryzykiem cyberbezpieczeństwa, mierzalność wdrożonych środków oraz aktywną odpowiedzialność najwyższego kierownictwa. Metodologia NIS2 opiera się na ocenie zdolności organizacji do zapobiegania, wykrywania, reagowania i odtwarzania po incydentach, a nie wyłącznie na formalnym spełnieniu określonych obowiązków[62].

W kontekście uczelni wyższych różnica ta ma fundamentalne znaczenie. Przyjęcie wyłącznie podejścia compliance-based, charakterystycznego dla KSC, może prowadzić do koncentracji zasobów na spełnianiu wymogów administracyjnych, kosztem inwestycji w realne zdolności techniczne i organizacyjne. Z kolei podejście risk-based, promowane przez NIS2, umożliwia dostosowanie zakresu i głębokości zabezpieczeń do rzeczywistego profilu ryzyka, skali działalności badawczej oraz krytyczności świadczonych usług.

Metodologia zastosowana w niniejszej ocenie zakładała zatem:

- analizę formalnej zgodności z obowiązkami KSC (struktury, dokumentacja, procesy),
- ocenę dojrzałości technicznej i organizacyjnej w odniesieniu do obszarów wskazanych w NIS2,
- identyfikację obszarów, w których nadregulacja KSC może prowadzić do nieproporcjonalnych obciążeń organizacyjnych i finansowych,

[62] 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 (NIS2), EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

- określenie luki pomiędzy zgodnością deklaratywną a rzeczywistą odpornością cybernetyczną.

Tak przyjęta metodologia pozwala nie tylko na ocenę aktualnego poziomu zgodności, lecz również na sformułowanie wniosków dotyczących racjonalności i proporcjonalności obowiązków nakładanych na uczelnie wyższe w krajowym systemie cyberbezpieczeństwa w zestawieniu z kierunkiem regulacyjnym Unii Europejskiej.

7.2. Zgodność formalna z KSC – ujęcie organizacyjne:

Analiza zgodności formalnej z wymaganiami Krajowego Systemu Cyberbezpieczeństwa w uczelniach wyższych koncentruje się przede wszystkim na istnieniu wymaganych struktur organizacyjnych, procedur wewnętrznych oraz dokumentacji potwierdzającej realizację obowiązków ustawowych. W ujęciu compliance-based kluczowe znaczenie mają takie elementy jak formalne wyznaczenie odpowiedzialności za cyberbezpieczeństwo, posiadanie procedur obsługi incydentów, utrzymywanie kontaktu z właściwymi zespołami CSIRT oraz prowadzenie udokumentowanych działań w zakresie zarządzania ryzykiem.

Do najczęściej weryfikowanych obszarów należą w szczególności:

- formalne przypisanie odpowiedzialności za cyberbezpieczeństwo na poziomie organizacyjnym,
- istnienie procedur identyfikacji, obsługi i zgłaszania incydentów,
- mechanizmy współpracy i raportowania do właściwych CSIRT,
- posiadanie dokumentacji analizy ryzyka cyberbezpieczeństwa.

Z perspektywy KSC spełnienie powyższych wymogów stanowi podstawę uznania organizacji za zgodną z przepisami. Jednocześnie konstrukcja regulacji powoduje, że ocena zgodności ma charakter w dużej mierze formalny i dokumentacyjny, a nie operacyjny. W praktyce oznacza to, że kluczowym kryterium staje się posiadanie odpowiednich dokumentów, struktur i procedur, niezależnie od ich rzeczywistego funkcjonowania i skuteczności.

Najwyższa Izba Kontroli wskazuje, że w wielu jednostkach sektora publicznego spełnienie wymogów w obszarze cyberbezpieczeństwa ma charakter deklaratywny,

a dokumentacja bezpieczeństwa nie jest spójnie powiązana z praktyką operacyjną ani codziennymi procesami zarządzania systemami informatycznymi[63]. Procedury funkcjonują często jako odrębny byt formalny, przygotowany na potrzeby kontroli lub audytu, bez realnego wpływu na sposób reagowania na incydenty czy podejmowania decyzji technicznych.

W kontekście uczelni wyższych problem ten jest dodatkowo wzmacniany przez specyfikę organizacyjną sektora akademickiego, charakteryzującą się rozproszeniem struktur decyzyjnych, autonomią jednostek oraz dużą liczbą użytkowników. W takich warunkach formalne wyznaczenie odpowiedzialności za cyberbezpieczeństwo nie zawsze przekłada się na faktyczne umocowanie decyzyjne, dostęp do zasobów ani możliwość egzekwowania jednolitych standardów bezpieczeństwa w całej organizacji.

Nadregulacyjny charakter KSC powoduje, że uczelnie mogą osiągać stan tzw. **pozornej zgodności**, w którym wymogi formalne są spełnione na poziomie dokumentacyjnym, lecz nie prowadzą do istotnego wzrostu odporności organizacyjnej na incydenty cyberbezpieczeństwa. W takim modelu:

- zarządzanie ryzykiem ma charakter statyczny i nie jest integrowane z procesami decyzyjnymi,
- procedury obsługi incydentów nie są regularnie testowane ani doskonalone,
- współpraca z CSIRT ogranicza się do spełnienia obowiązku raportowego,
- odpowiedzialność kierownictwa ma charakter formalny, bez realnego nadzoru nad skutecznością środków bezpieczeństwa.

Z perspektywy organizacyjnej oznacza to, że KSC sprzyja budowie systemu cyberbezpieczeństwa opartego na zgodności formalnej, a nie na zarządzaniu ryzykiem i ciągłym doskonaleniu. W porównaniu z podejściem przyjętym w dyrektywie NIS2, która akcentuje odpowiedzialność kierownictwa, mierzalność skuteczności oraz integrację cyberbezpieczeństwa z governance organizacji, KSC koncentruje się na spełnieniu minimalnych obowiązków, co w przypadku uczelni wyższych może

[63] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

prowadzić do nieproporcjonalnych obciążeń administracyjnych przy ograniczonym efekcie bezpieczeństwa.

7.3. Główne obszary niezgodności z KSC w uczelniach wyższych:

Na podstawie analizy literatury przedmiotu, raportów kontrolnych, obserwacji praktyk wdrożeniowych oraz doświadczeń sektora akademickiego można wyróżnić typowe obszary niezgodności uczelni wyższych z wymaganiami Krajowego Systemu Cyberbezpieczeństwa (KSC) [64]. Wiele z tych niezgodności ma charakter systemowy, a nie jedynie techniczny, i wynika z niedojrzałości procesów governance oraz braku integracji cyberbezpieczeństwa z zarządzaniem ryzykiem i ciągłością działania.

Główne obszary niezgodności to:

a) **Brak formalnego i scentralizowanego systemu zarządzania ryzykiem cyberbezpieczeństwa** – w wielu przypadkach uczelnie prowadzą analizy ryzyka ad hoc lub jedynie na potrzeby wykazania zgodności formalnej. Tymczasem KSC oczekuje systemowego i cyklicznego podejścia do zarządzania ryzykiem, w tym dowodów na weryfikację skuteczności środków bezpieczeństwa. Brak tego elementu prowadzi do rozbieżności między spełnieniem wymogów formalnych a realnym ograniczaniem ryzyka operacyjnego.
b) **Niejednoznaczny podział ról i odpowiedzialności** – pomimo formalnego przypisania odpowiedzialności kierownikowi jednostki, w praktyce role związane z cyberbezpieczeństwem (CISO / Pełnomocnik, zespoły IT, IOD) pozostają nieuporządkowane, co utrudnia realizację obowiązków wynikających z KSC. To z kolei wpływa na jakość obsługi incydentów, zarządzania ryzykiem oraz monitorowania zgodności.
c) **Brak testów planów ciągłości działania (BCP/DR)** – choć KSC wskazuje obowiązek zapewnienia odporności usług, uczelnie często ograniczają się do posiadania planów dokumentacyjnych, bez regularnych testów odtwarzania, scenariuszy kryzysowych czy weryfikacji realnych parametrów

[64]Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity), ISAP, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560.,

RTO/RPO. W efekcie deklaratywne procedury nie przekładają się na zdolność organizacji do reagowania na incydenty.

d) **Ograniczona współpraca organizacyjna w zakresie obsługi incydentów** – w praktyce uczelnie wyższe mogą nie posiadać formalnych mechanizmów współpracy między działami IT, CSIRT a procesami zarządzania ryzykiem, co skutkuje fragmentaryczną odpowiedzią na incydenty. W kontekście KSC brak takiej integracji stanowi lukę w realizacji obowiązków ustawowych.

European Union Agency for Cybersecurity podkreśla, że tego rodzaju luki mają charakter systemowy i wynikają z niedojrzałości governance, a nie z braku pojedynczych narzędzi technicznych. Skuteczna odporność cybernetyczna wymaga zintegrowanego podejścia, w którym cyberbezpieczeństwo jest traktowane jako element systemu zarządzania organizacją, a nie jedynie jako obszar IT lub zbiór procesów formalnych[65].

Należy zauważyć, że **projektowane zmiany w KSC**, które mają na celu uszczegółowienie obowiązków i mechanizmów nadzoru, mogą wzmocnić formalne aspekty zgodności, ale jednocześnie **potęgować ryzyko nadregulacji** – przesuwając ciężar oceny z dowodów operacyjnych i skuteczności działań na realizację obowiązków dokumentacyjnych i proceduralnych. W takim modelu organizacje, w tym uczelnie wyższe, mogą formalnie wykazywać zgodność z zasadami KSC, nie osiągając jednocześnie adekwatnego poziomu realnej odporności na incydenty cybernetyczne.

W kontekście wymogów unijnych określonych w dyrektywie NIS2[66], problem ten jest dodatkowo uwydatniony. NIS2 koncentruje się bardziej na skuteczności środków zarządzania ryzykiem, odpowiedzialności kierownictwa i mierzalnej odporności, a mniej na samym spełnieniu katalogu formalnych obowiązków. Zatem luka między

[65] European Union Agency for Cybersecurity (ENISA), A Governance Framework for National Cybersecurity Strategies, ENISA, 28 Feb 2023,https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies

[66] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

zgodnością formalną (KSC) a zgodnością skuteczną (NIS2) uwidacznia się szczególnie w obszarach, takich jak:

- realne wdrożenie systemu zarządzania ryzykiem zgodnie z podejściem risk -based,
- powiązanie polityk i procedur z mierzalnymi KPI i wskaźnikami bezpieczeństwa,
- zdolność do wykazywania skuteczności środków (analizy po incydentach, retrospekcje),
- integracja cyberbezpieczeństwa z decyzjami strategicznymi organizacji.

7.4. Dyrektywa NIS2 jako punkt odniesienia do analizy nadregulacji w KSC

Dyrektywa (UE) 2022/2555, znana jako **NIS2**, istotnie rozszerza zakres oczekiwań wobec odporności cybernetycznej organizacji w porównaniu do Krajowego Systemu Cyberbezpieczeństwa (KSC). Dyrektywa ta wprowadza bardziej precyzyjne wymagania dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa, nadzoru nad ich skutecznością oraz odpowiedzialności najwyższego kierownictwa podmiotu. Szczególne znaczenie ma **art. 21 dyrektywy NIS2**, który wskazuje szczegółowy katalog obszarów, jakie powinny zostać objęte działaniami ochronnymi[1].

W kontekście uczelni wyższych dyrektywa NIS2 wymusza przejście od podejścia opartego głównie na dokumentacji i formalnym spełnianiu obowiązków, charakterystycznego dla KSC, do podejścia opartego na dowodach skuteczności wdrożonych środków zarządzania ryzykiem, ich monitorowaniu i ciągłym doskonaleniu. NIS2 zakłada nie tylko istnienie polityk, procedur i planów działania, lecz również wymaga wykazania ich faktycznej efektywności w praktyce operacyjnej.

Kluczowe różnice metodologiczne: NIS2 vs KSC

Obszar regulacyjny	Dyrektywa NIS2	Projekt ustawy KSC
Model zgodności	*Risk-based*: wykazanie skuteczności działań i ich wpływu na odporność	*Compliance-based*: spełnienie katalogu obowiązków i formalnych kryteriów
Odpowiedzialność kierownictwa	Silne powiązanie z governance i strategicznym nadzorem	Formalne przypisanie odpowiedzialności, często bez realnych narzędzi nadzoru
Zarządzanie ryzykiem	Konieczność rzetelnej identyfikacji, oceny i działań w cyklu życia ryzyka	Podejście ogólne, brak wymogów dowodzenia skuteczności środków
Dowody działania	Wymagane dowody operacyjne: logi, testy, metryki, wyniki auditów	Wymogi dokumentacyjne bez wyraźnej wymogi mierzalności
Środki techniczne	Proporcjonalne i relatywne do profilu ryzyka	Katalog formalnych środków, często „checkbox compliance”
Raportowanie/zgłaszanie	Ramy czasowe i zakres określone, nacisk na treść i jakość informacji	Wymogi formalne bez nacisku na znaczenie treści

7.5. Nadregulacja KSC w świetle NIS2

W świetle NIS2 nadregulacja KSC może przejawiać się na kilku poziomach:

1. **Formalna koncentracja na dokumentacji** – KSC akcentuje posiadanie procedur, polityk i planów jako podstawowych dowodów zgodności, podczas gdy NIS2 wymaga, aby te elementy prowadziły do rzeczywistych działań i rezultatów, a nie jedynie istniały na papierze.
2. **Brak wyraźnej miary skuteczności** – KSC nie precyzuje wskaźników ani metryk, które pozwalałyby dowieść, że środki zarządzania ryzykiem faktycznie działają. NIS2 oczekuje takich dowodów operacyjnych, co czyni ocenę nie tylko formalną, ale i faktyczną.
3. **Ograniczona rola governance** – KSC formalnie przypisuje odpowiedzialność kierownikowi jednostki, nie stawiając równie silnych nacisków na strategiczne zarządzanie ryzykiem i jego mierzalność, jak czyni to NIS2, np. przez wymagania dotyczące roli kierownictwa oraz przejrzyste dowody działania.
4. **Podejście „checkbox compliance" vs odporność operacyjna** – KSC, szczególnie w wersji projektowanej, może prowadzić do sytuacji, w której działania są projektowane pod kątem „udowodnienia zgodności", a nie pod kątem faktycznej zwiększonej odporności na realne zagrożenia.

Te różnice metodologiczne sprawiają, że zgodność formalna z KSC nie zawsze odpowiada celom i intencjom NIS2, szczególnie w kontekście organizacji o charakterze akademickim, gdzie specyfika procesów, heterogeniczna infrastruktura oraz rotacja użytkowników wymagają podejścia *risk-based* i *evidence-based*.

Wniosek

Podsumowując, dyrektywa NIS2 stanowi ważny punkt odniesienia dla analizy nadregulacji KSC, wskazując, że ujmowanie zgodności jedynie jako spełnienia katalogu obowiązków formalnych jest niewystarczające w kontekście budowania rzeczywistej odporności cybernetycznej organizacji. Wymagania NIS2 – skoncentrowane na skuteczności działań, mierzalności środków bezpieczeństwa i odpowiedzialności kierownictwa – dostarczają ram, które uwypuklają niedostatki i nadregulacyjne elementy polskiego systemu KSC.

7.6. Analiza dysproporcji organizacyjnej pomiędzy KSC a NIS2 (w świetle projektu nowelizacji KSC)

Analiza dysproporcji organizacyjnej pomiędzy KSC a NIS2[67] wskazuje, że największe różnice – istotne szczególnie dla uczelni wyższych – dotyczą: (1) roli i odpowiedzialności kierownictwa, (2) sposobu sprawowania formalnego nadzoru nad cyberbezpieczeństwem, oraz (3) integracji cyberbezpieczeństwa z zarządzaniem strategicznym i budżetowym.

Z perspektywy NIS2 kluczowe jest odejście od modelu, w którym cyberbezpieczeństwo jest obszarem „technicznym", delegowanym do IT, na rzecz modelu governance, w którym najwyższe kierownictwo odpowiada za zatwierdzanie, nadzorowanie i rozliczanie środków zarządzania ryzykiem. ENISA w materiałach dot. NIS2 podkreśla, że dyrektywa wzmacnia filary: obowiązki podmiotów, nadzór i wymagania dotyczące zarządzania ryzykiem, w tym w sposób „systemowy", a nie wyłącznie proceduralny[68].

7.7. Wpływ projektu nowelizacji KSC: przesunięcie z „minimalnych obowiązków" w stronę reżimu nadzorczo-sankcyjnego

Wprowadzenie projektu nowelizacji KSC (wprost implementującego NIS2 do porządku krajowego) istotnie zmienia punkt odniesienia dla oceny organizacyjnej. Projekt nie tylko przenosi logikę NIS2 (podmioty kluczowe/ważne, podejście risk -based), ale równolegle wzmacnia instrumenty krajowe, które w praktyce mogą tworzyć **dysproporcję regulacyjną** (tj. obciążenia organizacyjne wykraczające poza

[67] Dyrektywa (UE) 2022/2555 (NIS2), EUR-Lex (tekst aktu), https://eur-lex.europa.eu/eli/dir/2022/2555/oj .
[68] ENISA, *Network and Information Systems Directive 2 (NIS2) – information campaign / materiały wyjaśniające*, https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2.

„czyste" minimum NIS2 albo prowadzące do silniejszego nacisku na formalny nadzór). Sam fakt formalnej publikacji projektu przez Ministerstwo Cyfryzacji (BIP) potwierdza aktualność kierunku regulacyjnego i jego bezpośrednie przełożenie na sektor publiczny, w tym potencjalnie uczelnie[69].

W praktyce projektowane zmiany KSC mogą podbić „koszt organizacyjny" zgodności w trzech obszarach:

a) **Odpowiedzialność kierownictwa + realne ryzyko sankcyjne**
W projekcie KSC (wg analiz rynkowych omawiających nowe przepisy) przewidziano kary administracyjne powiązane z progiem „milionowym" oraz procentem przychodów, a w określonych, szczególnie poważnych przypadkach – dodatkowo możliwość nałożenia sankcji o bardzo wysokiej wartości w PLN. To wzmacnia presję na kierownictwo, aby cyberbezpieczeństwo traktować jako ryzyko strategiczne, ale równocześnie zwiększa prawdopodobieństwo wdrożeń „pod kontrolę", tj. skoncentrowanych na formalnej wykazywalności zgodności zamiast na proporcjonalności środków do profilu ryzyka uczelni[70].

b) **Formalny nadzór i „dowody działania" – wzrost obciążeń governance**
W modelu NIS2 nacisk kładzie się na skuteczność i zarządzanie ryzykiem (w tym mierzalność), a ENISA publikuje materiały, które wskazują jak budować dowody skuteczności (evidence)[71]. Jednocześnie projekt KSC – obok wdrożenia NIS2 – wzmacnia krajowe

[69] Ministerstwo Cyfryzacji, *Projekt ustawy o zmianie ustawy o KSC oraz niektórych innych ustaw* (publikacja projektu), https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw

[70] KPMG, *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – omówienie zakresu i sankcji*, https://kpmg.com/pl/pl/wiedza/podatki/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa.html

[71] ENISA, *NIS2 Technical Implementation Guidance* (przykłady dowodów i mapowania wymagań na środki), 26.06.2025, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

mechanizmy nadzoru, w tym rolę struktur sektorowych (np. CSIRT sektorowe) oraz formalne kanały współpracy/koordynacji. To może powodować, że uczelnia będzie musiała nie tylko „mieć" procedury, ale stale utrzymywać ekosystem: role, rejestry, raportowanie, metryki, ścieżki eskalacji i cykliczne przeglądy – w praktyce jako „żywy system zarządzania" (co jest zgodne z NIS2), lecz często realizowany w reżimie administracyjnej wykazywalności (co zwiększa koszty)[72].

c) **Integracja cyberbezpieczeństwa z zarządzaniem strategicznym: konieczność przebudowy modelu decyzyjnego**
Dla uczelni kluczowe staje się powiązanie cyberbezpieczeństwa z: planowaniem finansowym, zarządzaniem usługami krytycznymi (dydaktyka, rekrutacja, e-usługi), zakupami ICT i zarządzaniem dostawcami. Projekt KSC rozbudowuje warstwę systemową (m.in. nowe elementy współpracy, rola podmiotów sektorowych), co w praktyce wymusza reorganizację: ustanowienie właścicieli ryzyk i procesów, cykliczne przeglądy decyzji, protokołowanie nadzoru oraz włączenie cyber ryzyka do zarządzania strategicznego uczelni.

Wniosek operacyjny dla uczelni

W praktyce oznacza to, że uczelnie spełniające jedynie „minimalny" wariant KSC (w rozumieniu podejścia proceduralno-dokumentacyjnego) mogą być nieprzygotowane nie tylko do standardu NIS2, ale również do krajowego reżimu po nowelizacji KSC – ponieważ projekt wzmacnia instrumenty nadzoru i sankcji oraz formalizuje elementy systemowe (sektorowe CSIRT/SOC, mechanizmy koordynacyjne). W efekcie dysproporcja organizacyjna pomiędzy „zgodnością deklaratywną" a „odpornością + wykazywalnością" staje się jednym z głównych ryzyk wdrożeniowych w sektorze szkolnictwa wyższego.

[72] Cyberpolicy NASK, *Nowy projekt nowelizacji ustawy o KSC – omówienie kluczowych zmian (m.in. CSIRT sektorowe, SOC, dostawcy wysokiego ryzyka, rekomendacje)*, https://cyberpolicy.nask.pl/nowy-projekt-nowelizacji-ustawy-o-krajowym-systemie-cyberbezpieczenstwa/

7.8. Znaczenie dowodów operacyjnych w ocenie zgodności – NIS2 a nadregulacja KSC

Jednym z kluczowych elementów podejścia przyjętego w dyrektywie NIS2 jest wymóg wykazania skuteczności wdrożonych środków zarządzania ryzykiem cyberbezpieczeństwa poprzez **dowody operacyjne** (*evidence-based compliance*). Oznacza to konieczność posiadania i utrzymywania mierzalnych, aktualnych oraz możliwych do weryfikacji danych potwierdzających faktyczne funkcjonowanie systemu cyberbezpieczeństwa w organizacji.

Do podstawowych kategorii dowodów operacyjnych należą w szczególności:

- rejestry i klasyfikacje incydentów cyberbezpieczeństwa,
- raporty z testów bezpieczeństwa (testy podatności, testy penetracyjne),
- wyniki szkoleń, ćwiczeń i symulacji incydentów,
- metryki skuteczności działań, takie jak czas wykrycia incydentu (MTTD), czas reakcji (MTTR), skuteczność odtwarzania (RTO/RPO).

CERT Polska podkreśla, że brak takich dowodów znacząco utrudnia ocenę realnego poziomu cyberbezpieczeństwa organizacji oraz uniemożliwia obiektywną analizę skuteczności stosowanych środków ochronnych[73]. W praktyce oznacza to, że bez dowodów operacyjnych nie jest możliwe odróżnienie systemu bezpieczeństwa działającego efektywnie od systemu funkcjonującego wyłącznie na poziomie deklaratywnym.

7.9. Dowody operacyjne w modelu NIS2

W modelu NIS2 dowody operacyjne pełnią funkcję centralnego mechanizmu oceny zgodności. Dyrektywa zakłada, że podmiot powinien być w stanie wykazać:

[73] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025, https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

- **ciągłość procesu zarządzania ryzykiem**, a nie jednorazowe spełnienie wymogów,
- **skuteczność** wdrożonych środków technicznych i organizacyjnych,
- **aktywne zaangażowanie kierownictwa** w nadzór nad cyberbezpieczeństwem,
- **uczenie się organizacji** na podstawie incydentów, testów i ćwiczeń.

Takie podejście sprzyja budowie „żywego" systemu cyberbezpieczeństwa, w którym dokumentacja jest wtórna wobec danych operacyjnych, a zgodność regulacyjna wynika z faktycznego funkcjonowania procesów.

7.10. Nadregulacja KSC a dowody operacyjne

W Krajowym Systemie Cyberbezpieczeństwa pojęcie dowodów operacyjnych nie zostało wprost zdefiniowane ani systemowo osadzone w modelu oceny zgodności. W praktyce KSC akcentuje przede wszystkim:

- posiadanie procedur i polityk,
- formalne przypisanie ról i odpowiedzialności,
- spełnienie obowiązków raportowych i organizacyjnych.

Taki model sprzyja **nadregulacji dokumentacyjnej**, w której kluczowym kryterium oceny staje się istnienie dokumentów, a nie ich faktyczne zastosowanie i skuteczność. W konsekwencji organizacje, w tym uczelnie wyższe, mogą koncentrować się na tworzeniu i utrzymywaniu rozbudowanej dokumentacji bezpieczeństwa, bez równoległego rozwijania mechanizmów zbierania i analizy danych operacyjnych.

Projekt nowelizacji KSC, implementujący NIS2 do prawa krajowego, częściowo wzmacnia znaczenie skuteczności i nadzoru, jednak jednocześnie rozszerza katalog obowiązków formalnych oraz mechanizmów kontrolnych. Może to prowadzić do sytuacji, w której dowody operacyjne są gromadzone głównie na potrzeby wykazania zgodności administracyjnej, a nie jako narzędzie realnego zarządzania bezpieczeństwem.

Implikacje dla uczelni wyższych

Dla uczelni wyższych oznacza to istotne wyzwanie organizacyjne i kosztowe. Budowa systemu dowodów operacyjnych zgodnego z logiką NIS2 wymaga:

- wdrożenia narzędzi monitoringu i detekcji (SIEM, EDR, SOC/MDR),
- standaryzacji rejestrów incydentów i procesów raportowania,
- regularnych testów bezpieczeństwa i ćwiczeń,
- zbierania i analizowania metryk efektywności.

W reżimie nadregulacyjnym KSC istnieje ryzyko, że uczelnie będą zmuszone do prowadzenia **podwójnego wysiłku**: utrzymywania rozbudowanej dokumentacji formalnej oraz równoległego systemu dowodów operacyjnych, bez jasnego powiązania obu obszarów. Taki model zwiększa koszty zgodności i obciążenie organizacyjne, nie zawsze przekładając się na proporcjonalny wzrost realnej odporności cybernetycznej.

Wniosek

Podsumowując, podejście NIS2 jednoznacznie promuje ocenę zgodności opartą na dowodach operacyjnych i skuteczności działań. W porównaniu z tym modelem KSC – zarówno w wersji obowiązującej, jak i projektowanej – pozostaje regulacją o silnym charakterze formalno-administracyjnym. Dla uczelni wyższych oznacza to konieczność świadomego zaprojektowania systemu cyberbezpieczeństwa w taki sposób, aby dowody operacyjne stanowiły fundament zarządzania ryzykiem, a nie jedynie dodatkowy obowiązek narzucony przez krajowe wymogi regulacyjne.

<u>Wnioski z oceny zgodności oraz analizy dysproporcji regulacyjnej (KSC – NIS2)</u>

Przeprowadzona ocena zgodności z Krajowym Systemem Cyberbezpieczeństwa oraz analiza odniesienia do dyrektywy NIS2 wskazują, że kluczowe wyzwania stojące przed uczelniami wyższymi nie wynikają z niespełnienia pojedynczych, izolowanych wymagań regulacyjnych. Mają one charakter **systemowy** i dotyczą całościowego modelu zarządzania cyberbezpieczeństwem, obejmującego governance, odpowiedzialność kierownictwa, integrację ryzyka cybernetycznego z zarządzaniem strategicznym oraz dojrzałość techniczną i operacyjną.

W świetle projektu nowelizacji KSC szczególnie istotna staje się **dysproporcja regulacyjna** pomiędzy podejściem krajowym a logiką dyrektywy NIS2. NIS2 opiera się na modelu *risk-based* i *evidence-based*, koncentrując się na skuteczności wdrożonych środków, ich proporcjonalności do profilu ryzyka oraz realnym zaangażowaniu najwyższego kierownictwa w nadzór nad cyberbezpieczeństwem[1]. Tymczasem projektowane zmiany KSC, obok implementacji NIS2, wzmacniają krajowe mechanizmy nadzorcze, sankcyjne i dokumentacyjne, co w praktyce może prowadzić do **nadregulacji organizacyjnej**, szczególnie dotkliwej dla podmiotów sektora publicznego.

Nadregulacja a włączanie uczelni do kategorii „podmiotów ważnych"

Jednym z najbardziej kontrowersyjnych elementów projektowanej nowelizacji KSC jest potencjalne **rozszerzenie zakresu podmiotowego**, w tym możliwość kwalifikowania uczelni wyższych jako „podmiotów ważnych" ze względu na prowadzoną działalność badawczą. Takie podejście budzi istotne wątpliwości z punktu widzenia proporcjonalności regulacyjnej.

Dyrektywa NIS2 przewiduje objęcie regulacją przede wszystkim tych organizacji, które świadczą usługi o znaczeniu krytycznym dla funkcjonowania gospodarki i społeczeństwa lub prowadzą działalność badawczą o **strategicznym znaczeniu dla bezpieczeństwa państwa lub Unii**. Tymczasem projekt KSC nie wprowadza jednoznacznych, precyzyjnych kryteriów odróżniających działalność badawczą o charakterze strategicznym od szerokiego spektrum badań akademickich, które stanowią podstawową misję większości uczelni.

W praktyce może to prowadzić do **niepotrzebnego i nieproporcjonalnego włączania uczelni wyższych do reżimu właściwego dla podmiotów o podwyższonej krytyczności**, co skutkuje:

- znacznym wzrostem obowiązków organizacyjnych i dokumentacyjnych,
- koniecznością utrzymywania „żywego" systemu dowodów operacyjnych,
- zwiększonym ryzykiem sankcyjnym dla kierownictwa uczelni,

- trwałym obciążeniem budżetów uczelni kosztami zgodności, niezależnymi od realnego profilu ryzyka.

Skutki organizacyjne i techniczne nadregulacji

Analiza wykazała, że luka pomiędzy KSC a NIS2 – rozumiana jako **rozbieżność pomiędzy formalną zgodnością a skuteczną odpornością** – ma charakter zarówno organizacyjny, jak i techniczny. Projekt nowelizacji KSC może tę rozbieżność pogłębiać, jeśli nacisk regulacyjny będzie koncentrował się na spełnieniu wymogów administracyjnych, a nie na rzeczywistym zarządzaniu ryzykiem.

W szczególności uczelnie wyższe stają przed koniecznością:

- przejścia z modelu reaktywnego do **proaktywnego i zintegrowanego systemu cyberbezpieczeństwa**,
- powiązania cyberbezpieczeństwa z procesami decyzyjnymi i budżetowymi,
- wdrożenia rozwiązań technicznych umożliwiających generowanie dowodów operacyjnych (monitoring, detekcja, testy, ćwiczenia),
- zdefiniowania nowych ról organizacyjnych (właściciele ryzyk, właściciele procesów, nadzór kierownictwa).

Jednocześnie brak jasnego rozróżnienia pomiędzy uczelniami o rzeczywistym znaczeniu krytycznym a podmiotami realizującymi standardową działalność dydaktyczno-badawczą może skutkować **alokacją znacznych zasobów na zapewnienie zgodności formalnej**, bez adekwatnego wzrostu realnej odporności cybernetycznej.

Wniosek końcowy

Podsumowując, ocena zgodności z KSC oraz odniesienie do NIS2 wskazują, że główne wyzwania uczelni wyższych nie leżą w braku pojedynczych mechanizmów technicznych, lecz w **systemowej transformacji modelu zarządzania cyberbezpieczeństwem**. Projekt nowelizacji KSC, poprzez wzmocnienie instrumentów nadzorczych i sankcyjnych oraz nieprecyzyjne kryteria kwalifikacji podmiotów, niesie ryzyko nadregulacji, która może w sposób nieproporcjonalny obciążyć sektor szkolnictwa wyższego.

Z perspektywy racjonalnej implementacji NIS2 kluczowe znaczenie ma zapewnienie, aby uczelnie wyższe były obejmowane reżimem „podmiotów ważnych" wyłącznie w przypadkach uzasadnionych rzeczywistym znaczeniem prowadzonych badań, a nie na podstawie ogólnej charakterystyki działalności akademickiej. W przeciwnym razie zgodność regulacyjna może stać się celem samym w sobie, zamiast narzędziem budowy rzeczywistej, proporcjonalnej odporności cybernetycznej

8. Analiza ryzyka cyberbezpieczeństwa w uczelniach wyższych

8.1. Znaczenie analizy ryzyka w systemie cyberbezpieczeństwa

Analiza ryzyka cyberbezpieczeństwa stanowi fundament współczesnych systemów zarządzania bezpieczeństwem informacji oraz kluczowy element podejścia regulacyjnego przyjętego zarówno w Krajowym Systemie Cyberbezpieczeństwa, jak i w dyrektywie NIS2. Jej podstawowym celem jest identyfikacja zagrożeń, podatności oraz potencjalnych skutków ich materializacji, a następnie określenie poziomu ryzyka akceptowalnego dla organizacji oraz doboru adekwatnych środków zaradczych.

Zgodnie z normą ISO/IEC 27005, analiza ryzyka powinna mieć charakter ciągły, być zintegrowana z procesami zarządczymi organizacji oraz uwzględniać zarówno kontekst biznesowy, jak i technologiczny jednostki[74]. W tym ujęciu analiza ryzyka nie jest jednorazowym ćwiczeniem dokumentacyjnym, lecz dynamicznym procesem wspierającym podejmowanie decyzji strategicznych, alokację zasobów oraz priorytetyzację działań w obszarze cyberbezpieczeństwa.

W kontekście uczelni wyższych analiza ryzyka nabiera szczególnego znaczenia ze względu na rozproszoną strukturę organizacyjną, dużą liczbę użytkowników (studenci, pracownicy, doktoranci, współpracownicy zewnętrzni), znaczną rotację tożsamości oraz różnorodność przetwarzanych danych – od danych osobowych po dane badawcze o potencjalnym znaczeniu strategicznym. W takich warunkach

[74] International Organization for Standardization, *ISO/IEC 27005:2022 – Information security risk management*, https://www.iso.org/standard/80585.html

skuteczna analiza ryzyka powinna stanowić narzędzie integrujące perspektywę techniczną, organizacyjną i biznesową uczelni.

Analiza ryzyka w KSC – wymóg formalny a rzeczywista użyteczność

W Krajowym Systemie Cyberbezpieczeństwa analiza ryzyka została ujęta jako jeden z obowiązków organizacyjnych podmiotów objętych regulacją. Zarówno obowiązująca ustawa, jak i projekt jej nowelizacji, wskazują na konieczność podejścia opartego na ryzyku, jednak nie precyzują w sposób jednoznaczny metodologii, częstotliwości ani kryteriów oceny skuteczności prowadzonej analizy[75].

W praktyce prowadzi to do ryzyka nadregulacji formalnej, w której analiza ryzyka realizowana jest głównie w celu wykazania zgodności z przepisami, a nie jako realne narzędzie zarządcze. W sektorze publicznym, w tym w uczelniach wyższych, analiza ryzyka bywa sporządzana jednorazowo lub okresowo w formie dokumentu statycznego, który nie jest aktualizowany wraz ze zmianą architektury IT, profilu zagrożeń czy modelu działalności uczelni.

Projekt nowelizacji KSC, implementujący dyrektywę NIS2, wzmacnia wymóg stosowania podejścia risk-based, lecz jednocześnie rozszerza zakres odpowiedzialności formalnej i nadzorczej. Może to skutkować sytuacją, w której analiza ryzyka staje się narzędziem kontroli administracyjnej, a nie mechanizmem wspierającym decyzje strategiczne. W takim modelu kluczowe znaczenie zyskuje nie tyle jakość samej analizy, ile jej audytowalność i zgodność z oczekiwaniami organów nadzorczych.

Analiza ryzyka w NIS2 – podejście skutecznościowe

W odróżnieniu od KSC, dyrektywa NIS2 jednoznacznie wiąże analizę ryzyka z odpowiedzialnością najwyższego kierownictwa, skutecznością wdrożonych

[75]Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt ustawy o jej zmianie, ISAP / Ministerstwo Cyfryzacji, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw

środków oraz ich proporcjonalnością do rzeczywistego profilu zagrożeń[76]. Analiza ryzyka w NIS2 nie jest celem samym w sobie, lecz punktem wyjścia do:

- doboru środków technicznych i organizacyjnych,
- określenia priorytetów inwestycyjnych,
- nadzoru nad odpornością operacyjną,
- wykazywania skuteczności działań poprzez dowody operacyjne.

Takie podejście sprzyja traktowaniu analizy ryzyka jako elementu governance, a nie jedynie jako obowiązku formalnego.

Implikacje dla uczelni wyższych

W świetle nowelizacji KSC oraz wymogów NIS2 uczelnie wyższe stają przed wyzwaniem transformacji analizy ryzyka z narzędzia dokumentacyjnego w centralny mechanizm zarządzania cyberbezpieczeństwem. Jednocześnie nadregulacyjny charakter krajowych przepisów może powodować, że analiza ryzyka będzie realizowana w sposób nadmiernie sformalizowany, bez odpowiedniego przełożenia na decyzje organizacyjne i techniczne.

W konsekwencji istnieje ryzyko, że uczelnie:

- będą ponosiły znaczące koszty utrzymania formalnych analiz ryzyka,
- nie uzyskają realnej poprawy odporności cybernetycznej,
- skoncentrują się na minimalizacji ryzyka regulacyjnego zamiast ryzyka operacyjnego.

8.2. Metodologiczne podejście do analizy ryzyka cyberbezpieczeństwa

Analiza ryzyka cyberbezpieczeństwa w uczelniach wyższych powinna obejmować zarówno aspekty organizacyjne, jak i techniczne, a jej zakres musi uwzględniać specyfikę środowiska akademickiego. W ujęciu metodycznym oznacza to konieczność systematycznej identyfikacji:

[76] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

- kluczowych aktywów informacyjnych (dane osobowe, dane badawcze, systemy krytyczne),
- zagrożeń oddziałujących na te aktywa (technicznych, organizacyjnych i ludzkich),
- podatności systemów, procesów oraz struktur zarządczych,
- potencjalnych skutków materializacji zagrożeń, zarówno operacyjnych, jak i reputacyjnych czy finansowych.

European Union Agency for Cybersecurity rekomenduje stosowanie podejścia risk -based, w którym ryzyko definiowane jest jako funkcja prawdopodobieństwa wystąpienia zdarzenia oraz jego wpływu na organizację[77]. W takim modelu analiza ryzyka powinna być procesem iteracyjnym, aktualizowanym wraz ze zmianami architektury IT, modelu organizacyjnego oraz krajobrazu zagrożeń.

Zgodnie z dobrymi praktykami ENISA oraz normami ISO, analiza ryzyka powinna również:

- uwzględniać zależności pomiędzy aktywami,
- brać pod uwagę scenariusze ataków wieloetapowych,
- integrować perspektywę techniczną z kontekstem misji organizacji,
- stanowić podstawę doboru środków bezpieczeństwa i priorytetyzacji inwestycji.

Analiza ryzyka a praktyka uczelni wyższych

W praktyce funkcjonowania wielu uczelni wyższych analiza ryzyka cyberbezpieczeństwa ma jednak charakter formalny i statyczny. Często jest ona sporządzana jednorazowo lub okresowo w celu spełnienia wymogów regulacyjnych, bez rzeczywistej integracji z procesami decyzyjnymi, budżetowymi czy zarządczymi. Taki model znacząco ogranicza użyteczność analizy ryzyka w kontekście dynamicznie zmieniającego się krajobrazu zagrożeń.

[77] European Union Agency for Cybersecurity, *Risk Management – guidelines and good practices*, ENISA, 2022, https://www.enisa.europa.eu/topics/risk-management

Przyczyną tego stanu rzeczy nie jest wyłącznie brak świadomości organizacyjnej, lecz również presja regulacyjna, która skłania podmioty sektora publicznego do traktowania analizy ryzyka jako dokumentu „na potrzeby zgodności", a nie jako narzędzia zarządczego.

Nadregulacja KSC a metodologia analizy ryzyka

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa, implementujący dyrektywę NIS2, formalnie wzmacnia znaczenie podejścia opartego na ryzyku. Jednocześnie jednak rozszerza zakres odpowiedzialności formalnej oraz nadzorczej, co w praktyce może prowadzić do nadregulacji metodologicznej analizy ryzyka.

W szczególności:

- KSC nie narzuca jednej spójnej metodologii analizy ryzyka, lecz oczekuje jej audytowalności i wykazywalności,
- brak precyzyjnych kryteriów jakości analizy ryzyka sprzyja koncentracji na formie dokumentu, a nie na jego wartości decyzyjnej,
- analiza ryzyka może być oceniana przez pryzmat kompletności formalnej (zakres, podpisy, aktualność), a nie trafności przyjętych założeń i scenariuszy.

W efekcie analiza ryzyka w reżimie KSC może przekształcić się w narzędzie zarządzania ryzykiem regulacyjnym, a nie cybernetycznym. Organizacje dążą wówczas do minimalizacji ryzyka sankcji administracyjnych, a nie do rzeczywistego ograniczania ekspozycji na zagrożenia.

Porównanie podejścia: ENISA / NIS2 vs KSC (projekt)

Obszar	ENISA / NIS2	KSC (projekt)
Charakter analizy	Dynamiczna, iteracyjna	Często statyczna, okresowa
Cel	Wsparcie decyzji i odporności	Wykazanie zgodności
Kryterium oceny	Skuteczność i proporcjonalność	Audytowalność i kompletność

Obszar	ENISA / NIS2	KSC (projekt)
Integracja z zarządzaniem	Silna	Ograniczona
Ryzyko	Operacyjne i strategiczne	Regulacyjne i formalne

Wniosek

Metodologiczne podejście do analizy ryzyka cyberbezpieczeństwa w uczelniach wyższych powinno opierać się na podejściu *risk-based* rekomendowanym przez ENISA i dyrektywę NIS2. Jednak w warunkach projektowanej nowelizacji KSC istnieje istotne ryzyko, że analiza ryzyka będzie realizowana w sposób nadmiernie sformalizowany, bez odpowiedniego przełożenia na decyzje techniczne i organizacyjne.

Dla uczelni wyższych kluczowym wyzwaniem staje się zatem zaprojektowanie procesu analizy ryzyka, który z jednej strony spełni wymogi formalne KSC, a z drugiej zachowa realną wartość zarządczą i będzie wspierał budowę odporności cybernetycznej zgodnie z intencją NIS2.

8.3. Identyfikacja aktywów krytycznych

Pierwszym i fundamentalnym etapem analizy ryzyka cyberbezpieczeństwa jest identyfikacja aktywów, których naruszenie mogłoby mieć istotny wpływ na realizację misji uczelni wyższej, w szczególności w obszarach dydaktyki, badań naukowych, administracji oraz reputacji instytucji. W ujęciu metodycznym identyfikacja aktywów stanowi punkt wyjścia do dalszych etapów analizy ryzyka, takich jak identyfikacja zagrożeń, podatności oraz szacowanie skutków ich materializacji.
Do aktywów krytycznych w środowisku uczelni wyższych zalicza się w szczególności:

- dane osobowe studentów, pracowników oraz kandydatów na studia,
- dane badawcze, wyniki projektów naukowych oraz własność intelektualną,
- systemy dziekanatowe, rekrutacyjne oraz kadrowo-płacowe,

- platformy e-learningowe i systemy komunikacyjne wspierające proces dydaktyczny,
- infrastrukturę sieciową, serwerową oraz środowiska przetwarzania danych.

Z perspektywy zarządzania ryzykiem istotne jest nie tylko wskazanie samych aktywów, lecz również określenie ich krytyczności, zależności pomiędzy nimi oraz wpływu ich niedostępności, utraty poufności lub integralności na funkcjonowanie uczelni. Takie podejście jest zgodne z rekomendacjami ENISA oraz normami ISO, które wskazują, że klasyfikacja aktywów powinna być procesem dynamicznym i powiązanym z analizą procesów biznesowych organizacji[78].

Najwyższa Izba Kontroli wskazuje, że w jednostkach sektora publicznego brak formalnej i spójnej klasyfikacji aktywów informacyjnych stanowi jedną z głównych barier skutecznego zarządzania ryzykiem cyberbezpieczeństwa[79]. W praktyce aktywa są często identyfikowane fragmentarycznie, bez jednoznacznego przypisania właścicieli oraz bez powiązania z oceną wpływu na realizację kluczowych procesów.

Identyfikacja aktywów w świetle projektu nowelizacji KSC

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa wzmacnia znaczenie identyfikacji aktywów, w szczególności w kontekście:

- zarządzania ryzykiem cyberbezpieczeństwa,
- zapewnienia ciągłości działania,
- oceny wpływu incydentów na usługi istotne lub krytyczne,
- współpracy z CSIRT i organami nadzorczymi.

Jednocześnie sposób implementacji tych wymagań w KSC może prowadzić do **nadregulacji procesu identyfikacji aktywów**. Projektowane przepisy nie ograniczają się do ogólnego wskazania potrzeby identyfikacji aktywów, lecz pośrednio wymuszają:

- szczegółową inwentaryzację zasobów IT i danych,
- przypisanie formalnych właścicieli aktywów i procesów,

[78] European Union Agency for Cybersecurity, *Risk Management – guidelines and good practices*, ENISA, 2022, https://www.enisa.europa.eu/topics/risk-management

[79] Najwyższa Izba Kontroli, Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

- utrzymywanie aktualnych rejestrów aktywów jako elementu „dowodów zgodności”,
- gotowość do wykazania klasyfikacji aktywów w toku kontroli lub audytu.

W przypadku uczelni wyższych, charakteryzujących się dużą skalą, decentralizacją i złożonością infrastruktury, oznacza to istotne obciążenie organizacyjne. Identyfikacja aktywów przestaje być wyłącznie narzędziem analizy ryzyka, a staje się elementem zarządzania ryzykiem regulacyjnym, którego celem jest minimalizacja potencjalnych zarzutów niezgodności z KSC.

Porównanie podejścia: NIS2 / ENISA vs KSC (projekt)

W podejściu NIS2 identyfikacja aktywów stanowi środek do osiągnięcia celu, jakim jest skuteczne zarządzanie ryzykiem i odporność operacyjna. Dyrektywa kładzie nacisk na proporcjonalność – organizacja powinna identyfikować te aktywa, które są istotne z punktu widzenia świadczonych usług i profilu ryzyka[80].

Projekt KSC, poprzez rozbudowanie obowiązków formalnych i nadzorczych, może prowadzić do sytuacji, w której:

- zakres identyfikacji aktywów jest rozszerzany ponad realne potrzeby analizy ryzyka,
- klasyfikacja aktywów jest prowadzona w sposób statyczny i dokumentacyjny,
- głównym kryterium staje się kompletność formalna rejestru, a nie jego użyteczność decyzyjna.

Wniosek

Identyfikacja aktywów krytycznych pozostaje niezbędnym elementem skutecznej analizy ryzyka cyberbezpieczeństwa w uczelniach wyższych. Jednak w świetle projektowanej nowelizacji KSC istnieje ryzyko, że proces ten zostanie nadmiernie sformalizowany i podporządkowany wymogom zgodności regulacyjnej, zamiast realnemu zarządzaniu ryzykiem. Dla uczelni kluczowe znaczenie ma zatem takie zaprojektowanie procesu identyfikacji aktywów, aby spełniał on wymogi KSC, a jednocześnie zachował charakter narzędzia wspierającego decyzje strategiczne i operacyjne, zgodnie z intencją dyrektywy NIS2.

[80] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

8.4. Identyfikacja zagrożeń cyberbezpieczeństwa

Identyfikacja zagrożeń cyberbezpieczeństwa stanowi kluczowy etap analizy ryzyka, ponieważ umożliwia określenie scenariuszy zdarzeń mogących prowadzić do naruszenia poufności, integralności lub dostępności zasobów uczelni wyższej. Zagrożenia te mają zarówno charakter techniczny, jak i organizacyjny, a ich skuteczność jest w dużej mierze determinowana specyfiką środowiska akademickiego.

Zgodnie z analizami publikowanymi przez European Union Agency for Cybersecurity (ENISA), sektor edukacyjny charakteryzuje się podwyższoną podatnością na zagrożenia wynikające z dużej liczby użytkowników, rozproszonej infrastruktury oraz wysokiego poziomu otwartości informacyjnej[81]. ENISA wskazuje, że w tego typu organizacjach dominują zagrożenia oparte na czynniku ludzkim oraz błędach konfiguracyjnych, które często prowadzą do dalszej eskalacji incydentów.

Równolegle CERT Polska identyfikuje jako najczęściej występujące zagrożenia w sektorze publicznym, w tym w uczelniach wyższych:

- ataki phishingowe i inne formy socjotechniki,
- ataki ransomware prowadzące do utraty dostępności systemów,
- wykorzystanie niezałatanych podatności w oprogramowaniu,
- błędy konfiguracji systemów i infrastruktury,
- nadużycia uprawnień użytkowników, w szczególności kont uprzywilejowanych[82].

W środowisku akademickim skuteczność powyższych zagrożeń jest dodatkowo wzmacniana przez niski poziom świadomości bezpieczeństwa części użytkowników, znaczną rotację tożsamości oraz dużą autonomię jednostek organizacyjnych, co utrudnia egzekwowanie jednolitych standardów ochrony.

Zagrożenia a nadregulacja KSC

W kontekście Krajowego Systemu Cyberbezpieczeństwa identyfikacja zagrożeń powinna stanowić element procesu zarządzania ryzykiem prowadzącego

[81] European Union Agency for Cybersecurity (ENISA), *Threat Landscape*, ENISA, 2022–2023

[82] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025, https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

do proporcjonalnego doboru środków bezpieczeństwa. Jednak projektowana nowelizacja KSC, poprzez rozbudowanie obowiązków formalnych i dokumentacyjnych, stwarza ryzyko nadregulacji tego etapu.
W praktyce może to prowadzić do sytuacji, w której:

- identyfikacja zagrożeń realizowana jest w formie rozbudowanego katalogu formalnego,
- wszystkie zagrożenia traktowane są w sposób równoważny, niezależnie od ich realnego prawdopodobieństwa i wpływu,
- analiza zagrożeń służy przede wszystkim wykazaniu kompletności dokumentacji na potrzeby kontroli, a nie wsparciu decyzji technicznych i organizacyjnych.

Takie podejście osłabia skuteczność zarządzania ryzykiem, ponieważ ograniczone zasoby uczelni są rozpraszane pomiędzy wiele hipotetycznych zagrożeń, zamiast koncentrować się na tych, które – zgodnie z danymi ENISA i CERT Polska – materializują się najczęściej, takich jak phishing czy ransomware.

Podejście NIS2 a praktyka KSC

Dyrektywa NIS2 kładzie nacisk na identyfikację zagrożeń w kontekście ich wpływu na ciągłość i odporność organizacji oraz na konieczność regularnej aktualizacji analizy w oparciu o bieżące dane o krajobrazie zagrożeń[83]. Projekt KSC, mimo formalnego odwołania do podejścia risk-based, może sprzyjać modelowi checklistowemu, w którym kluczowym kryterium oceny staje się zakres formalny analizy, a nie jej aktualność i użyteczność operacyjna.

8.5. Identyfikacja podatności technicznych i organizacyjnych

Podatności cyberbezpieczeństwa stanowią słabe punkty w systemach, procesach lub strukturach organizacyjnych, które mogą zostać wykorzystane przez zagrożenia do naruszenia bezpieczeństwa informacji lub ciągłości działania. W środowisku uczelni wyższych podatności mają zwykle zarówno **techniczny**, jak i **organizacyjny**

[83] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

charakter, często wchodząc ze sobą w synergiczne zależności, co potęguje ryzyko materializacji incydentów.

8.5.1. Podatności techniczne

Podatności techniczne wynikają z cech technologicznych infrastruktury, systemów i usług. W uczelniach wyższych najczęściej identyfikowane obejmują:

- **brak aktualizacji systemów i aplikacji**, prowadzący do zalegania znanych błędów bezpieczeństwa,
- **nieprawidłowe konfiguracje usług oraz urządzeń sieciowych**, co ułatwia eskalację ataków lub obejście zabezpieczeń,
- **niewystarczającą segmentację sieci**, skutkującą łatwym przemieszczaniem się napastnika między środowiskami,
- **ograniczony monitoring bezpieczeństwa**, w szczególności brak centralnej korelacji zdarzeń, co ogranicza zdolność do wykrywania ataków wieloetapowych (tzw. dwell time)[84].

Techniczne podatności wynikają często z historycznego rozwoju infrastruktury, ograniczonych zasobów IT oraz specyficznych wymagań eksperymentalnych w środowiskach badawczych.

8.5.2. Podatności organizacyjne

Podatności organizacyjne odnoszą się do aspektów zarządzania, procesów i zachowań ludzkich. Najczęściej występujące w uczelniach wyższych obejmują:

- **brak jasno określonych ról i odpowiedzialności** w obszarze cyberbezpieczeństwa, co prowadzi do rozmycia decyzyjności,
- **niedostateczne szkolenia i kampanie edukacyjne dla użytkowników**, co zwiększa podatność na ataki socjotechniczne,
- **brak ustandaryzowanych i testowanych procedur reagowania na incydenty**, co wydłuża czas reakcji i poprawy stanu po naruszeniach.

[84] ENISA, *Threat and Vulnerability Landscape*, ENISA, 2022,

ENISA wskazuje, że podatności organizacyjne często wzmacniają skutki podatności technicznych, np. poprzez błędy w konfiguracji wynikające z braku kompetencji personelu lub niewystarczające procesy przeglądów[85].

8.5.3. Podatności w świetle projektu nowelizacji KSC

W kontekście projektowanej nowelizacji Krajowego Systemu Cyberbezpieczeństwa, która implementuje dyrektywę NIS2 do prawa krajowego, istnieje istotne ryzyko **nadregulacyjnego potraktowania identyfikacji podatności**. Choć formalnie KSC i NIS2 przyjmują podejście *risk-based*, to projekt nowelizacji kładzie jednocześnie duży nacisk na **formalną dokumentację, audytowalność i rozliczalność** procesów, co może prowadzić do kilku negatywnych implikacji:

a) **Priorytety formalne nad operacyjnymi**
Uczelnie mogą koncentrować się na spełnianiu formalnych wymogów identyfikacji podatności (np. posiadanie listy, procedur, dokumentacji) zamiast na **wdrożeniu praktycznych mechanizmów** ich detekcji i eliminacji. Formalna kompletność dokumentów staje się celem samym w sobie – kosztem realnej poprawy odporności.

b) **Rozbudowane raportowanie sprzyja nadmiernej klasyfikacji**
Projekt KSC rozszerza obowiązki raportowe, co może prowadzić do sytuacji, w której każde potencjalne naruszenie konfiguracji lub słabość procesu jest opisywane w kontekście ryzyka regulacyjnego, nawet jeśli w praktyce ma minimalne znaczenie operacyjne.

c) **Formalizacja nad elastycznością**
W projekcie KSC pojawiają się wymagania dotyczące okresowych przeglądów, audytów i dowodów działania, co może skłaniać organizacje do sztywnego trzymania się ustalonych harmonogramów, niezależnie od dynamicznych zmian w krajobrazie ryzyka. Tymczasem dobre praktyki (ENISA / NIS2) promują podejście elastyczne i oparte na aktualnych przesłankach ryzyka.

[85] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025 — Highlights of cyber threats and trends impacting the EU, ENISA, 2025, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

d) **Koszt zarządzania podatnościami może przewyższać efekty** Ponieważ KSC nie precyzuje proporcjonalności środków do profilu organizacji, projekty nadregulacyjne mogą wymusić inwestycje w narzędzia i procesy (np. skanery podatności, testy penetracyjne, SOC/SIEM) w skali nieadekwatnej do profilu ryzyka uczelni, co generuje dodatkowe koszty i obciążenia administracyjne.

W rezultacie identyfikacja podatności może stać się działania formalnym, wykonywanym w celu wykazania zgodności z wymogami KSC, zamiast stać się dynamicznym procesem wspierającym decyzje operacyjne i strategiczne.

8.5.4. Wniosek

Podatności techniczne i organizacyjne w uczelniach wyższych mają charakter złożony i wymagają podejścia systemowego. Nadregulacja wynikająca z projektu nowelizacji KSC może ograniczać wykorzystanie analizy podatności jako realnego narzędzia ograniczania ryzyka na rzecz spełniania formalnych wymogów. Tymczasem model *risk-based* promowany przez ENISA oraz dyrektywę NIS2 wskazuje, że identyfikacja podatności powinna być dynamiczna, proporcjonalna i ściśle powiązana z podejmowanymi działaniami zabezpieczającymi.

8.6. Scenariusze ryzyk cyberbezpieczeństwa:

Na podstawie zidentyfikowanych zagrożeń oraz podatności technicznych i organizacyjnych możliwe jest opracowanie **scenariuszy ryzyk cyberbezpieczeństwa**, które opisują potencjalne zdarzenia niepożądane, ich przebieg, skutki oraz możliwe reakcje organizacyjne i techniczne. Podejście scenariuszowe pozwala przejść od abstrakcyjnej identyfikacji zagrożeń do analizy **realnych zdarzeń operacyjnych**, z jakimi organizacja może się zetknąć.

W środowisku uczelni wyższych typowe scenariusze ryzyk obejmują w szczególności:

- przejęcie konta pracownika lub doktoranta i eskalację uprawnień w systemach administracyjnych lub badawczych,
- zaszyfrowanie systemów krytycznych (np. dziekanatowych, kadrowych, repozytoriów danych) w wyniku ataku ransomware,

- wyciek danych osobowych studentów i pracowników w następstwie ataku phishingowego lub błędu konfiguracji,
- niedostępność platform e-learningowych i systemów egzaminacyjnych w okresach krytycznych dla realizacji procesu dydaktycznego.

CERT Polska wskazuje, że brak scenariuszowego podejścia do analizy ryzyka istotnie utrudnia przygotowanie organizacji na rzeczywiste incydenty oraz ogranicza skuteczność reagowania w sytuacjach kryzysowych[86]. Analiza oparta wyłącznie na ogólnych kategoriach zagrożeń nie pozwala bowiem na ocenę kaskadowych skutków incydentów ani na weryfikację gotowości organizacyjnej.

Scenariusze ryzyka a podejście NIS2

Dyrektywa NIS2 wprost promuje podejście scenariuszowe jako element zarządzania ryzykiem cyberbezpieczeństwa. Wymaga ona, aby środki zaradcze były dobierane **w odniesieniu do konkretnych scenariuszy zagrożeń**, a nie w sposób abstrakcyjny czy checklistowy. Scenariusze ryzyka stanowią w tym modelu podstawę:

- projektowania środków technicznych i organizacyjnych,
- testowania planów reagowania i ciągłości działania,
- oceny skuteczności zabezpieczeń poprzez ćwiczenia i symulacje,
- wykazywania zgodności poprzez dowody operacyjne[87].

Takie podejście sprzyja koncentracji na realnych zdarzeniach o wysokim wpływie i prawdopodobieństwie, zamiast na hipotetycznych zagrożeniach o marginalnym znaczeniu.

Scenariusze ryzyka w kontekście nadregulacji KSC

W świetle projektu nowelizacji Krajowego Systemu Cyberbezpieczeństwa istnieje ryzyko, że podejście scenariuszowe zostanie **zredukowane do obowiązku formalnego**, a nie wykorzystane jako narzędzie budowy odporności. Nadregulacyjny charakter KSC może prowadzić do kilku negatywnych zjawisk:

a) **Formalizacja zamiast realizmu**
Scenariusze ryzyka mogą być tworzone w sposób abstrakcyjny i oderwany

[86] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025, https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

[87] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

od realiów uczelni, wyłącznie w celu spełnienia wymogów dokumentacyjnych i audytowych.

b) **Rozszerzanie katalogu scenariuszy ponad realne potrzeby**
Projekt KSC, poprzez brak jednoznacznych kryteriów proporcjonalności, może skłaniać do uwzględniania bardzo szerokiego spektrum scenariuszy, niezależnie od ich rzeczywistego wpływu i prawdopodobieństwa.

c) **Scenariusze jako narzędzie zarządzania ryzykiem regulacyjnym**
Zamiast koncentrować się na scenariuszach o największym znaczeniu operacyjnym (np. ransomware, phishing), uczelnie mogą być zmuszone do dokumentowania scenariuszy pod kątem potencjalnych sankcji administracyjnych, a nie rzeczywistych zagrożeń.

d) **Ograniczona integracja z testami i ćwiczeniami**
W modelu nadregulacyjnym scenariusze ryzyka często nie są wykorzystywane do ćwiczeń, testów technicznych czy symulacji decyzyjnych, co ogranicza ich wartość praktyczną.

Implikacje dla uczelni wyższych

Dla uczelni wyższych scenariuszowe podejście do ryzyka cyberbezpieczeństwa ma szczególne znaczenie ze względu na złożoność środowiska IT oraz krytyczność procesów dydaktycznych i badawczych. Jednak w warunkach nadregulacji KSC istnieje ryzyko, że scenariusze ryzyka staną się elementem „papierowej zgodności", generując dodatkowe koszty organizacyjne, bez proporcjonalnego wzrostu odporności.

Z perspektywy dobrych praktyk ENISA i NIS2 kluczowe znaczenie ma zapewnienie, aby scenariusze ryzyka:

- były aktualizowane w oparciu o rzeczywiste incydenty i dane z monitoringu,
- stanowiły podstawę testów i ćwiczeń,
- były powiązane z analizą BIA oraz planami ciągłości działania,
- wspierały decyzje strategiczne, a nie jedynie spełnienie wymogów formalnych.

Wniosek

Scenariusze ryzyk cyberbezpieczeństwa są jednym z najważniejszych narzędzi operacjonalizacji analizy ryzyka. W kontekście projektu nowelizacji KSC istnieje jednak istotne ryzyko ich nadmiernej formalizacji i podporządkowania logice regulacyjnej. Dla uczelni wyższych kluczowe jest zachowanie scenariuszowego

podejścia jako narzędzia realnego przygotowania na incydenty, zgodnie z intencją dyrektywy NIS2, a nie jako kolejnego obowiązku dokumentacyjnego wynikającego z prawa krajowego.

8.7. Ocena ryzyka – prawdopodobieństwo i wpływ

Ocena ryzyka cyberbezpieczeństwa polega na oszacowaniu **prawdopodobieństwa wystąpienia określonego scenariusza zagrożenia** oraz **skali jego wpływu na organizację**. Etap ten stanowi kluczowy element analizy ryzyka, ponieważ umożliwia priorytetyzację zagrożeń oraz racjonalny dobór środków technicznych i organizacyjnych.

Wpływ materializacji ryzyka w uczelniach wyższych może mieć wielowymiarowy charakter i obejmować w szczególności:

- **operacyjny** – zakłócenie ciągłości dydaktyki, badań lub administracji,
- **prawny i regulacyjny** – naruszenia przepisów o ochronie danych osobowych, KSC lub innych regulacji sektorowych,
- **finansowy** – koszty usuwania skutków incydentu, przestoje, kary administracyjne,
- **reputacyjny** – utrata zaufania studentów, pracowników, partnerów badawczych i grantodawców.

Zgodnie z normą **ISO/IEC 27005**, skuteczna ocena ryzyka wymaga zdefiniowania **jednoznacznych, spójnych i mierzalnych kryteriów** zarówno dla prawdopodobieństwa, jak i wpływu. Brak takich kryteriów prowadzi do subiektywizmu analizy oraz trudności w porównywaniu poziomów ryzyka w czasie i pomiędzy obszarami organizacji[88].

Ocena ryzyka w praktyce uczelni wyższych

W praktyce funkcjonowania uczelni wyższych ocena prawdopodobieństwa i wpływu bywa obarczona znaczną niepewnością. Wynika to m.in. z:

- ograniczonego dostępu do danych historycznych o incydentach,

[88] International Organization for Standardization, *ISO/IEC 27005:2022 – Information security risk management*, https://www.iso.org/standard/80585.html

- braku mierników skuteczności zabezpieczeń,
- trudności w wycenie wpływu reputacyjnego i badawczego,
- złożoności i rozproszenia środowiska IT.

W efekcie ocena ryzyka często przyjmuje charakter **ekspercki i jakościowy**, co samo w sobie nie stanowi wady, o ile proces ten jest spójny, udokumentowany i cyklicznie weryfikowany.

Nadregulacja KSC a ocena prawdopodobieństwa i wpływu

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa, mimo deklarowanego podejścia opartego na ryzyku, wprowadza mechanizmy, które mogą **zniekształcać sens oceny ryzyka**. W szczególności:

a) **Presja na formalną audytowalność zamiast trafności**
Projekt KSC wzmacnia rolę kontroli i sankcji administracyjnych, co może prowadzić do sytuacji, w której ocena ryzyka jest kształtowana pod kątem „bezpiecznym regulacyjnie", a nie realistycznym operacyjnie. Prawdopodobieństwo i wpływ mogą być zawyżane lub ujednolicane, aby uzasadnić wdrożenie określonych środków i uniknąć zarzutu niedochowania należytej staranności.

b) **Rozszerzenie wpływu o komponent sankcyjny**
W nowym KSC wpływ ryzyka jest coraz częściej oceniany nie tylko przez pryzmat skutków operacyjnych, lecz także potencjalnych kar administracyjnych. Powoduje to przesunięcie ciężaru analizy z **ryzyka cybernetycznego** na **ryzyko regulacyjne**, co nie zawsze prowadzi do poprawy rzeczywistej odporności.

c) **Brak proporcjonalności wymagań**
Projekt KSC nie wprowadza precyzyjnych mechanizmów różnicowania skali i głębokości oceny ryzyka w zależności od profilu organizacji. W przypadku uczelni wyższych może to skutkować koniecznością stosowania **modeli oceny ryzyka właściwych dla podmiotów o wysokiej krytyczności**, mimo że rzeczywisty wpływ incydentu może mieć charakter lokalny lub czasowy.

d) **Ryzyko „konserwatywnej" oceny ryzyka**
W warunkach nadregulacji organizacje mają tendencję do klasyfikowania większości scenariuszy jako wysokiego ryzyka, co prowadzi do:

- utraty zdolności do realnej priorytetyzacji,
- rozproszenia zasobów,
- nadmiernych inwestycji w obszary o ograniczonym znaczeniu operacyjnym.

Porównanie z podejściem NIS2

Dyrektywa NIS2, w przeciwieństwie do krajowego projektu KSC, kładzie nacisk na **proporcjonalność i skuteczność** oceny ryzyka. Wymaga ona, aby prawdopodobieństwo i wpływ były oceniane w kontekście:

- charakteru i skali działalności,
- rzeczywistego profilu zagrożeń,
- skuteczności istniejących zabezpieczeń,
- znaczenia usług dla społeczeństwa i gospodarki[89].

NIS2 nie oczekuje eliminacji subiektywizmu, lecz jego **kontrolowania poprzez dowody operacyjne**, takie jak dane z monitoringu, testów i incydentów.

Wniosek:

Ocena ryzyka oparta na prawdopodobieństwie i wpływie pozostaje kluczowym elementem systemu cyberbezpieczeństwa uczelni wyższych. Jednak w świetle projektu nowelizacji KSC istnieje realne ryzyko, że proces ten zostanie podporządkowany logice nadregulacyjnej, w której dominującym czynnikiem stanie się ryzyko sankcyjne, a nie rzeczywiste zagrożenia cybernetyczne. Dla uczelni kluczowe znaczenie ma zachowanie równowagi pomiędzy spełnieniem wymogów formalnych KSC a stosowaniem proporcjonalnej, realistycznej oceny ryzyka zgodnej z podejściem promowanym przez ISO/IEC 27005 oraz dyrektywę NIS2.

8.8. <u>Akceptacja ryzyka i odpowiedzialność kierownictwa:</u>

Zarządzanie ryzykiem cyberbezpieczeństwa nie polega wyłącznie na jego identyfikacji i ocenie, lecz również na **podejmowaniu świadomych decyzji dotyczących akceptowalnego poziomu ryzyka**. Decyzje te powinny być podejmowane na poziomie kierownictwa uczelni, w ramach systemu governance,

[89] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

który łączy kwestie cyberbezpieczeństwa z celami strategicznymi, finansowymi oraz reputacyjnymi organizacji.

Dyrektywa NIS2 jednoznacznie wskazuje, że **najwyższe kierownictwo ponosi odpowiedzialność za zatwierdzanie środków zarządzania ryzykiem cyberbezpieczeństwa oraz nadzór nad ich skutecznością**[90]. W modelu tym akceptacja ryzyka jest decyzją świadomą, udokumentowaną i opartą na rzetelnej analizie, a nie konsekwencją braku zasobów lub niedojrzałości organizacyjnej.

Brak formalnych decyzji o akceptacji ryzyka prowadzi w praktyce do **przenoszenia odpowiedzialności na poziom operacyjny**, w szczególności na działy IT lub pojedynczych administratorów. Skutkuje to nie tylko rozmyciem odpowiedzialności, lecz także podejmowaniem decyzji o charakterze strategicznym bez odpowiedniego mandatu decyzyjnego.

Akceptacja ryzyka w świetle projektu nowelizacji KSC

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa formalnie wzmacnia odpowiedzialność kierownictwa jednostki za cyberbezpieczeństwo, jednak sposób implementacji tych wymogów rodzi istotne wątpliwości z perspektywy **realnej akceptacji ryzyka**.

W szczególności nadregulacyjny charakter projektu KSC może prowadzić do następujących zjawisk:

1. **Pozorna akceptacja ryzyka**
   W warunkach wysokiego ryzyka sankcyjnego decyzje o akceptacji ryzyka mogą mieć charakter czysto deklaratywny lub być całkowicie eliminowane z procesu decyzyjnego. Kierownictwo, obawiając się odpowiedzialności administracyjnej lub osobistej, może dążyć do formalnego „zero-risk approach", który w praktyce jest niemożliwy do osiągnięcia.
2. **Zastąpienie decyzji biznesowych decyzjami regulacyjnymi**
   Zamiast rozważać ryzyko w kontekście wpływu na misję uczelni, projekt KSC sprzyja podejmowaniu decyzji zorientowanych na minimalizację ryzyka regulacyjnego. Akceptacja ryzyka przestaje być elementem governance, a staje się problemem zgodności z przepisami.

[90] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 20–21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

3. **Eskalacja odpowiedzialności bez realnych narzędzi decyzyjnych** Projekt KSC rozszerza odpowiedzialność kierownika jednostki, nie zapewniając jednocześnie proporcjonalnych mechanizmów wsparcia decyzyjnego, takich jak jednoznaczne kryteria akceptacji ryzyka, bezpieczne „harbour rules" czy wytyczne sektorowe dla uczelni wyższych.
4. **Ograniczenie elastyczności decyzyjnej** W modelu nadregulacyjnym akceptacja ryzyka staje się trudna do formalnego udokumentowania, ponieważ każda decyzja o tolerowaniu określonego ryzyka może zostać zakwestionowana ex post przez organ nadzorczy. W efekcie kierownictwo może unikać formalnego podejmowania decyzji, przenosząc odpowiedzialność na niższe poziomy organizacyjne.

Porównanie podejścia: NIS2 vs KSC (projekt)

W podejściu NIS2 akceptacja ryzyka jest integralnym elementem systemu zarządzania cyberbezpieczeństwem i zakłada:

- istnienie świadomych decyzji zarządczych,
- proporcjonalność środków do profilu ryzyka,
- możliwość tolerowania określonego poziomu ryzyka przy jednoczesnym monitorowaniu jego skutków.

Projekt KSC, poprzez nacisk na sankcje, obowiązki formalne i audytowalność, może prowadzić do sytuacji, w której:

- decyzje o akceptacji ryzyka są ograniczane lub wypierane,
- cyberbezpieczeństwo staje się obszarem defensywnym,
- odpowiedzialność kierownictwa ma charakter głównie formalno-prawny, a nie strategiczny.

Implikacje dla uczelni wyższych

Dla uczelni wyższych, działających w warunkach ograniczonych budżetów, autonomii akademickiej oraz rozproszonej struktury organizacyjnej, możliwość **świadomej i proporcjonalnej akceptacji ryzyka** jest kluczowa. Nadregulacja w projekcie KSC może jednak prowadzić do sytuacji, w której:

- decyzje strategiczne są paraliżowane przez obawę przed odpowiedzialnością,
- cyberbezpieczeństwo nie jest integrowane z zarządzaniem ryzykiem instytucjonalnym,
- formalna zgodność zastępuje realną odporność.

Wniosek

Akceptacja ryzyka cyberbezpieczeństwa powinna być postrzegana jako nieodłączny element governance uczelni wyższej, zgodny z podejściem promowanym przez dyrektywę NIS2. Projekt nowelizacji KSC, poprzez nadregulacyjny model odpowiedzialności, może jednak ograniczać zdolność kierownictwa do podejmowania świadomych decyzji o akceptowalnym poziomie ryzyka. W efekcie istnieje ryzyko, że odpowiedzialność kierownictwa stanie się odpowiedzialnością formalną, oderwaną od realnych mechanizmów zarządzania cyberbezpieczeństwem[91].

8.9. Wnioski z analizy ryzyka cyberbezpieczeństwa

Przeprowadzona analiza ryzyka cyberbezpieczeństwa w uczelniach wyższych wskazuje jednoznacznie, że identyfikowane ryzyka mają **charakter systemowy**, a ich źródłem jest współwystępowanie podatności technicznych oraz organizacyjnych. Ryzyka te nie wynikają z pojedynczych luk technologicznych, lecz z braku spójnego modelu zarządzania cyberbezpieczeństwem, obejmującego governance, odpowiedzialność decyzyjną, procesy oraz mechanizmy kontroli skuteczności.

W szczególności analiza wykazała, że bez **formalnego, ciągłego i zintegrowanego procesu zarządzania ryzykiem** uczelnie wyższe nie są w stanie:

- racjonalnie priorytetyzować zagrożeń i scenariuszy ryzyka,
- planować działań ochronnych w oparciu o rzeczywisty profil ryzyka,
- skutecznie integrować cyberbezpieczeństwa z zarządzaniem strategicznym,
- wykazywać odporności operacyjnej w sposób oparty na dowodach.

W tym kontekście należy podkreślić, że zarówno Krajowy System Cyberbezpieczeństwa, jak i dyrektywa NIS2 formalnie odwołują się do podejścia *risk-based*. Jednak sposób implementacji tych wymagań w projektowanej nowelizacji KSC

[91] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt ustawy o jej zmianie, ISAP / Ministerstwo Cyfryzacji, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw
.

istotnie odbiega od **praktycznej logiki zarządzania ryzykiem**, promowanej na poziomie europejskim.

Nadregulacja KSC a realne zarządzanie ryzykiem

Projekt nowelizacji KSC, implementujący dyrektywę NIS2, wprowadza rozbudowany katalog obowiązków organizacyjnych, dokumentacyjnych oraz nadzorczych. W efekcie istnieje wysokie ryzyko, że w sektorze szkolnictwa wyższego zarządzanie ryzykiem cyberbezpieczeństwa będzie realizowane przede wszystkim jako **instrument zapewnienia zgodności regulacyjnej**, a nie jako narzędzie faktycznego podnoszenia odporności.

W szczególności nadregulacja KSC może prowadzić do:

- koncentracji na spełnianiu wymogów formalnych kosztem działań operacyjnych,
- nadmiernego rozbudowania dokumentacji ryzyka przy ograniczonej jej aktualności,
- przesunięcia ciężaru decyzyjnego z ryzyka cybernetycznego na ryzyko sankcyjne,
- paraliżu decyzyjnego kierownictwa uczelni w obawie przed odpowiedzialnością administracyjną.

Takie podejście stoi w sprzeczności z intencją dyrektywy NIS2, która kładzie nacisk na **skuteczność, proporcjonalność i odpowiedzialność zarządczą**, a nie na formalne spełnianie obowiązków proceduralnych[1].

Specyfika uczelni wyższych a proporcjonalność regulacji

Analiza ryzyka wykazała również, że uczelnie wyższe charakteryzują się unikalnym profilem ryzyka, wynikającym z:

- wysokiego poziomu autonomii organizacyjnej,
- rozproszonej infrastruktury IT,
- dużej liczby użytkowników o zróżnicowanym poziomie świadomości bezpieczeństwa,
- istotnej roli procesów dydaktycznych i badawczych.

W tym kontekście **automatyczne lub szerokie włączanie uczelni do kategorii „podmiotów ważnych”**, przewidziane w projekcie KSC, może prowadzić do nieproporcjonalnych obciążeń organizacyjnych i finansowych. Dyrektywa NIS2 przewiduje objęcie regulacją jedynie tych instytucji badawczych, których działa

9. Analiza wpływu biznesowego (BIA) oraz ciągłość działania w uczelniach wyższych

9.1. Rola analizy wpływu biznesowego (BIA) w systemie cyberbezpieczeństwa:

Analiza wpływu biznesowego (Business Impact Analysis – BIA) stanowi kluczowy element systemowego podejścia do zarządzania ciągłością działania oraz odpornością organizacyjną. Jej zasadniczym celem jest identyfikacja procesów krytycznych dla realizacji misji organizacji, określenie skutków ich zakłócenia oraz zdefiniowanie dopuszczalnych parametrów odtworzenia, takich jak maksymalny akceptowalny czas przerwy (RTO) oraz maksymalna utrata danych (RPO).
W kontekście cyberbezpieczeństwa BIA pełni funkcję **łącznika pomiędzy analizą ryzyka a projektowaniem środków technicznych i organizacyjnych**, umożliwiając przełożenie abstrakcyjnych scenariuszy ryzyka na konkretne wymagania dotyczące odporności systemów, procesów i struktur organizacyjnych. Bez przeprowadzenia rzetelnej analizy BIA działania w zakresie cyberbezpieczeństwa mają charakter fragmentaryczny i reaktywny, a priorytety inwestycyjne są ustalane w sposób intuicyjny lub doraźny.
Zgodnie z normą **International Organization for Standardization ISO 22301**, analiza BIA powinna stanowić fundament systemu zarządzania ciągłością działania oraz podstawę do planowania reakcji na incydenty, katastrofy i zakłócenia operacyjne[92]. Norma jednoznacznie wskazuje, że BIA powinna być procesem:

- systematycznym i udokumentowanym,
- opartym na procesach, a nie wyłącznie na zasobach IT,
- cyklicznie aktualizowanym wraz ze zmianą modelu działalności organizacji.

Specyfika BIA w uczelniach wyższych
W uczelniach wyższych analiza wpływu biznesowego ma szczególne znaczenie ze względu na złożony charakter misji instytucji, obejmującej jednocześnie:

- działalność dydaktyczną,

[92] International Organization for Standardization, *ISO 22301:2019 – Business continuity management systems*, https://www.iso.org/standard/75106.html

- działalność badawczo-rozwojową,
- rozbudowane procesy administracyjne,
- współpracę międzynarodową i grantową.

Zakłócenia w funkcjonowaniu systemów informatycznych uczelni nie mają wyłącznie charakteru technicznego, lecz mogą prowadzić do:

- przerwania procesu kształcenia,
- utraty ciągłości badań naukowych,
- naruszenia zobowiązań grantowych,
- szkód reputacyjnych trudnych do odwrócenia.

W tym kontekście BIA umożliwia racjonalne określenie, **które procesy rzeczywiście wymagają wysokiej odporności**, a które mogą być odtwarzane w dłuższym horyzoncie czasowym bez istotnego wpływu na funkcjonowanie uczelni.

BIA w świetle NIS2

Dyrektywa NIS2 traktuje zapewnienie ciągłości działania i odporności operacyjnej jako jeden z filarów zarządzania ryzykiem cyberbezpieczeństwa. Art. 21 dyrektywy jednoznacznie wskazuje na konieczność wdrożenia środków umożliwiających:

- zapewnienie dostępności usług,
- przygotowanie organizacji na sytuacje kryzysowe,
- testowanie planów ciągłości działania i reagowania[93].

Choć NIS2 nie narzuca wprost jednej metodologii BIA, jej logika regulacyjna jednoznacznie zakłada, że **BIA jest narzędziem praktycznym**, służącym do oceny skutków zakłóceń i projektowania proporcjonalnych mechanizmów odporności.

Nadregulacja KSC a analiza BIA

W kontekście projektu nowelizacji Krajowego Systemu Cyberbezpieczeństwa rola analizy BIA ulega istotnemu przekształceniu. Choć KSC formalnie odnosi się do konieczności zapewnienia ciągłości działania, projektowane przepisy:

- nie precyzują proporcjonalnego zakresu BIA dla poszczególnych kategorii podmiotów,
- wzmacniają wymogi dokumentacyjne i dowodowe,

[93] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

- łączą BIA z odpowiedzialnością sankcyjną kierownictwa.

W praktyce może to prowadzić do **nadregulacji analizy BIA**, polegającej na:

- traktowaniu BIA jako obowiązku formalnego, a nie narzędzia decyzyjnego,
- rozszerzaniu zakresu analizy na wszystkie procesy organizacyjne, niezależnie od ich rzeczywistej krytyczności,
- konieczności szczegółowego dokumentowania parametrów RTO/RPO dla szerokiego spektrum procesów, nawet tam, gdzie nie ma to uzasadnienia operacyjnego.

Dla uczelni wyższych oznacza to ryzyko istotnego wzrostu kosztów organizacyjnych i administracyjnych, bez proporcjonalnego wzrostu realnej odporności. Analiza BIA może zostać sprowadzona do elementu **zarządzania ryzykiem regulacyjnym**, którego głównym celem jest wykazanie zgodności z KSC, a nie faktyczne przygotowanie organizacji na zakłócenia.

Porównanie podejścia: NIS2 vs KSC (projekt)

W podejściu NIS2 analiza BIA pełni funkcję:

- narzędzia priorytetyzacji,
- wsparcia decyzji strategicznych,
- podstawy testowania i doskonalenia odporności.

W projekcie nowelizacji KSC BIA może natomiast zostać podporządkowana:

- obowiązkom formalnym,
- mechanizmom kontrolnym,
- logice odpowiedzialności administracyjnej.

Taka rozbieżność prowadzi do sytuacji, w której uczelnie są zmuszone do realizacji rozbudowanych analiz BIA, które nie zawsze przekładają się na rzeczywiste usprawnienia w zakresie ciągłości działania.

Wniosek

Analiza wpływu biznesowego (BIA) jest niezbędnym elementem skutecznego systemu cyberbezpieczeństwa i ciągłości działania w uczelniach wyższych. Jednak w świetle projektowanej nowelizacji KSC istnieje istotne ryzyko jej nadmiernej formalizacji i oderwania od realnych potrzeb operacyjnych. Kluczowym wyzwaniem dla uczelni staje się zatem takie zaprojektowanie procesu BIA, aby spełniał on wymogi

regulacyjne KSC, a jednocześnie zachował charakter narzędzia proporcjonalnego, praktycznego i zgodnego z intencją dyrektywy NIS2[94].

9.2. Specyfika BIA w środowisku uczelni wyższych:

Środowisko uczelni wyższych charakteryzuje się **wysoką złożonością procesową** oraz znacznym zróżnicowaniem znaczenia poszczególnych procesów dla realizacji misji instytucji. Obejmuje ono nie tylko działalność dydaktyczną, lecz również procesy administracyjne, badawcze, finansowe, grantowe oraz wspierające współpracę międzynarodową. Taka struktura powoduje, że przeprowadzenie analizy wpływu biznesowego (BIA) w uczelni wyższej wymaga uwzględnienia wielu grup interesariuszy oraz skomplikowanych zależności pomiędzy procesami, systemami informatycznymi i zasobami ludzkimi.
W praktyce BIA w uczelni musi obejmować m.in.:

- procesy dydaktyczne (rekrutacja, obsługa toku studiów, egzaminy),
- procesy badawcze (realizacja projektów, dostęp do danych i aparatury),
- procesy administracyjne i finansowe (kadry, płace, rozliczenia),
- procesy infrastrukturalne i IT (sieć, centra danych, platformy e-learningowe).

Najwyższa Izba Kontroli wskazuje, że brak formalnej identyfikacji procesów krytycznych w jednostkach sektora publicznego prowadzi do **chaotycznego reagowania w sytuacjach kryzysowych**, braku priorytetyzacji działań oraz nieefektywnego wykorzystania zasobów organizacyjnych[95]. W konsekwencji organizacje nie są w stanie szybko odtworzyć tych funkcji, które mają kluczowe znaczenie dla ciągłości działania.

---

[94] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt ustawy o jej zmianie, ISAP / Ministerstwo Cyfryzacji,

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw

[95] Najwyższa Izba Kontroli, *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania instytucji publicznych*, NIK, 2024, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf

Trudności identyfikacji procesów krytycznych w uczelniach

W praktyce funkcjonowania uczelni wyższych często występuje **brak jednoznacznego rozróżnienia pomiędzy procesami krytycznymi a procesami wspierającymi**. Wynika to m.in. z:

- autonomii wydziałów i jednostek organizacyjnych,
- równoległego funkcjonowania wielu systemów informatycznych,
- braku formalnych właścicieli procesów,
- historycznego rozwoju struktur organizacyjnych.

Skutkiem jest sytuacja, w której znaczna liczba procesów jest traktowana jako „równie ważna", co uniemożliwia skuteczne określenie priorytetów odtworzeniowych (RTO/RPO) oraz racjonalne planowanie środków zapewnienia ciągłości działania.

Specyfika BIA a wymogi NIS2

Dyrektywa NIS2, choć nie narzuca jednej metodologii BIA, zakłada podejście **proporcjonalne i oparte na rzeczywistym wpływie zakłóceń**. Oznacza to, że identyfikacja procesów krytycznych powinna być:

- selektywna, a nie pełna,
- oparta na analizie wpływu na usługi istotne,
- powiązana z realnymi scenariuszami zakłóceń,
- integrowana z planami ciągłości działania i testami[96].

W takim ujęciu BIA stanowi narzędzie wspierające decyzje zarządcze, a nie cel sam w sobie.

Nadregulacja KSC a analiza BIA w uczelniach

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa znacząco wzmacnia obowiązki podmiotów w zakresie zapewnienia ciągłości działania, jednak **nie różnicuje w sposób wystarczający specyfiki poszczególnych sektorów**, w tym szkolnictwa wyższego[97]. W efekcie istnieje ryzyko **nadregulacyjnego podejścia do BIA**, polegającego na:

---

[96] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[97] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt ustawy o jej zmianie, ISAP / Ministerstwo Cyfryzacji,

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

- oczekiwaniu kompleksowej analizy wszystkich procesów organizacyjnych,
- formalnym przypisywaniu parametrów RTO/RPO nawet dla procesów o marginalnym znaczeniu,
- konieczności utrzymywania rozbudowanej dokumentacji BIA jako dowodu zgodności,
- rozszerzeniu odpowiedzialności kierownictwa bez zapewnienia proporcjonalnych narzędzi decyzyjnych.

Dla uczelni wyższych oznacza to potencjalnie **znaczący wzrost kosztów organizacyjnych i administracyjnych**, bez adekwatnego wzrostu realnej odporności operacyjnej. BIA może zostać zredukowana do narzędzia zarządzania ryzykiem regulacyjnym, a nie do mechanizmu racjonalnego planowania ciągłości działania.

Implikacje praktyczne

W warunkach nadregulacji KSC uczelnie mogą zostać zmuszone do:

- nadmiernego rozszerzania zakresu BIA,
- traktowania procesów wspierających na równi z krytycznymi,
- alokowania zasobów na utrzymanie formalnej zgodności zamiast na realne zabezpieczenia.

Tymczasem skuteczna BIA w środowisku akademickim powinna koncentrować się na **wąskim, jasno zdefiniowanym zbiorze procesów krytycznych**, których zakłócenie rzeczywiście zagraża realizacji podstawowej misji uczelni.

Wniosek

Specyfika środowiska uczelni wyższych wymaga elastycznego i proporcjonalnego podejścia do analizy wpływu biznesowego. Projekt nowelizacji KSC, poprzez nadmierne sformalizowanie wymogów w zakresie ciągłości działania, niesie ryzyko przekształcenia BIA w kosztowny i pracochłonny obowiązek administracyjny. Kluczowym wyzwaniem dla uczelni pozostaje zatem takie zaprojektowanie procesu BIA, aby spełniał wymogi KSC, a jednocześnie zachował zgodność z intencją dyrektywy NIS2 – czyli realne wsparcie odporności operacyjnej, a nie jedynie formalnej zgodności.

---

https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw

9.3. Identyfikacja procesów krytycznych i zależności systemowych:

Kluczowym etapem analizy wpływu biznesowego (BIA) jest identyfikacja procesów krytycznych, których zakłócenie może w sposób istotny wpłynąć na realizację podstawowej misji uczelni wyższej. Procesy te obejmują zarówno obszary bezpośrednio związane z dydaktyką i badaniami naukowymi, jak i procesy administracyjne oraz finansowe, bez których funkcjonowanie uczelni byłoby niemożliwe.

Do procesów krytycznych w środowisku akademickim zalicza się w szczególności:

- proces rekrutacji oraz obsługi toku studiów,
- realizację zajęć dydaktycznych, egzaminów i zaliczeń,
- obsługę kadrowo-płacową pracowników,
- realizację projektów badawczych i grantowych,
- obsługę finansową, księgową i sprawozdawczą.

Każdy z powyższych procesów jest **ściśle uzależniony od określonych systemów informatycznych**, takich jak systemy dziekanatowe, platformy e-learningowe, systemy ERP, systemy finansowo-księgowe, repozytoria danych badawczych czy infrastruktura sieciowa i serwerowa. W praktyce oznacza to, że zakłócenie jednego komponentu technicznego może prowadzić do kaskadowych skutków dla wielu procesów jednocześnie.

ENISA podkreśla, że nieuwzględnienie zależności systemowych w analizie BIA prowadzi do **niedoszacowania skutków incydentów cyberbezpieczeństwa**, w szczególności w organizacjach o złożonej i rozproszonej infrastrukturze IT[1]. Analiza BIA powinna zatem obejmować nie tylko identyfikację procesów, lecz również mapowanie ich powiązań z:

- systemami informatycznymi,
- zasobami danych,
- infrastrukturą techniczną,
- kluczowymi rolami organizacyjnymi.

Nadregulacja KSC a identyfikacja procesów krytycznych

Projekt nowelizacji Krajowego Systemu Cyberbezpieczeństwa wzmacnia obowiązki podmiotów w zakresie zapewnienia ciągłości działania, jednak nie precyzuje w sposób

jednoznaczny **zakresu i poziomu szczegółowości identyfikacji procesów krytycznych**, adekwatnego do specyfiki sektora szkolnictwa wyższego[98].
W efekcie istnieje ryzyko, że uczelnie będą zmuszone do:

- kwalifikowania znacznej części procesów jako „krytyczne",
- prowadzenia rozbudowanej dokumentacji zależności systemowych,
- utrzymywania szczegółowych map procesów i systemów wyłącznie na potrzeby zgodności regulacyjnej.

Takie podejście może prowadzić do nadmiernego rozproszenia zasobów oraz osłabienia zdolności do rzeczywistej priorytetyzacji procesów, co stoi w sprzeczności z intencją BIA jako narzędzia decyzyjnego.

9.4. Określanie parametrów RTO i RPO:

Na podstawie wyników analizy BIA organizacja powinna określić kluczowe parametry ciągłości działania, w szczególności:

- **RTO (Recovery Time Objective)** – maksymalny dopuszczalny czas odtworzenia procesu lub systemu,
- **RPO (Recovery Point Objective)** – maksymalną dopuszczalną utratę danych wyrażoną w jednostkach czasu.

Parametry RTO i RPO stanowią fundament dla projektowania rozwiązań technicznych zapewniających ciągłość działania, takich jak mechanizmy kopii zapasowych, replikacji danych, architektury wysokiej dostępności czy procedury odtworzeniowe. Zgodnie z normą **International Organization for Standardization ISO 22301**, brak formalnie określonych parametrów RTO i RPO uniemożliwia skuteczne planowanie i testowanie ciągłości działania[99].
W środowisku uczelni wyższych parametry te:

---

[98] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt ustawy o jej zmianie, ISAP / Ministerstwo Cyfryzacji,

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw

[99] International Organization for Standardization, *ISO 22301:2019 – Business continuity management systems*, https://www.iso.org/standard/75106.html

- często nie są formalnie zdefiniowane,
- mają charakter orientacyjny lub historyczny,
- nie są powiązane z rzeczywistymi możliwościami technicznymi.

Skutkuje to rozbieżnością pomiędzy oczekiwaniami interesariuszy a realnymi zdolnościami odtworzeniowymi uczelni.

RTO/RPO a projekt nowelizacji KSC

Projekt nowelizacji KSC, poprzez silny nacisk na zapewnienie ciągłości działania oraz wykazywanie zdolności odtworzeniowych, może prowadzić do **nadmiernego formalizowania parametrów RTO i RPO**. W praktyce oznacza to ryzyko:

- konieczności definiowania RTO/RPO dla szerokiego spektrum procesów,
- narzucania krótkich czasów odtworzenia bez analizy kosztów i wykonalności,
- presji na wdrażanie kosztownych rozwiązań technicznych wyłącznie w celu spełnienia wymogów regulacyjnych.

Dla uczelni wyższych, funkcjonujących w warunkach ograniczonych budżetów, może to skutkować **nieproporcjonalnym wzrostem kosztów infrastrukturalnych**, bez realnego wzrostu odporności operacyjnej. W odróżnieniu od podejścia promowanego przez NIS2, projekt KSC w niewystarczającym stopniu akcentuje zasadę proporcjonalności pomiędzy znaczeniem procesu a wymaganym poziomem odtworzenia.

Wniosek

Identyfikacja procesów krytycznych oraz określanie parametrów RTO i RPO stanowią kluczowe elementy skutecznej analizy BIA w uczelniach wyższych. Jednak w świetle projektu nowelizacji KSC istnieje realne ryzyko nadmiernej formalizacji tych działań, prowadzącej do wzrostu obciążeń organizacyjnych i finansowych. Kluczowym wyzwaniem pozostaje zatem zachowanie równowagi pomiędzy spełnieniem wymogów regulacyjnych a wdrożeniem proporcjonalnych, realnie wykonalnych mechanizmów ciągłości działania, zgodnych z intencją dyrektywy NIS2.

9.5. Techniczne aspekty zapewnienia ciągłości działania (BCP/DR):

Zapewnienie ciągłości działania (Business Continuity Planning – BCP) oraz zdolności odtworzeniowych (Disaster Recovery – DR) w kontekście cyberbezpieczeństwa wymaga wdrożenia odpowiednich środków technicznych, które umożliwiają

utrzymanie lub szybkie przywrócenie kluczowych procesów uczelni po wystąpieniu incydentu. Do podstawowych mechanizmów technicznych należą w szczególności:

- systemy kopii zapasowych (backup),
- replikacja danych i systemów,
- redundancja infrastruktury (sprzętowej i sieciowej),
- procedury odtwarzania systemów po awarii lub ataku.

ENISA wskazuje, że skuteczność rozwiązań technicznych w zakresie ciągłości działania jest uzależniona nie tylko od ich wdrożenia, lecz przede wszystkim od **regularnego testowania, aktualizacji oraz dostosowywania do zmieniającego się krajobrazu zagrożeń**, w szczególności zagrożeń typu ransomware[100]. Mechanizmy, które nie są testowane w warunkach zbliżonych do rzeczywistych, często okazują się nieskuteczne w sytuacji kryzysowej.

Również CERT Polska podkreśla, że brak testów planów DR stanowi jedną z głównych przyczyn niepowodzeń w odtwarzaniu systemów po atakach ransomware. W wielu przypadkach organizacje posiadają kopie zapasowe, jednak nie są one możliwe do skutecznego wykorzystania w wymaganym czasie[101].

Nadregulacja KSC a techniczne BCP/DR

Projekt nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa (2026) wzmacnia wymagania w zakresie ciągłości działania, w praktyce przesuwając ciężar odpowiedzialności na **wykazanie formalnej zdolności odtworzeniowej**[102]. W odniesieniu do uczelni wyższych rodzi to istotne ryzyka nadregulacyjne, w szczególności:

- presję na wdrażanie kosztownych rozwiązań wysokiej dostępności również dla procesów o ograniczonej krytyczności,

[100] ENISA Threat Landscape for Ransomware Attacks (2022), https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[101] CERT Polska – Raport roczny o stanie cyberbezpieczeństwa w Polsce 2024, CERT Polska, 2025, https://www.cert.pl/raporty/2025/04/raport-roczny-2024/

[102] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt nowej ustawy KSC (2026), ISAP / Ministerstwo Cyfryzacji, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 https://www.gov.pl/web/cyfryzacja

- konieczność dokumentowania szczegółowych scenariuszy DR dla szerokiego zakresu systemów,
- oczekiwanie krótkich RTO/RPO bez analizy realnych kosztów i wykonalności.

W efekcie środki techniczne BCP/DR mogą być projektowane **pod kątem audytowalności i zgodności**, a nie proporcjonalnej odporności. Takie podejście odbiega od logiki NIS2, która akcentuje adekwatność środków do profilu ryzyka i znaczenia usług, a nie jednolity poziom zabezpieczeń dla wszystkich procesów.

9.6. Organizacyjne aspekty ciągłości działania i zarządzania kryzysowego:

Ciągłość działania nie ogranicza się wyłącznie do aspektów technicznych. Równie istotne znaczenie mają **mechanizmy organizacyjne**, które decydują o zdolności uczelni do reagowania na incydenty o charakterze kryzysowym. Obejmują one w szczególności:

- strukturę zespołów zarządzania kryzysowego,
- jasno określone role i odpowiedzialności decyzyjne,
- procedury komunikacji wewnętrznej i zewnętrznej,
- współpracę z podmiotami zewnętrznymi, w tym CSIRT oraz dostawcami usług ICT.

Dyrektywa NIS2 kładzie silny nacisk na **gotowość organizacyjną**, zdolność podejmowania decyzji w warunkach presji czasowej oraz utrzymanie ciągłości kluczowych usług nawet w trakcie trwania incydentu[103]. Oznacza to konieczność posiadania nie tylko dokumentów, lecz również przećwiczonych struktur decyzyjnych i procedur eskalacyjnych.

W praktyce uczelni wyższych brak jasno określonych ról i procedur decyzyjnych może prowadzić do:

- opóźnień w podejmowaniu decyzji,
- niejednoznaczności kompetencyjnej pomiędzy jednostkami,
- eskalacji skutków incydentów wskutek braku koordynacji działań.

[103] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), art. 21 oraz art. 23, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Nadregulacja KSC a organizacyjne BCP

Projekt nowej ustawy KSC istotnie rozszerza zakres obowiązków organizacyjnych związanych z ciągłością działania i zarządzaniem kryzysowym, jednak czyni to w sposób **silnie sformalizowany**. W odniesieniu do uczelni wyższych może to skutkować:

- koniecznością tworzenia rozbudowanych, wielopoziomowych struktur kryzysowych,
- formalizacją ścieżek decyzyjnych kosztem elastyczności,
- wzrostem odpowiedzialności kierownictwa bez zapewnienia proporcjonalnych mechanizmów wsparcia.

W konsekwencji zarządzanie kryzysowe może zostać podporządkowane logice zgodności regulacyjnej, zamiast realnej zdolności do reagowania. Jest to podejście odmienne od NIS2, które akcentuje **skuteczność i odporność operacyjną**, a nie wyłącznie istnienie struktur formalnych.

Wniosek

Zapewnienie ciągłości działania w uczelniach wyższych wymaga zrównoważonego podejścia, łączącego środki techniczne BCP/DR z dojrzałymi mechanizmami organizacyjnymi. Projekt nowej ustawy KSC (2026), poprzez nadregulację i silny nacisk na formalną zgodność, niesie ryzyko przekształcenia ciągłości działania w kosztowny obowiązek administracyjny. Kluczowym wyzwaniem pozostaje zachowanie proporcjonalności działań oraz zgodności z intencją dyrektywy NIS2, która traktuje ciągłość działania jako element realnej odporności, a nie jedynie wymóg formalny.

9.7. Testowanie, ćwiczenia i doskonalenie planów ciągłości działania:

Normy międzynarodowe oraz wytyczne instytucji europejskich jednoznacznie wskazują, że **testowanie i ćwiczenia** stanowią kluczowy element skutecznego systemu ciągłości działania. Bez regularnej weryfikacji planów BCP/DR organizacja nie jest w stanie potwierdzić, czy przyjęte założenia – w tym RTO i RPO – są realnie osiągalne w warunkach incydentu.

Zgodnie z **International Organization for Standardization ISO 22301**, testowanie planów ciągłości działania powinno być procesem cyklicznym i obejmować różne

formy weryfikacji, dostosowane do profilu ryzyka organizacji[104]. Do najczęściej stosowanych należą:

- **testy techniczne**, obejmujące odtwarzanie systemów, danych i infrastruktury,
- **ćwiczenia symulacyjne**, sprawdzające współpracę zespołów oraz ścieżki decyzyjne,
- **testy scenariuszowe**, bazujące na realistycznych incydentach cyberbezpieczeństwa (np. ransomware, awaria centrum danych).

Również **ENISA** podkreśla, że brak testów lub ich realizacja w sposób nieformalny prowadzi do **fałszywego poczucia bezpieczeństwa**, ponieważ plany ciągłości działania często zawodzą w momencie rzeczywistego kryzysu[105].

W praktyce uczelni wyższych testowanie planów BCP/DR jest jednak często:

- pomijane z uwagi na ograniczenia organizacyjne,
- realizowane wyłącznie „na papierze",
- odkładane w czasie ze względu na ryzyko zakłóceń dydaktyki.

Skutkiem jest sytuacja, w której plany ciągłości działania istnieją formalnie, lecz **nie zostały zweryfikowane w warunkach zbliżonych do rzeczywistych**.

Nadregulacja KSC a testowanie BCP/DR

Projekt nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa (2026) istotnie wzmacnia wymagania dotyczące testowania i doskonalenia planów ciągłości działania, jednak czyni to w sposób **silnie sformalizowany i audytowalny**[106]. W odniesieniu do uczelni wyższych może to prowadzić do:

- presji na realizację testów wyłącznie w celu spełnienia wymogów kontrolnych,
- koncentracji na dokumentowaniu testów zamiast na ich jakości,
- nadmiernej częstotliwości ćwiczeń, nieadekwatnej do profilu ryzyka.

W efekcie testowanie może zostać zredukowane do **mechanizmu zarządzania ryzykiem regulacyjnym**, a nie realnego doskonalenia odporności operacyjnej.

---

[104] International Organization for Standardization, *ISO 22301:2019 – Business continuity management systems*, https://www.iso.org/standard/75106.html

[105] ENISA, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024*

[106] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt nowej ustawy KSC (2026), ISAP / Ministerstwo Cyfryzacji, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 https://www.gov.pl/web/cyfryzacja

9.8. Ciągłość działania a wymagania KSC i NIS2:

Zarówno Krajowy System Cyberbezpieczeństwa, jak i dyrektywa NIS2 odnoszą się do konieczności zapewnienia ciągłości działania systemów informacyjnych oraz usług kluczowych. Różnice pomiędzy tymi regulacjami ujawniają się jednak na poziomie **filozofii wdrożeniowej**.

Dyrektywa **NIS2** w sposób jednoznaczny akcentuje:

- odporność operacyjną organizacji,
- zdolność reagowania na incydenty o charakterze kryzysowym,
- konieczność wykazania **skuteczności** wdrożonych środków poprzez dowody operacyjne[107].

W praktyce oznacza to, że organizacje – w tym uczelnie wyższe – powinny być w stanie przedstawić nie tylko dokumentację, lecz również:

- wyniki przeprowadzonych analiz BIA,
- jasno określone i uzasadnione RTO oraz RPO,
- raporty z testów BCP/DR,
- działania doskonalące wdrażane na podstawie wniosków z ćwiczeń.

Projekt nowej ustawy KSC (2026) formalnie implementuje część tych wymagań, jednak wprowadza je w sposób **znacznie bardziej restrykcyjny i administracyjny**.

W szczególności:

- rozszerza zakres obowiązków dokumentacyjnych,
- zwiększa odpowiedzialność kierownictwa za brak wykazania zgodności,
- ogranicza elastyczność w doborze zakresu i częstotliwości testów.

W rezultacie uczelnie wyższe mogą zostać zobowiązane do spełniania **wymogów porównywalnych z podmiotami o wysokiej krytyczności**, mimo że rzeczywisty wpływ zakłóceń ma często charakter lokalny lub czasowy.

Wniosek

Testowanie i doskonalenie planów ciągłości działania stanowi niezbędny element realnej odporności uczelni wyższych na incydenty cyberbezpieczeństwa. Jednak

[107] NIS2, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, art. 21–23, EUR-Lex,https://eur-lex.europa.eu/eli/dir/2022/2555/oj

w świetle projektu nowej ustawy KSC (2026) istnieje istotne ryzyko nadregulacji tego obszaru, prowadzącej do nadmiernej formalizacji działań oraz wzrostu obciążeń organizacyjnych i finansowych. Kluczowym wyzwaniem pozostaje zachowanie zgodności z KSC przy jednoczesnym wdrażaniu proporcjonalnych, skutecznych i testowanych mechanizmów ciągłości działania, zgodnych z intencją dyrektywy NIS2.

9.9. Wnioski z analizy BIA i ciągłości działania:

Przeprowadzona analiza wpływu biznesowego (BIA) oraz ciągłości działania w środowisku szkolnictwa wyższego wskazuje na istotne luki w podejściu do odporności operacyjnej systemów informacyjnych i procesów organizacyjnych. Brak formalnie przeprowadzonej analizy BIA, nieokreślone lub jedynie orientacyjne parametry RTO i RPO, a także brak regularnych testów planów odtworzeniowych (DR) powodują, że **rzeczywista zdolność organizacji do reagowania na poważne incydenty cyberbezpieczeństwa pozostaje w dużej mierze niezweryfikowana**.
Z perspektywy zarządzania ryzykiem oznacza to, że odporność operacyjna ma charakter deklaratywny, a nie potwierdzony empirycznie. Taki stan uniemożliwia racjonalne planowanie inwestycji w bezpieczeństwo, właściwą priorytetyzację procesów krytycznych oraz podejmowanie świadomych decyzji w zakresie akceptacji ryzyka.
Wnioski w świetle NIS2
Dyrektywa **NIS2** jednoznacznie przesuwa akcent z posiadania dokumentacji na **wykazywalną skuteczność wdrożonych środków**. W obszarze ciągłości działania oznacza to konieczność:

- przeprowadzenia rzetelnej analizy BIA obejmującej procesy kluczowe,
- określenia realistycznych i uzasadnionych parametrów RTO oraz RPO,
- regularnego testowania planów BCP/DR,
- doskonalenia mechanizmów ciągłości działania w oparciu o wyniki testów i incydentów[108].

[108] NIS2, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, art. 21–23, EUR-Lex, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

W tym ujęciu BIA oraz ciągłość działania nie stanowią jednorazowego projektu, lecz **ciągły proces zarządczy**, ściśle powiązany z analizą ryzyka, governance oraz odpowiedzialnością kierownictwa.

Nadregulacja KSC (projekt 2026) a realna odporność

Projekt nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa (2026) formalnie wzmacnia znaczenie ciągłości działania, jednak czyni to w sposób **silnie sformalizowany i administracyjny**[109]. W szczególności projekt:

- rozszerza zakres obowiązków dokumentacyjnych,
- wzmacnia odpowiedzialność kierownictwa za brak wykazania zgodności,
- w ograniczonym stopniu uwzględnia zasadę proporcjonalności do profilu ryzyka i specyfiki sektora.

W rezultacie istnieje ryzyko, że wdrażanie BIA i ciągłości działania będzie realizowane przede wszystkim jako **mechanizm spełnienia wymogów regulacyjnych**, a nie jako narzędzie realnego zwiększania odporności operacyjnej. Nadregulacja może prowadzić do:

- rozbudowy dokumentacji bez równoległego wzrostu zdolności odtworzeniowych,
- koncentracji na audytowalności zamiast na testowalności,
- wzrostu kosztów organizacyjnych i technicznych nieadekwatnych do faktycznych zagrożeń.

Takie podejście stoi w sprzeczności z intencją NIS2 oraz dobrymi praktykami opartymi na normach **International Organization for Standardization ISO 22301**, które traktują BIA i ciągłość działania jako narzędzia zarządcze, a nie wyłącznie obowiązki formalne[110].

---

[109] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity) oraz projekt nowej ustawy KSC (2026), ISAP / Ministerstwo Cyfryzacji,

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

https://www.gov.pl/web/cyfryzacja

[110] International Organization for Standardization, *ISO 22301:2019 – Business continuity management systems*, https://www.iso.org/standard/75106.html

Kierunki działań wynikające z analizy

W świetle powyższych ustaleń działania w obszarze BIA i ciągłości działania powinny koncentrować się na:

a) **Ustrukturyzowaniu analizy BIA**
Analiza BIA powinna zostać przeprowadzona w sposób selektywny i proporcjonalny, obejmując wyłącznie procesy, których zakłócenie ma istotny wpływ na realizację podstawowych funkcji organizacji.

b) **Realistycznym określeniu RTO i RPO**
Parametry te powinny wynikać z rzeczywistych możliwości technicznych i organizacyjnych, a nie wyłącznie z oczekiwań regulacyjnych.

c) **Systematycznym testowaniu planów BCP/DR**
Testy powinny obejmować zarówno aspekty techniczne, jak i organizacyjne, a ich wyniki powinny prowadzić do rzeczywistych działań doskonalących.

d) **Integracji ciągłości działania z zarządzaniem ryzykiem**
BIA, testy oraz plany DR powinny stanowić integralną część systemu zarządzania ryzykiem cyberbezpieczeństwa, a nie odrębny, izolowany obszar.

e) **Zachowaniu proporcjonalności wobec wymogów KSC**
Wdrożenie wymagań nowej ustawy KSC powinno być realizowane w sposób minimalizujący ryzyko nadregulacji, z naciskiem na realną odporność operacyjną, a nie wyłącznie formalną zgodność.

Wniosek końcowy

Analiza BIA i ciągłości działania wskazuje, że kluczowym wyzwaniem w obszarze cyberbezpieczeństwa nie jest brak regulacji, lecz **ryzyko ich nieproporcjonalnej implementacji**. Projekt nowej ustawy KSC (2026), w zestawieniu z wymaganiami NIS2, wymaga podejścia selektywnego i opartego na ryzyku. Tylko wówczas możliwe będzie zbudowanie systemu ciągłości działania, który nie tylko spełnia wymogi formalne, lecz przede wszystkim realnie zwiększa odporność operacyjną organizacji na incydenty cyberbezpieczeństwa.

10. Synteza wyników analizy:

Przeprowadzona analiza cyberbezpieczeństwa w środowisku szkolnictwa wyższego, obejmująca specyfikę zagrożeń, ocenę stanu obecnego organizacyjnego i technicznego,

ocenę zgodności z Krajowym Systemem Cyberbezpieczeństwa oraz analizę rozbieżności względem dyrektywy **NIS2**, analizę ryzyka oraz analizę wpływu biznesowego i ciągłości działania, pozwala na sformułowanie spójnych wniosków o charakterze systemowym i strategicznym.

Kluczowym rezultatem badań jest stwierdzenie, że zasadnicze problemy cyberbezpieczeństwa w uczelniach wyższych **nie wynikają z braku pojedynczych zabezpieczeń technicznych**, lecz z **niedojrzałości całościowego modelu zarządzania cyberbezpieczeństwem**. W analizowanych obszarach dominują rozwiązania:

- reaktywne,
- fragmentaryczne,
- silnie uzależnione od wiedzy i dostępności pojedynczych pracowników,
- słabo osadzone w strukturach decyzyjnych i governance.

Zarówno analiza zgodności z **Krajowy System Cyberbezpieczeństwa**, jak i porównanie z wymaganiami dyrektywy NIS2 wskazują, że wiele organizacji funkcjonuje w stanie **pozornej zgodności formalnej**, która nie przekłada się na realną odporność operacyjną. Zidentyfikowana rozbieżność pomiędzy stanem obecnym (AS-IS) a oczekiwanym poziomem dojrzałości (TO-BE) ma charakter **zarówno organizacyjny, jak i techniczny**, przy czym kluczowe znaczenie mają czynniki organizacyjne i decyzyjne.

10.1. Kluczowe wnioski końcowe – wymiar operacyjny i legislacyjny:

Na podstawie przeprowadzonych analiz sformułowano następujące wnioski końcowe:

a) **Cyberbezpieczeństwo nie jest traktowane jako ryzyko strategiczne.** W obecnym modelu cyberbezpieczeństwo funkcjonuje głównie jako problem operacyjny działów IT, a nie jako element zarządzania strategicznego i ryzyka instytucjonalnego. Ogranicza to skuteczność wdrażanych środków oraz zdolność do podejmowania decyzji o charakterze długofalowym.

b) **Brak dojrzałego systemu zarządzania ryzykiem cyberbezpieczeństwa.** Analiza wykazała, że zarządzanie ryzykiem ma często charakter formalny i jednorazowy, co prowadzi do nieadekwatnej alokacji zasobów, koncentracji na zgodności dokumentacyjnej oraz reaktywnego reagowania na incydenty.

c) **Strukturalne uwarunkowania środowiska akademickiego zwiększają złożoność ryzyka**
Autonomia jednostek organizacyjnych, rozproszenie infrastruktury IT oraz duża rotacja użytkowników znacząco utrudniają wdrażanie jednolitych standardów bezpieczeństwa i centralnych mechanizmów nadzoru.

d) **Zdolność reagowania i ciągłości działania nie została potwierdzona empirycznie**
W wielu przypadkach brak jest regularnych testów planów reagowania na incydenty oraz planów ciągłości działania, co oznacza, że rzeczywista odporność operacyjna pozostaje nieznana.

e) **NIS2 podnosi próg dojrzałości, ale opiera się na zasadzie proporcjonalności.** Dyrektywa NIS2 wymaga nie tylko istnienia procedur, lecz również wykazania ich skuteczności poprzez dowody operacyjne. Jednocześnie pozostawia państwom członkowskim przestrzeń do stosowania podejścia proporcjonalnego i sektorowego.

f) **Projekt KSC w obecnym kształcie wykazuje cechy nadregulacji wobec szkolnictwa wyższego**. Projekt nowej ustawy KSC zmierza w kierunku szerokiego i obligatoryjnego włączania uczelni do kategorii podmiotów ważnych, **bez wystarczającego uwzględnienia ich rzeczywistej roli systemowej, profilu ryzyka oraz dojrzałości organizacyjnej**.

g) **Uczelnie nie są systemowo przygotowane do obligatoryjnego statusu podmiotów ważnych**. Przeprowadzone analizy wskazują, że większość organizacji szkolnictwa wyższego nie posiada obecnie zasobów organizacyjnych, kompetencyjnych i finansowych umożliwiających spełnienie wymogów KSC w reżimie właściwym dla podmiotów ważnych, bez istotnego ryzyka paraliżu decyzyjnego lub formalizacji działań kosztem realnej odporności.

10.2. Wnioski legislacyjne i rekomendowany kierunek regulacyjny:

W świetle powyższych ustaleń zasadne jest przyjęcie podejścia **zgodnego z logiką dyrektywy NIS2**, w którym:

- szkolnictwo wyższe **nie jest automatycznie i obligatoryjnie** kwalifikowane jako sektor objęty statusem podmiotów ważnych,
- status podmiotu ważnego ma charakter **fakultatywny i deklaratywny**, a nie powszechny,
- decyzja o objęciu reżimem podmiotów ważnych powinna być podejmowana **na podstawie rzeczywistego profilu działalności**, a nie wyłącznie formy prawnej organizacji.

Zgodnie z art. 2 ust. 5 lit. b dyrektywy NIS2, uzasadnione jest objęcie pełnym reżimem regulacyjnym wyłącznie tych organizacji sektora szkolnictwa wyższego, które:

- prowadzą badania naukowe o charakterze odkrywczym, eksperymentalnym lub o znaczeniu strategicznym,
- realizują projekty badawcze o wysokiej wrażliwości lub znaczeniu międzynarodowym,
- posiadają status uczelni badawczej lub pełnią funkcję kluczowego ośrodka infrastruktury badawczej.

W takim modelu organizacje mogłyby **samodzielnie zadeklarować** gotowość do objęcia statusem podmiotu ważnego, przyjmując na siebie związane z tym obowiązki i odpowiedzialność. Pozostałe podmioty funkcjonowałyby w lżejszym reżimie, skoncentrowanym na budowaniu podstawowej odporności, a nie pełnej zgodności regulacyjnej.

10.3. Wniosek końcowy:

Przeprowadzona analiza prowadzi do wniosku, że kluczowym wyzwaniem w obszarze cyberbezpieczeństwa szkolnictwa wyższego nie jest brak regulacji, lecz **ryzyko ich nieproporcjonalnego zastosowania**. Projekt KSC, w zestawieniu z dyrektywą NIS2, wymaga rewizji w kierunku podejścia selektywnego, opartego na ryzyku, znaczeniu działalności badawczej oraz rzeczywistej zdolności organizacyjnej.

Tylko takie podejście umożliwi jednoczesne:

- podnoszenie realnej odporności cybernetycznej,
- racjonalne wykorzystanie zasobów publicznych,
- uniknięcie nadregulacji administracyjnej,

- zachowanie zgodności z prawem unijnym i zasadą proporcjonalności.

10.4. Rekomendacje strategiczne:

Rekomendacje strategiczne odnoszą się do decyzji podejmowanych na najwyższym poziomie zarządzania uczelnią i mają charakter długoterminowy.

10.4.1. Umiejscowienie cyberbezpieczeństwa w strategii uczelni:

Cyberbezpieczeństwo powinno zostać formalnie uznane za element strategii rozwoju uczelni oraz zarządzania ryzykiem instytucjonalnym, na równi z ryzykiem finansowym, prawnym i reputacyjnym.

10.4.2. Wzmocnienie governance cyberbezpieczeństwa:

Rekomenduje się ustanowienie jednoznacznego modelu governance, obejmującego:

- odpowiedzialność kierownictwa,
- formalne role (właściciel ryzyka, koordynator cyber),
- cykliczne raportowanie stanu cyberbezpieczeństwa.

10.4.3. Przygotowanie uczelni na wymagania NIS2:

Uczelnie powinny traktować NIS2 jako docelowy punkt odniesienia i rozpocząć transformację systemu cyberbezpieczeństwa jeszcze przed pełną implementacją dyrektywy do prawa krajowego.

10.5. Rekomendacje operacyjne:

Rekomendacje operacyjne dotyczą konkretnych działań organizacyjnych i technicznych.

10.5.1. Organizacyjne:

- wdrożenie cyklicznej analizy ryzyka cyberbezpieczeństwa,
- formalizacja procesu obsługi incydentów,
- systematyczne szkolenia użytkowników,
- standaryzacja zarządzania dostawcami ICT.

10.5.2. Techniczne:

- centralizacja monitoringu bezpieczeństwa,
- wdrożenie jednolitego zarządzania tożsamością i dostępem,
- regularne testy podatności i testy penetracyjne,
- testowanie planów ciągłości działania i odtwarzania systemów.

Wykonawca: **Instytut Patria Polonia Towarzystwa Naukowego KUL**

Partner: **SEQMA Security Management**

Konsultacja: **Instytut Gospodarki Narodowej**