# PROTOKÓŁ z XXVI posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 21 lutego 2025 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

## Otwarcie Posiedzenia – p. Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Pani Przewodnicząca powitała członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości.

## Systemowe wsparcie w zakresie cyberbezpieczeństwa dla sektora naukowo-badawczego.

- Pani Izabela Albrycht, członkini Rady ds. Cyfryzacji, Dyrektor Centrum Cyberbezpieczeństwa AGH - Wprowadzenie, przedstawienie skali problemu na podstawie dostępnych danych z raportów firm analitycznych, wniosków z rozmów przeprowadzonych z przedstawicielami pionów IT / cyber uczelni (2024/2025) i debaty na temat bezpieczeństw badań w kontekście nowego Programu Ramowego FP10.

Pani I. Albrycht wprowadziła do tematu wyzwań dla cyberbezpieczeństwa w sektorze naukowo-badawczym i przedstawiła uwarunkowania w jakich działa sektor. Poinformowała o skali problemu - rekordowym wzroście cyberataków na świecie, o 75% w III kwartale 2024 vs. 2023 (zgodnie z raportem Checkpoint). 50% organizacji, które padły ofiarą naruszeń danych, to instytucje akademickie (2024 Data Breach Investigations Report). Sektor badań i edukacji jest najbardziej narażonym na cyberataki, za nim znajdują się sektory: rządowy/wojskowy i sektor opieki zdrowotnej. Wskazane zostały takie kwestie jak:

- różne rodzaje cyberataków: ransomeware, kompromitacja haseł lub kradzież kont e-mail, ataki phishingowe;
- naruszenia danych: osobowych, badawczych, finansowych;
- ryzyko operacyjne: zakłócenia działalności edukacyjnej i badawczej;
- kradzież własności intelektualnej.

Rośnie znaczenie nowych i przełomowych technologii, także znaczenie sektora akademickiego, badawczo-naukowego dla innowacji na potrzeby bezpieczeństwa narodowego. Wspomniano o wynikach badania zaprezentowanego przez Boston Consulting Group i wskazano ponad 48% zainteresowanie Ministerstw Obrony Narodowej poszczególnych krajów zaangażowaniem uczelni i sektora akademickiego w rozwój ich zdolności. Ponadto, oczekiwane jest także zaangażowanie akceleratorów na rzecz innowacji. W związku z rosnącą potrzebą zaangażowania uczelni, rośnie konieczność zwiększenia cyberbezpieczeństwa i odporności na ataki, w tym cyberszpiegostwo związane z technologiami.

W dalszej części prezentacji Pani I. Albrycht przedstawiła zalecenia Rady UE z 23 maja 2024 r., która dostrzega zagrożenie i m.in. wzywa do podjęcia działań. Zalecenia Rady mają

wpływ również na dyskusję, która toczy się wokół programu *FP10 – Bezpieczeństwo Badań Naukowych* w nowej perspektywie. Przedstawiono także znaczenie FP10 dla cyberbezpieczeństwa, gdzie m.in wskazana została potrzeba powiązania ściśle tego tematu z Dyrektywą NIS2 i nowymi regulacjami UE w zakresie cyberbezpieczeństwa, a także potrzeba wsparcia dla infrastruktury badawczej poprzez zwiększenie inwestycji w bezpieczeństwo cyfrowe.

Przedstawione zostały także przykłady cyberataków wymierzonych w polskie uczelnie wyższe w ostatnich latach. Wymienione zostały wyzwania: zgodność z Dyrektywą NIS2, CER i UKSC, wzmacnianie polityk cyberbezpieczeństwa i systemów reagowania na incydenty, współpraca wewnątrz i międzysektorowa – inicjowanie wymiany informacji o cyberincydentach między uczelniami. Pani I. Albrycht poinformowała, że Centrum Cyberbezpieczeństwa AGH przeprowadziło rozmowy z wieloma uczelniami wyższymi w Polsce i przedstawiła wnioski z tych rozmów. Konieczne jest systemowe wsparcie dla uczelni w wielkim wysiłku budowania cyberbezpieczeństwa. Jednym z tematów do rozważenia jest stworzenie i udostępnienie podmiotom akademickim publicznego rozwiązania klasy SIEM, co znacznie wpłynęłoby na optymalizację wydatków publicznych na działania compliance m.in. z Dyrektywą NIS2, ze strony uczelni wyższych (ale także instytucji publicznych). Pani I. Albrycht wspomniała także o prowadzonym na AGH projekcie SOCCER. W podsumowaniu swojej wypowiedzi Pani I. Albrycht wskazała, że wyzwania cyberbezpieczeństwa będą narastać – konieczne jest proaktywne, strategiczne podejście i systemowe rozwiązania. Kluczowa jest współpraca w modelu *Triple Helix*, tak by sektor rządowy współpracował ze środowiskiem akademickim i przemysłem. Ochrona sektora akademickiego stanowi podstawę innowacyjności państwa, odporności gospodarki i bezpieczeństwa narodowego.

- Pani prof. Agnieszka Gryszczyńska, członkini Rady ds. Cyfryzacji – przedstawienie wniosków z badań potrzeb dot. budowania kompetencji w zakresie cyberbezpieczeństwa pionów IT uczelni (2023).

Pani A. Gryszczyńska zreferowała ustalenia realizowanego zadania - podnoszenia kompetencji cyfrowych w szkołach wyższych, gdzie liderem konsorcjum został Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie. Konsorcjanci, którzy podpisali umowy wykonawcze w 2023 r. to Katolicki Uniwersytet Lubelski, Uniwersytet Szczeciński, Uniwersytet Śląski w Katowicach i Uniwersytet Wrocławski. Zadanie było zlecone przez Ministra Edukacji i Nauki. Zrealizowano jedynie część tego zadania z uwagi na to, że po podjętych działaniach w 2023 r. i maju 2024 r. rozwiązano umowę, jako przyczynę wskazując uwagę o braku uzasadnienia dla jej realizacji wobec ograniczonych środków budżetowych w zakresie szkolnictwa wyższego i nauki. Badano programy studiów pod kątem kompetencji cyfrowych. Dokonano badania pilotażowego pionów informatycznych uczelni wyższych. Badanie zostało przeprowadzone w listopadzie i grudniu 2023 r. Ankiety zostały skierowane do sześciu uczelni - w sumie 161 ankiet, przy czym część nie była całkowicie wypełniona, wobec czego efektywnie ukończono 115. Badanie pozwoliło na wskazanie przyczyn zwiększającej się rotacji pracowników pionów informatycznych i określenie ich potrzeb w

kontekście rozwijania posiadanych kompetencji cyfrowych. Pani A. Gryszczyńska przedstawiła wnioski z przeprowadzonego badania - pracownicy działów informatycznych uczelni wyższych charakteryzują się zwykle bardzo krótkim stażem pracy, często brakiem wykształcenia informatycznego. Kluczowe dla dalszych analiz jest wyodrębnienie osób odpowiedzialnych za konkretne działania. Pracownicy działów IT otrzymują wynagrodzenie zdecydowanie poniżej oczekiwań i możliwości jakie w tym zakresie oferuje rynek. W kontekście stażu pracy na uczelni, dyskusyjne są zarobki pracowników działów informatycznych uczelni wyższych. Kwestia wynagrodzenia niewątpliwie rzutuje na poziom satysfakcji z pracy, co skłania do chęci zmiany zatrudnienia.

W dalszej części wypowiedzi Pani A. Gryszczyńska poinformowała, że w ramach realizowanych zadań odbyła się konferencja na temat wzmacniania odporności szkół wyższych na cyberataki, na której przedstawiono wyniki m.in. analizy ataków na uczelnie wojskowe. Podczas konferencji prezentowano również wyniki działań NASK w zakresie cyberbezpieczeństwa. Wśród rekomendacji wskazano m.in. centralizację usług, ale też skorzystanie z narzędzi oraz ochrony, którą zapewnia NASK.

- Pan dr hab. Dariusz Szostek, prof. UŚ, Przewodniczący Komitetu ds. Cyberbezpieczeństwa przy Konferencji Rektorów Akademickich Szkół Polskich (KRASP) - nowe obowiązki uczelni wynikające z NIS2/KSC 2.0 i problem zapewnienia finansowania na realizację tych obowiązków, działania KRASP.

Pan Profesor zauważył, że uczelnie wyższe do tej pory nie dostrzegały problematyki nie tylko cyberbezpieczeństwa, ale także cyfryzacji uczelni. Uczelnie powinny być podmiotem krytycznym nie tylko ze względu na problematykę prowadzonych w nich badań, ale także ze względu na powiązaną infrastrukturę internetu. Większość zaobserwowanych ataków dotyczyły głównie przejęcia infrastruktury. Obecnie uczelnie wyższe nie są w stanie samodzielnie podnieść kompetencji do poziomu określonego w ustawie o KSC. Pojawiło się pytanie czy nie należy popracować nad nieco innymi kryteriami w zakresie podziału i wskazania uczelni krytycznych oraz ważnych. Uczelnie wyższe są nadzorowane przez różne ministerstwa, co stanowi olbrzymi problem. Pan Profesor wskazał, że w ubiegłym roku zostało przeznaczonych 200 mln zł na uczelnie wyższe w zakresie podniesienia poziomu cyberbezpieczeństwa. W rzeczywistości te środki zostały wykorzystane na nieznaczne poprawienie długu technologicznego.

Przede wszystkim najważniejszym dostrzeżonym elementem jest brak stałego finasowania w zakresie zabezpieczenia uczelni wyższych przed cyberzagrożeniami. Aktualna subwencja nie obejmuje zadań wynikających z UKSC, a te wymagają zarówno jednorazowych nakładów jak i później stałych. Dlatego należy utworzyć, i o co KRASP wnioskuje fundusz Cyberbezpieczna Uczelnia, w ramach którego możliwe by było dostosowanie uczelni do wymogów projektowanej regulacji. Drugim elementem jest podniesienie świadomości kierownictwa uczelni wyższych w zakresie zagrożeń i obowiązków, które będą z tym związane. Ponadto, problemem jest niewielki prestiż dyrektorów IT czy osób zajmujących się cyberbezpieczeństwem, w tym bardzo niskie zarobki uczelnianych informatyków. Pan

Profesor skierował do Rady prośbę o rekomendacje w zakresie działań jakie powinny podejmować uczelnie wyższe, aby dostosować wymogi do projektowanych przepisów. W tym rekomendacje techniczne, z uwzględnieniem specyfiki uczelni wyższych. Wsparcie w zakresie działań (także finansowe) dla podniesienia świadomości kierownictwa, a także działów IT oraz wsparcie, w tym finansowe w zakresie tworzenia regionalnych SOK dla uczelni, również większe wsparcie NASK.

Zwrócił także uwagę, iż jest niewłaściwym działaniem nakładanie nowych obowiązków bez zapewnienia finansowania ich wykonania.

Ponadto, polepszenia wymagają kompetencje cyfrowe wśród młodzieży i studentów. Pan Profesor zgłosił propozycję wykorzystania kadr uczelni wyższych – infrastruktura i możliwości, które są związane z dotarciem bezpośrednio do miliona studentów oraz kilkudziesięciu tysięcy pracowników dają olbrzymią szansę podniesienia w dosyć szybkim trybie tych umiejętności, poprzez powszechne a nawet obowiązkowe szkolenie z zakresu cyberzagrożeń i cyberhigieny.

- Pan prof. Mirosław Kutyłowski, Przewodniczący Sekcji Bezpieczeństwa Teleinformatycznego Komitetu Informatyki PAN - Wsparcie działań na rzecz rozwoju rozwiązań dla bezpieczeństwa sieci i systemów ICT, w tym inwestycje w R&I dla cyberbezpieczeństwa i kształcenie zaawansowanych kadr oraz badań podstawowych w obszarze AI, cyberbezpieczeństwa i innych technologii ICT w kontekście dyskusji o FP 10.

Pan Profesor poinformował, że pod koniec ubiegłego roku Komitet Informatyki PAN ogłosił *List Otwarty w sprawie inwestycji w kształcenie zaawansowanych kadr i badania podstawowe w obszarze AI, cyberbezpieczeństwa i innych technologii ICT*. Wskazał, że otwiera się duży rynek na wysoko wykwalifikowanych informatyków, zwłaszcza w obszarach krytycznych, jak sztuczna inteligencja i cyberbezpieczeństwo. Są jednostki, które reprezentują bardzo wysoki poziom, jednak mają dramatyczne problemy z pozyskaniem kadry posiadającej odpowiednie wykształcenie czy umiejętności. W Polsce brak jest dedykowanych programów na cyberbezpieczeństwo czy AI tak jak ma to miejsce w innych krajach. W swoim stanowisku Komitet Informatyki PAN wskazał, że potrzebna jest długofalowa strategia w rozwoju ICT w Polsce. Należy zwiększyć nakłady na kształcenie zaawansowanych specjalistów w tych dziedzinach. Zauważonym w stanowisku problemem, jest brak udziału środowiska akademickiego z zaawansowanych technik w gremiach dot. ICT. W odniesieniu do tematu edukacji, stwierdzone zostało, że jest bardzo mało specjalistów z tej dziedziny oraz wskazano na ich rozproszenie. Obecne przeszkody formalne czy szkoły doktorskie skutecznie likwidują możliwości skupienia tych środków mimo możliwości technicznych. W nawiązaniu do tematyki cyberbezpieczeństwa dokonujący się proces, to kierowanie w stronę braku cyberbezpieczeństwa i kontroli nad danymi – informacje naukowe często krytyczne są przesyłane do usług chmurowych bez kontroli. Kontroli brakuje także nad efektami prac o dualnym wykorzystaniu. Pan Profesor wskazał na pilną konieczność zagwarantowania podstawowego poziomu bezpieczeństwa poprzez

zapewnienie dostępu do kilku kluczowych narzędzi, jak wskazano w stanowisku Sekcji Bezpieczeństwa Teleinformatycznego KI PAN:

1) przestrzeń do przechowywania danych z zapewnieniem silnej kontroli dostępu i odporności na zniszczenie i manipulacje, z wykorzystaniem szyfrowania E2E oraz replikacji,
2) narzędzia do bezpiecznej edycji materiałów naukowych (wraz z możliwością jednoczesnej edycji, automatyczną korektą językową itp.)
3) narzędzia do bezpiecznego przetwarzania danych (np. narzędzia statystyczne),
4) narzędzia do bezpiecznej komunikacji (telekonferencje, czat) w trybie szyfrowania E2E. Stanowisko Sekcji wskazuje także na potrzebę systemowej zmiany w podejściu do ochrony danych o podwójnym zastosowaniu.

Obecny na posiedzeniu Pan Dyrektor Paweł Dziuba wskazał, że z jednej strony istnieje potrzeba udostępniania danych i dzielenia się wynikami, a z drugiej strony nałożenia pewnego mechanizmu, który to działanie ogranicza. Im wcześniej uczelnie rozpoczną swoją pracę od podstaw – cyberhigieny, budowania świadomości do wdrażania odpowiednich mechanizmów poprzez narzędzia i procedury, tym szybciej nastąpi uniemożliwienie albo ograniczenie niebezpieczeństwa wydostawania się lub przekazywania wyników prac na zewnątrz.

- Pan Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa MC oraz Pani Monika Pieniek, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa MC – przedstawienie krajobrazu cyberzagrożeń dla sektora naukowo-badawczego w Polsce.

Pan Dyrektor M. Wysocki omówił statystyki z NASK dot. zagrożeń dla uczelni i podmiotów badawczych, ze wskazaniem, że są one na poziomie edukacji i oświaty, stąd też metodyka porównawcza jest inna. Pan Dyrektor odniósł się do wypowiedzi Pana Profesora D. Szostka co do kwalifikacji podmiotów z perspektywy Dyrektywy NIS 2 i nowelizacji ustawy o KSC. Logika tego podziału jest taka, że sektor badania naukowe to tzw. sektor ważny, na który składają się organizacje badawcze oraz m.in. uczelnie, Polska Akademia Nauk, instytuty naukowe PAN. Bycie podmiotem ważnym oznacza pewną odwilż obowiązków, zmniejszenie kosztów po stronie podmiotów ważnych co do wdrożenia rozwiązań, ponieważ nie będą zobowiązane do wprowadzania cyklicznych audytów. W tej kwestii nie ma znaczenia czy uczelnia jest prywatna czy publiczna. Obecnie, uczelnie publiczne są zobowiązane do stosowania wymagań dot. systemów bezpieczeństwa informacji z Rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

Pani Dyrektor M. Pieniek wskazała, że do tej pory uczelnie nie były tak mocno wspierane przez MC, ze względu na ogrom pracy do zrealizowania w innych obszarach, w szczególności dotyczących podmiotów, od których zależy ludzkie życie jak w sektorze zdrowia czy

funkcjonowanie usług publicznych świadczonych przez urzędy np. administrację samorządową.

Wypracowując systemowe wsparcie, MC skupia się na wdrożeniu przepisów Dyrektywy NIS2 oraz nowelizacji ustawy o KSC, a co za tym zmierza, należy w pierwszej kolejności wesprzeć podmioty, które będą zobowiązane do wspierania kolejnych podmiotów, aby system mógł funkcjonować (to dot. CSIRTów sektorowych). Powstanie obowiązek ustanowienia CSIRTu sektorowego dla sektora edukacji, który częściowo będzie finansowany ze środków Krajowego Planu Odbudowy, a w pozostałym zakresie zwiększone zostaną odpowiednio części budżetowe poszczególnych dysponentów. Kolejnym planowanym przez MC wsparciem dla CSIRTów sektorowych będzie wsparcie szkoleniowe – specjalistyczne szkolenia dedykowane tylko kadrze pracującej w tych CSIRTach. W zamierzeniach jest także wsparcie merytoryczne – uświadamianie o faktycznie spoczywających obowiązkach na odpowiednich osobach w danych instytucjach. Ponadto, MC oferuje dołączenie pracowników uczelni do szkoleń z cyberhigieny. Szkolenia prowadzone są z partnerami z PWCyber oraz NASK. Pani Dyrektor poinformowała także, że MC organizuje wiele różnych wydarzeń mających na celu zarówno promocję cyberbezpieczeństwa, jak i docieranie z problematyką do różnych kręgów odbiorców.

Po zreferowaniu zagadnień zawartych w agendzie posiedzenia, głos zabrał Pan Prezes Wiesław Paluszyński, który zauważył że nauczenie studenta cyberhigieny musi być związane jednocześnie z budową na uczelni działań zgodnych z zasadami cyberhigieny, co pozwala na osiągniecie zamierzonego efektu. Kolejną, istotną sprawą jest zbudowanie szkoleń ekspertów. Stwierdzono, że brakuje formalnego systemu potwierdzania kwalifikacji nabytych podczas szkoleń. Należy najpierw zbudować rozwiązania systemowe, które wesprą m.in. sektor nauki.

Jeden z członków Rady poparł ideę SOCów oraz ISACA– to rozwiązanie, które może pomóc w działaniach u podstaw kwestii związanych ze zwalczaniem cyberzagrożeń w środowisku uczelni wyższych. Odniesiono się do współpracy międzysektorowej i nie zauważono możliwości współpracy z wyższymi uczelniami wojskowymi ze względu na specyfikę tych uczelni, które są atakowane w ramach wojny hybrydowej, co bezpośrednio wpływa na sytuację tych instytucji oraz ich funkcjonowanie. Za istotną uznano koncepcję Cyberparków Technologicznych – międzyresortowych i międzysektorowych. Wyrażano zdanie, że ta koncepcja jest najlepsza w kontekście budowania pierwszych działań związanych ze wsparciem wynalazków tajnych czy organizacją badań mających charakter strategiczny.

W toku dyskusji pojawiła się wypowiedź zachęcająca do uruchomienia programu analogicznego jak PWCyber. Ponadto, zwrócono uwagę, że element cyberbezpieczeństwa to jeden z trzech podstawowych elementów bezpieczeństwa w ogólnym tego słowa znaczeniu. Bezpieczeństwo fizyczne, zabezpieczenie budynków i dostępów do nich jest dużym zadaniem dla uczelni. Na kwestie cyberbezpieczeństwa należy patrzeć z punktu wdrożenia Dyrektywy CER. Może okazać się, że uczelnie lub instytuty znajdą się w łańcuchu różnych ważnych

podmiotów krytycznych i usług nawet na szczeblu lokalnym. Poruszono także kwestię zabezpieczenia przetwarzania i przesyłania informacji niejawnych.

Pani Przewodnicząca poinformowała, że zostanie przygotowany projekt stanowiska w zakresie przedmiotowego tematu. Poprosiła zaproszonych gości o ewentualne przesłanie dodatkowych materiałów, które mogłyby stanowić inspirację dla stanowiska Rady, a także członków Rady do przesyłania mailowo propozycji treści stanowiska.

## Sprawy różne.

Pani Przewodnicząca wspomniała o przygotowaniu stanowiska w sprawie cyberbezpieczeństwa w ochronie zdrowia, a także w temacie technologicznym, który pojawił się w kontekście opublikowanego projektu amerykańskiej regulacji ograniczającej możliwości sprzedaży chipów AI do niektórych krajów.

Dyskutowano także nad szczegółami tematyki najbliższych posiedzeń Rady.

## Uczestnicy posiedzenia:

### Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska – Przewodnicząca
6. Janusz Kosiński
7. Anna Beata Kwiatkowska
8. Jarosław Mojsiejuk
9. Krzysztof Silicki
10. Katarzyna Szymielewicz
11. Sławomir Wojciechowski

### Zaproszeni goście:

12. Dariusz Szostek, prof. UŚ, Przewodniczący Komitetu ds. Cyberbezpieczeństwa przy Konferencji Rektorów Akademickich Szkół Polskich (KRASP)
13. Mirosław Kutyłowski**,** Przewodniczący Sekcji Bezpieczeństwa Teleinformatycznego Komitetu Informatyki PAN
14. Paweł Dziuba, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Obrony Narodowej
15. Wiesław Paluszyński, Prezes Polskiego Towarzystwa Informatycznego
16. Monika Pieniek, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
17. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC

### Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

18. Karolina Taczalska, Biuro Ministra w MC
19. Joanna Gójska, Biuro Ministra w MC