CYBERSEC
EXPO & FORUM

UMIEJĘTNOŚCI I CYBERHIGIENA – WSPARCIE I ROZWÓJ KOMPETENCJI CYFROWYCH

POLICY BRIEF

Spis treści

Szanowni Państwo,

podczas **CYBERSEC EXPO & FORUM 2024**, w dniu 19 czerwca w Krakowie, w obecności wicepremiera i ministra cyfryzacji Krzysztofa Gawkowskiego, został podpisany list intencyjny pomiędzy Instytutem Kościuszki a Europejską Organizacją Cyberbezpieczeństwa (ECSO) w sprawie organizacji cyklu wydarzeń poświęconych priorytetom polityki cyfrowej i technologicznej polskiej prezydencji w Radzie UE.

Celem inicjatywy jest wsparcie polskiej prezydencji w realizacji celów związanych z cyberbezpieczeństwem i nowymi technologiami, wzmocnienie międzysektorowego dialogu na temat wyzwań cyfrowych oraz zaangażowanie zróżnicowanych interesariuszy w kształtowanie polityk publicznych, przyczyniając się do opracowania konkretnych strategii i rozwiązań.

W obliczu szybko postępującej cyfryzacji oraz rosnących wyzwań związanych z cyberbezpieczeństwem, kompetencje cyfrowe i świadomość zasad cyberhigieny stanowią niezbędne fundamenty dla stabilnego rozwoju społeczeństwa informacyjnego. Dokument ten, przygotowany dla Ministerstwa Cyfryzacji, zawiera rekomendacje dotyczące działań mających na celu wskazanie luk, podniesienie poziomu wiedzy i umiejętności w zakresie bezpiecznego użytkowania technologii cyfrowych w Polsce. Rekomendacje te opierają się na wiedzy i doświadczeniu ekspertów uzasadnionych wynikach analizy kluczowych wyzwań w obszarze umiejętności cyfrowych i cyberhigieny, zidentyfikowanych przez grupę roboczą złożoną z ekspertów sektora publicznego, przedstawicieli Europejskiej Organizacji Cyberbezpieczeństwa (ECSO), sektora prywatnego oraz ośrodków edukacyjnych.

Prace nad policy brief są spójne ze Strategią Rozwoju Kompetencji Cyfrowych na lata 2025-2035, opublikowaną przez Ministerstwo Cyfryzacji oraz uwzględniają kluczowe priorytety Polski wynikające z objęcia przewodnictwa w Radzie Unii Europejskiej.

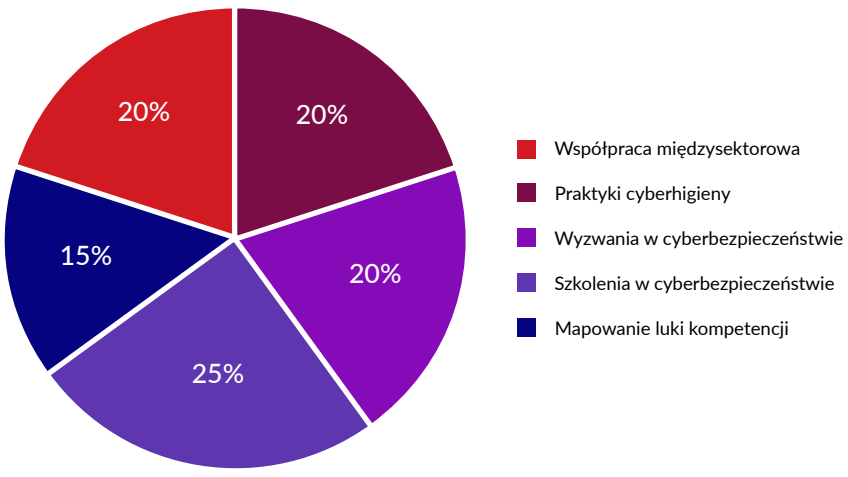
Wypracowane rekomendacje będą stanowić wkład w realizację celów wspólnotowych, takich jak budowa bezpiecznej i cyfrowo odpornej Europy, poprzez rozwój narzędzi wsparcia i edukacji w zakresie cyberbezpieczeństwa.

Niniejszy dokument zawiera propozycje konkretnych działań, które mają pomóc w realizacji założeń strategii Ministerstwa, zapewniając tym samym, że społeczeństwo i instytucje zyskają świadomość oraz przygotowanie do wyzwań cyfrowej przyszłości, a także zyskają zdolność do skutecznej ochrony swoich zasobów oraz danych w coraz bardziej skomplikowanym środowisku cyfrowym.

Policy brief został podzielony na pięć obszarów:

1. Wyzwania w cyberbezpieczeństwie – umiejętności
2. Mapowanie luki w umiejętnościach cyberbezpieczeństwa
3. Szkolenia w dziedzinie cyberbezpieczeństwa
4. Praktyki cyberhigieny i bieżące wyzwania
5. Współpraca międzysektorowa

Udział głównych obszarów rekomendacji



Pragniemy serdecznie podziękować wszystkim członkom grupy roboczej, których zaangażowanie, wiedza i doświadczenie przyczyniły się do powstania niniejszego dokumentu. Wypracowane rekomendacje stanowią istotny krok w budowaniu cyfrowego i bezpiecznego społeczeństwa. Składamy serdeczne podziękowania Ministerstwu Cyfryzacji za nieocenione wsparcie i zaangażowanie, które w istotny sposób przyczyniły się do realizacji naszego przedsięwzięcia. Doceniamy Państwa profesjonalizm, otwartość na współpracę oraz wkład, które mają znaczenie dla szerokiego grona odbiorców i wspierają naszą wspólną misję.

Skład grupy roboczej:

1. dr inż. Jędrzej Bieniasz – Centrum Cyberbezpieczeństwa, Politechnika Warszawska
2. Wojciech Bobak – Wyższa Szkoła Biznesu National-Louis University
3. Ivan Bornacelly – OECD Centre for Skills
4. Beata Chodacka – Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
5. Marietta Gieroń – Instytut Kościuszki
6. Kayle Giroud – Global Cyber Alliance
7. Paulina Górska – Instytut Kościuszki
8. Sid Hollman – Digital Europe
9. Karol Jędrasiak – GETES Institute
10. Łukasz Jędrzejczak – Deloitte
11. Katarzyna Nowak –Ministerstwo Cyfryzacji
12. płk dr Piotr Potejko – Uniwersytet Warszawski
13. Michał Pukaluk – Ministerstwo Cyfryzacji
14. Krzysztof Sierański – Fundacja Bezpieczeństwa Informacji
15. Alek Tarkowski – Open Future Foundation
16. Mariusz Ustyjańczuk – Deloitte
17. Martyna Wilk – Wrocławskie Centrum Rozwoju Społecznego
18. Katarzyna Wójtowicz-Garcarz – GETES Institute

Dziękujemy również **wszystkim instytucjom partnerskim i ekspertom**, którzy wspierali nasze prace merytoryczne i organizacyjne.

TEMAT I:

Wyzwania w cyberbezpieczeństwie – umiejętności

Kompetencje w obszarze cyberbezpieczeństwa są dziś kluczowe dla funkcjonowania społeczeństwa i gospodarki, jednak luka umiejętności w tej dziedzinie stanowi poważne wyzwanie. Identyfikujemy niedobór specjalistów, brak podstawowej edukacji cyfrowej oraz wykluczenie technologiczne w różnych grupach społecznych, które wymagają pilnych działań. Cyberbezpieczeństwo to nie tylko ochrona systemów, ale także rozwijanie umiejętności praktycznych, krytycznego myślenia i odporności na dezinformację. Inwestycje w edukację, zharmonizowane programy certyfikacji i współpraca międzysektorowa są niezbędne, by budować odporne społeczeństwo i sprostać wyzwaniom cyfrowej rzeczywistości.

WYZWANIA I REKOMENDACJE

WYZWANIA

W Unii Europejskiej brakuje około 3 milionów specjalistów ds. cyberbezpieczeństwa, w Polsce również występuje znacząca luka w tej dziedzinie. Luka w umiejętnościach obejmuje zarówno kompetencje techniczne, jak i miękkie, co stanowi ogromne wyzwanie dla rynku pracy. Sytuację pogarsza odpływ ekspertów za granicę oraz podstawowe braki edukacyjne w społeczeństwie, co wymaga kompleksowego podejścia obejmującego całe społeczeństwo.

Jednocześnie widoczny jest wyraźny niedobór podstawowej wiedzy w zakresie cyfrowego BHP i umiejętności praktycznych, takich jak rozumienie struktury danych czy zasady bezpiecznego udostępniania informacji. Aby wypełnić te luki, pracodawcy coraz częściej wybierają szkolenia w miejscu pracy i coaching jako skuteczne metody rozwijania wymaganych kompetencji.

Problem luki w umiejętnościach cyfrowych dotyczy nie tylko branży technologicznej, ale całego społeczeństwa. Wciąż wiele osób ma podstawowe braki w obsłudze komputera czy programów software, jak Microsoft Office. Choć fundacje i organizacje pozarządowe prowadzą programy mające na celu rozwój świadomości w zakresie cyberbezpieczeństwa i kompetencji cyfrowych, w praktyce uwidaczniają się bardziej fundamentalne braki w wiedzy i umiejętnościach. Brak motywacji do ich uzupełnienia pogłębia zjawisko wykluczenia cyfrowego.

Paradoksalnie, szybki rozwój technologii nie przyczynił się do zmniejszenia luki, lecz ją pogłębił. Osoby wykazujące deficyty w zakresie kompetencji cyfrowych, w szczególności osoby starsze, doświadczają narastających trudności w procesie kompensacji tych braków. Wykluczenie cyfrowe jest szczególnie dotkliwe w grupie wiekowej 60+, gdzie umiejętności często ograniczają się do podstawowej obsługi komputera, a dostęp do możliwości rozwoju pozostaje ograniczony.

Różnice pokoleniowe w podejściu do technologii dodatkowo wzmacniają te nierówności. Starsze pokolenie często wykazuje brak zaufania do technologii oraz trudności w ich przyswajaniu, podczas gdy młodsze, choć wychowane w cyfrowym środowisku, często nie posiada umiejętności krytycznej analizy informacji ani odporności na dezinformację. Te rozbieżności prowadzą do powstawania błędnych przekonań i mitów, które utrwalają bariery międzypokoleniowe oraz hamują rozwój niezbędnych kompetencji cyfrowych w społeczeństwie.

REKOMENDACJE

6. Podstawą jest stworzenie kompleksowego katalogu kompetencji, który obejmie zarówno umiejętności miękkie, jak i twarde w obszarze cyfrowym. Kluczowym elementem tego procesu powinno być wsparcie dla ciągłego rozwoju kompetencji oraz promowanie idei kształcenia przez całe życie. Niezbędne jest precyzyjne określenie zakresu kompetencji w sylwetce absolwenta, tak aby odpowiadała ona bieżącym potrzebom rynku pracy. W tym celu katalog kompetencji powinien być opracowywany we współpracy z przedstawicielami biznesu, co pozwoli dostosować go do aktualnych wymagań zawodowych. Absolwenci szkół powinni nie tylko posiadać podstawowe umiejętności cyfrowe, ale także być przygotowani do funkcjonowania w intensywnie zmieniających się warunkach technologicznych. Systematyzacja sylwetki absolwenta oraz jasno określony katalog umiejętności będą kluczowe dla skutecznego przygotowania osób do wyzwań współczesnego świata. Ważnym partnerem w tym procesie może być Unia Europejska, która stanowi naturalną platformę współpracy w zakresie budowania jednolitych standardów kompetencji cyfrowych.

7. Programy edukacyjne powinny integrować zarówno kompetencje cyfrowe, jak i umiejętności miękkie, takie jak krytyczne myślenie, analiza sytuacji oraz rozwiązywanie problemów. Należy przyjąć strukturalne podejście do nauczania, które koncentruje się na zrozumieniu procesów systemowych i działania technologii, zamiast ograniczać się do obsługi konkretnych narzędzi. Niezbędna jest także reorganizacja programów edukacyjnych. Cyberbezpieczeństwo powinno być włączone w programach edukacyjnych na wczesnych etapach, promując świadomość i rozwój umiejętności już w młodym wieku. System edukacyjny powinien łączyć formalne ścieżki uniwersyteckie z nieformalnym kształceniem, zapewniając wzajemne uzupełnianie się certyfikatów i studiów. Dostosowanie programów szkoleniowych do zmieniających się potrzeb rynku pracy wymaga bliskiej współpracy z pracodawcami, decydentami politycznymi i instytucjami edukacyjnymi. Wprowadzenie minimum programowego, obejmującego podstawy cyfrowego BHP, wraz z jego skutecznym wdrażaniem i egzekwowaniem, stanowi priorytet w budowaniu świadomego społeczeństwa. Dodatkowo, edukację i świadomość społeczną należy wspierać za pomocą efektywnych kampanii informacyjnych, które budują zaufanie i podkreślają znaczenie kształcenia w obszarze IT oraz cyberbezpieczeństwa. Przekrojowe podejście do nauczania, łączące kompetencje miękkie i twarde, stanowi solidną podstawę współczesnych programów edukacyjnych, odpowiadając na potrzeby zmieniającego się rynku pracy. Budowa strategii edukacyjnej wspierającej rozwój kompetencji cyfrowych na poziomie lokalnym i centralnym, w tym współpraca z samorządami, jest istotnym krokiem w eliminowaniu luki w umiejętnościach.

8. Istotne jest poszerzenie dostępu do stanowisk juniorskich, praktyk i staży, które koncentrują się na zdobywaniu praktycznego doświadczenia, a nie wymagają obszernych certyfikatów. Ważne jest tworzenie środowisk wspierających przekwalifikowanie i budowanie kompetencji, np. przez organizację warsztatów i dedykowanych szkoleń. Jednocześnie potrzebna jest zmiana narracji – warto mówić o cyberbezpieczeństwie jako o przestrzeni, w której liczy się nauka i rozwój, a nie tylko wąskie specjalizacje. Pracodawcy powinni zrewidować swoje wymagania kwalifikacyjne, koncentrując się na praktycznych umiejętnościach, takich jak portfolio projektów czy testy praktyczne, zamiast formalnych referencji. Mikro-certyfikaty, kursy online oraz inne alternatywne kwalifikacje powinny być bardziej doceniane.

9. Fundamentalna jest zmiana całego podejścia zachęcająca do przekwalifikowania osób z innych dziedzin oraz włączenie osób z umiejętnościami nietechnicznymi, które mogą rozwijać swoje kompetencje w miejscu pracy. Rekomendujemy komunikowanie, że umiejętności miękkie, takie jak krytyczne myślenie i zarządzanie projektami, mają ogromne znaczenie w cyberbezpieczeństwie. Zespoły różnorodne pod względem kompetencji funkcjonują znacznie sprawniej, co powinno być podkreślane w działaniach informacyjno-promocyjnych.

10. Biorąc pod uwagę alarmująco niski wskaźnik kobiet pracujących w branży ITC, należy unikać stereotypowych kampanii reklamowych, takich jak „I Ty możesz pracować w IT", które pomijają dotychczasowe doświadczenia i umiejętności potencjalnych kandydatek oraz w rezultacie powodują odwrotny skutek. Wprowadzenie programów wspierających kobiety w IT, takich jak szkolenia z zakresu wykrywania incydentów, gdzie ich uważność jest niewątpliwym atutem, może przyczynić się do zwiększenia ich udziału w branży.

11. Warto rozważyć stworzenie platformy edukacyjnej, na przykład w ramach aplikacji M-Obywatel, która mogłaby służyć jako przestrzeń informacyjno-edukacyjna. Taka inicjatywa mogłaby zwiększać świadomość na temat metod oszustw skierowanych do seniorów, uczyć rozpoznawania wiarygodnych źródeł informacji oraz wspierać walkę z dezinformacją. Szczególną uwagę należy poświęcić problemowi niedostatecznych umiejętności cyfrowych wśród

starszych pokoleń, wspierając ich adaptację do dynamicznego rozwoju technologicznego. Działania te mogłyby obejmować tworzenie przestrzeni edukacyjnych związanych z cyberbezpieczeństwem, budowanie zaufania do technologii oraz podkreślanie znaczenia współdziałania na rzecz bezpieczeństwa w sieci. Ważnym elementem strategii jest wzmacnianie poczucia sprawczości w społecznościach oraz realizacja programów międzypokoleniowych, które pomagają pokonać bariery i integrować różne grupy wiekowe wokół wspólnych celów edukacyjnych. Jednocześnie należy przeciwdziałać „cyberoporowi" - postawie niechęci wobec nauki nowych kompetencji cyfrowych, które stają się niezbędne w życiu codziennym oraz cyfrowej rzeczywistości. Systematyczne monitorowanie i analiza działań w obszarze cyberprzestrzeni pozwolą na lepsze kształtowanie jej rozwoju. Tylko konsekwentne wsparcie w nauce i otwartości na nowe technologie pozwoli stworzyć świadome i odporne społeczeństwo cyfrowe.

12. Decydenci polityczni odgrywają istotną rolę w tworzeniu warunków sprzyjających rozwojowi kompetencji cyfrowych i zawodowych. Niezbędne jest zapewnienie stabilnego i adekwatnego finansowania, wspieranie regulacji umożliwiających większą elastyczność w edukacji i zatrudnieniu oraz promowanie uznawanych w całej UE standardów certyfikacji. Działania te powinny być skoordynowane z długoterminową strategią rozwoju rynku pracy, uwzględniającą dynamiczne zmiany technologiczne i potrzeby różnych grup społecznych. Organizacje pozarządowe mogą odegrać znaczącą rolę w organizacji szkoleń i certyfikacji dla ekspertów ICT, szczególnie w obszarach wykluczonych cyfrowo. Aby jednak w pełni wykorzystać ich potencjał, konieczne jest wsparcie finansowe oraz stworzenie odpowiednich ram prawnych ułatwiających współpracę międzysektorową. Taka współpraca mogłaby obejmować partnerstwa publiczno-prywatne, umożliwiające efektywne wykorzystanie dostępnych zasobów oraz wprowadzenie innowacyjnych rozwiązań. Ponadto warto zadbać o rozwój programów edukacyjnych skierowanych do grup defaworyzowanych, takich jak osoby starsze, kobiety wchodzące na rynek pracy w obszarze ICT, czy młodzież z regionów o ograniczonym dostępie do nowoczesnych technologii. Kluczowe jest także inwestowanie w działania promujące świadomość znaczenia kompetencji cyfrowych w codziennym życiu, zarówno w kontekście zawodowym, jak i społecznym. Budowanie świadomości społecznej, wspieranie rozwoju lokalnych liderów oraz motywowanie młodych ludzi do angażowania się w branżę ICT może przyczynić się do stworzenia bardziej zrównoważonego i odpornego rynku pracy, gotowego sprostać wyzwaniom przyszłości.

13. Niezwykle istotne jest wprowadzenie jednolitych, europejskich programów certyfikacji, które będą obejmować zarówno kompetencje techniczne, jak i umiejętności miękkie, niezbędne w nowoczesnych środowiskach pracy. Certyfikaty te, uznawane w całej Unii Europejskiej, mogą przyczynić się do stworzenia spójnego systemu oceny kwalifikacji, ułatwiając przepływ specjalistów między państwami członkowskimi. Kluczowym aspektem tego podejścia jest rozwijanie praktycznych programów edukacyjnych we współpracy z pracodawcami. Praktyczne kształcenie w rzeczywistych warunkach zawodowych oraz promowanie uznawalnych certyfikatów może zachęcić szersze grupy społeczne do podejmowania nauki w obszarze cyberbezpieczeństwa i innych dziedzin IT. Certyfikaty potwierdzające konkretne umiejętności otwierają drogę dla osób, które, mimo braku tradycyjnego wykształcenia akademickiego, posiadają talent i motywację do rozwoju. Dzięki temu możliwe jest pozyskiwanie nowych pracowników o różnorodnych profilach kompetencyjnych. Warto również rozwijać modułowe ścieżki edukacyjne, które pozwalają na stopniowe zdobywanie kwalifikacji dostosowanych do indywidualnych potrzeb i możliwości. Taki system sprzyja elastyczności, ułatwiając łączenie pracy z nauką, a także zwiększa dostępność edukacji dla osób z regionów defaworyzowanych lub o ograniczonym dostępie do tradycyjnych form kształcenia. Dodatkowo, rozwój zharmonizowanych programów certyfikacyjnych może znacząco przyczynić się do zmniejszenia barier wejścia na rynek pracy. Przejrzystość i uznawalność kwalifikacji na poziomie europejskim pozwolą pracodawcom szybciej ocenić kompetencje kandydatów, a osobom uczącym się – łatwiej dopasować się do wymagań rynku. Inwestowanie w takie rozwiązania wspiera także inkluzywność, umożliwiając większej liczbie ludzi rozwój w branży IT i cyberbezpieczeństwa, co w dłuższej perspektywie może przyczynić się do zmniejszenia deficytu specjalistów w tych dziedzinach. Ostatecznie, działania te powinny być częścią szerszej strategii, obejmującej nie tylko wprowadzenie certyfikacji, ale także promowanie współpracy międzynarodowej, wspieranie innowacyjnych metod kształcenia oraz budowanie społecznej świadomości znaczenia kompetencji cyfrowych dla przyszłości rynku pracy.

TEMAT II:

Mapowanie luki w umiejętnościach cyberbezpieczeństwa

Mapowanie luki w kompetencjach cyberbezpieczeństwa polega na identyfikowaniu obszarów, w których brakuje odpowiednich umiejętności, aby sprostać intensywnie rozwijającej się cyfrowej rzeczywistości. W obliczu dynamicznego rozwoju technologii i szybko zmieniającego się środowiska cyfrowego, kluczowe jest podejmowanie działań mających na celu zrozumienie krytycznych obszarów deficytu. Skuteczne mapowanie pozwala ocenić skalę problemów i wyznaczyć kroki niezbędne do ich rozwiązania, wspierając rozwój kadr oraz zwiększając odporność cyfrową organizacji i społeczeństwa.

WYZWANIA I REKOMENDACJE

WYZWANIA

Branża cyberbezpieczeństwa stoi w obliczu licznych wyzwań wynikających z niedoboru wykwalifikowanych kadr. Zapotrzebowanie na ekspertów posiadających umiejętności techniczne, takie jak zabezpieczanie chmury, ochrona systemów informacyjnych i sieci, zapewnienie prywatności danych, analiza zagrożeń czy zarządzanie incydentami, znacząco wzrasta. Kluczowe stanowiska, które wymagają odpowiednich kwalifikacji to Chief Information and Security Officer (CISO), Cybersecurity Implementer oraz Cyber Incident Responder.

Wiele firm zmaga się z koniecznością budowy działów cyberbezpieczeństwa od podstaw, co utrudnia ograniczona liczba wykwalifikowanych ekspertów, szczególnie w obszarach takich jak reagowanie na incydenty, identyfikowanie zagrożeń czy testowanie bezpieczeństwa systemów. Dodatkowym wyzwaniem jest niedobór techników i specjalistów średniego szczebla, co wskazuje na potrzebę poszerzenia możliwości kształcenia poza tradycyjne uczelnie wyższe.

Obecny system edukacji nie nadąża za rosnącymi potrzebami branży, co wymaga zróżnicowanego podejścia do rozwoju kompetencji, obejmującego szkolenia zawodowe i programy praktyczne. Brak takich inicjatyw skutkuje opóźnieniami w przygotowaniu specjalistów do pracy w dynamicznym i wymagającym środowisku cyberbezpieczeństwa.

REKOMENDACJE

1. Regularna identyfikacja kluczowych obszarów kompetencyjnych w zakresie cyberbezpieczeństwa jest niezbędna. Powinna opierać się na współpracy z sektorem prywatnym, instytucjami edukacyjnymi oraz ekspertami branżowymi, aby uwzględniać zarówno aktualne potrzeby, jak i nadchodzące trendy technologiczne.

2. Skuteczne mierzenie luki w umiejętnościach powinno opierać się na analizie obecnego i przyszłego zapotrzebowania na role, kompetencje, umiejętności i wiedzę zakresie cyberbezpieczeństwa, a także obecnej podaży programów edukacyjnych i szkoleniowych w tym zakresie. Społeczeństwo powinno być bardziej świadome obecnej i prognozowanej liczby specjalistów ds. Cyberbezpieczeństwa, a także niezapełnionych wakatów w tym obszarze.

3. Badania i raportowanie dotyczące identyfikacji kluczowych obszarów kompetencyjnych powinny być systematyczne, aby na bieżąco monitorować luki w umiejętnościach cyfrowych i skutecznie reagować na pojawiające się wyzwania oraz dynamicznie zmieniające się potrzeby rynku pracy.

4. Rekomendujemy utworzenie centralnego punktu informacyjnego w ramach działalności istniejących instytucji na poziomie krajowym (np. NCC) i/lub unijnym (np. ENISA), który dostarczałby informacji o najnowszych trendach w cyberbezpieczeństwie oraz zapewniał wskazówki ekspertów dotyczące skutecznych sposobów reagowania na nie. Kluczowe jest także wzmocnienie widoczności działań podejmowanych przez te instytucje na poziomie krajowym, dzięki czemu eksperci oraz społeczeństwo otrzymają kompleksową informację na temat sytuacji rynkowej w obszarze możliwości zatrudnienia.

5. Pracodawcy powinni aktywnie oraz regularnie przekazywać informacje o swoich potrzebach kadrowych i angażować się we współpracę z uczelniami, szkołami oraz innymi placówkami edukacyjnymi. Wspólne opracowywanie oraz aktualizacja programów nauczania pomoże dostosować kształcenie do dynamicznie zmieniających się wymagań rynku pracy. Sporządzanie raportów z takich działań pozwoli na skuteczniejsze zarządzanie i optymalizację procesów edukacyjnych.

6. Zapewnienie finansowania organizacjom NGO umożliwi im rozwijanie programów szkoleń dla specjalistów i pracowników w zakresie cyberbezpieczeństwa. Dzięki temu możliwe będzie zwiększenie dostępności rzetelnych kursów praktycznych oraz certyfikacji, a to pomoże w niwelowaniu niedoborów kadrowych w sektorze.

7. Sektor publiczny powinien intensywnie rozwijać współpracę z przedsiębiorstwami i instytucjami edukacyjnymi w celu podniesienia jakości kształcenia, zwłaszcza na poziomie szkolnym. Partnerstwa te mogą wspierać wdrażanie nowoczesnych metod nauczania informatyki i cyberbezpieczeństwa. Oraz pozwalać na dynamiczne dostosowanie treści szkoleń do potrzeb gospodarki cyfrowej.

8. Poszerzenie dostępu do stanowisk dla początkujących oraz tworzenie praktyk i staży ukierunkowanych na zdobywanie praktycznego doświadczenia może zaktywizować grupy niedostatecznie reprezentowane w branży, takie jak kobiety, osoby z niepełnosprawnościami czy imigranci. Programy te są bardziej elastyczne dla osób z różnymi zobowiązaniami.

TEMAT III:

Szkolenia w dziedzinie cyberbezpieczeństwa

Szkolenia w dziedzinie cyberbezpieczeństwa nabierają coraz większego znaczenia, jednak ich obecny poziom ujawnia poważne wyzwania. Brak odpowiedniej edukacji cyfrowej od wczesnych etapów nauczania skutkuje niską świadomością społeczną i ograniczonymi umiejętnościami w zakresie bezpiecznego poruszania się w cyberprzestrzeni. Dodatkowo, tradycyjne metody nauczania nie nadążają za dynamicznie rozwijającym się światem cyfrowym, co prowadzi do powstawania luki kompetencyjnej. Problem pogłębia ograniczony dostęp do szkoleń w mniej rozwiniętych regionach oraz powszechny opór wobec edukacji cyfrowej, który utrudnia przygotowanie społeczeństwa na wyzwania współczesnej technologii.

WYZWANIA I REKOMENDACJE

WYZWANIA

Brak odpowiednich programów nauczania i znaczące luki w edukacji stanowią główną przeszkodę w kształtowaniu niezbędnych kompetencji cyfrowych w społeczeństwie. Fundamentalne braki wynikają z niewłaściwego nauczania – młodzież nie rozumie podstawowych zasad funkcjonowania cyberprzestrzeni, co skutkuje niską świadomością w zakresie bezpiecznego poruszania się w środowisku cyfrowym. Niedostateczne wprowadzenie edukacji cyfrowej na wczesnych etapach edukacji prowadzi do trudności w adaptacji do współczesnego świata opartego na technologii.

Ponadto, problemem jest opór wobec wdrażania nowoczesnych metod nauczania, co potęguje trudności w zainteresowaniu młodego pokolenia i motywowaniu go do samodzielnego poszerzenia wiedzy. Tradycyjne podejście, bazujące na teoretycznym przekazie informacji, nie spełnia oczekiwań młodzieży preferującej interaktywną i praktyczną formę nauki. Co więcej, ograniczony dostęp do specjalistycznych szkoleń w mniej rozwiniętych regionach pogłębia nierówności w kompetencjach cyfrowych, utrudniając rozwój zawodowy i możliwości konkurowania na rynku pracy. Projektowanie efektywnych programów edukacyjnych w dziedzinie cyberbezpieczeństwa staje się coraz większym wyzwaniem, ze względu na dynamiczny rozwój technologii. Tempo cyfryzacji wyprzedza rozwój zorganizowanej wiedzy eksperckiej, co wymaga szybkiej adaptacji w obszarze edukacji. Tworzenie skutecznych programów wymaga uwzględnienia zmieniającego się charakteru branży oraz współpracy między różnymi sektorami. Tylko w ten sposób można dostosować treści edukacyjne do realnych potrzeb rynku i sprostać wymaganiom nowoczesnej gospodarki cyfrowej.

REKOMENDACJE

1. Edukację w zakresie bezpieczeństwa w Internecie należy rozpoczynać już w szkołach podstawowych, ucząc dzieci rozpoznawania dezinformacji i krytycznego myślenia w sieci, tłumacząc, że nie wszystko, na co natkną się w Internecie i mediach społecznościowych jest prawdą. Należy opracować jednolite minimum programowe, które zapewni każdemu podstawową wiedzę o bezpiecznym korzystaniu z cyberprzestrzeni oraz umożliwi zrozumienie i praktyczne wykorzystanie nowoczesnych technologii cyfrowych.

2. Szkolenia z cyberbezpieczeństwa muszą być elastyczne i zaprojektowane z myślą o regularnym odświeżaniu, aby uwzględnić dynamiczne zmiany w zagrożeniach i narzędziach cyfrowych. Opracowywanie tych programów powinno odbywać się we współpracy z ekspertami branżowymi oraz sektorem prywatnym, co pozwoli dostarczać najbardziej aktualną wiedzę w przystępny sposób. Ważne jest, aby kursy te były szeroko dostępne i o ile to możliwe, darmowe.

3. Materiały edukacyjne muszą być przystosowane do różnych grup społecznych, z użyciem prostego języka i intuicyjnych narzędzi, aby umożliwić przyswajanie wiedzy zarówno początkującym, jak i zaawansowanym użytkownikom technologii oraz wyeliminowaniem barier wejścia.

4. Wprowadzenie międzypokoleniowych warsztatów, które zwiększają świadomość na temat dezinformacji i bezpieczeństwa w sieci, to przykład działań, które mogą skutecznie wspierać edukację i jednocześnie wzmacniać więzi społeczne.

5. Ze względu na występujący opór wobec edukacji cyfrowej, kluczowe jest wykorzystanie nowoczesnych form edukacji, które wzbudzą zainteresowanie i zaangażowanie uczestników. Szczególnie rekomendujemy wprowadzenie gier edukacyjnych, które łączą elementy rozrywki z nauką i służą rozwijaniu konkretnych umiejętności oraz przekazywaniu wiedzy w realistycznym, interaktywnym kontekście i gamifikacji ścieżek edukacyjnych. Popularyzacja takiej metody dydaktycznej, która bazuje na elementach interakcji uczyni proces nauki bardziej angażującym i motywującym, a jednocześnie przystępnym dla szerokiego grona odbiorców.

6. Symulacje scenariuszy związanych z zagrożeniami cybernetycznymi, wzbogacone o praktyczne ćwiczenia i realistyczne przykłady, mogą znacząco zwiększyć skuteczność programów szkoleniowych, przygotowując uczestników do radzenia sobie z rzeczywistymi wyzwaniami w cyberprzestrzeni. Uczniowie powinni mieć możliwość rozwiązywania rzeczywistych problemów związanych z cyberzagrożeniami, takich jak zarządzanie incydentami cybernetycznymi czy analiza dezinformacji. Ćwiczenia te rozwijają zarówno kompetencje techniczne jak i zdolność współpracy oraz analitycznego myślenia.

7. Interaktywne zajęcia praktyczne, takie jak warsztaty czy laboratoria, są nieodzowne, aby efektywnie zaangażować młodzież i umożliwić naukę przez doświadczenie.

8. Jednocześnie należy podkreślać znaczenie umiejętności miękkich, obejmujących zagadnienia prawne, polityczne i etyczne, aby jednoznacznie zaznaczyć, że ochrona w sieci to nie tylko kwestie techniczne, ale także świadomość odpowiedzialności społecznej.

9. Rozwój interaktywnych platform oferujących kursy i innowacyjne narzędzia może pomóc w niwelowaniu braków w umiejętnościach cyfrowych, przygotowując młode pokolenie do wyzwań współczesnej cyfrowej rzeczywistości.

10. Firmy i instytucje powinny aktywnie wspierać edukację cyfrową, współtworząc programy szkoleniowe i promując idee odpowiedzialnego obywatelstwa cyfrowego. Kluczowe jest wykształcenie „E-Obywatela", zdolnego do funkcjonowania w coraz bardziej zdigitalizowanej rzeczywistości.

TEMAT IV:

Praktyki cyberhigieny i bieżące wyzwania

Cyberhigiena, czyli zestaw praktyk mających na celu bezpieczne korzystanie z technologii cyfrowych, staje się nieodzownym elementem współczesnego życia. Dynamiczny rozwój technologii i rosnące zagrożenia w cyberprzestrzeni uwidaczniają brak wystarczającej wiedzy w zakresie podstawowego cyfrowego BHP zarówno wśród pracowników, jak i ogółu społeczeństwa. Problem pogłębia brak regulacji prawnych, nieadekwatne podejście do szkoleń oraz niewystarczająca współpraca między sektorami. Pandemia COVID-19 i zastosowanie systemu pracy zdalnej znacząco uwypukliły te braki, zwiększając podatność organizacji i użytkowników na cyberzagrożenia. W kontekście coraz bardziej cyfrowego świata rozwój i wdrażanie skutecznych praktyk cyberhigieny jest kluczowe dla zapewnienia bezpieczeństwa zarówno na poziomie indywidualnym, jak i organizacyjnym.

WYZWANIA I REKOMENDACJE

WYZWANIA

Państwo odgrywa kluczową rolę w promowaniu i egzekwowaniu zasad cyberhigieny, ponieważ ma możliwość wprowadzania regulacji, które mogą uczynić ją integralną częścią codziennego życia społeczeństwa. Brak takich przepisów sprawia, że cyberhigiena nie jest traktowana priorytetowo, co prowadzi do obniżenia poziomu cyberodporności społecznej. Podejście do szkoleń w zakresie cyberhigieny wymaga zmiany, polegającej na zintensyfikowanej współpracy międzysektorowej. Współpraca pomaga ekspertom i prowadzącym w dostosowaniu programu do nowych zagrożeń i wymagań rynku pracy. Brak dostosowania szkoleń do rozwoju technologii może doprowadzić do niewystarczającego przygotowania społeczeństwa na nowe zagrożenia. Brak aktualizacji zakresu szkoleń może również spowodować brak zainteresowania, obniżając ich efektywność. Ewaluacja efektywności szkoleń jest niezbędna i pozwala na wprowadzanie potrzebnych modyfikacji, aby wspierać rozwój cyberhigieny.

Inicjatywy edukacyjne mogą wspierać rozwój cyberhigieny, umożliwiając dostęp do szkoleń. Przykładem takich działań jest GCA (Global Cyber Alliance), które opracowało zestawy narzędzi cyberbezpieczeństwa, eliminując bariery finansowe i umożliwiając dostęp do podstawowych narzędzi ochrony dla małych i średnich przedsiębiorstw, organizacji non-profit oraz użytkowników indywidualnych. Inną istotną inicjatywą jest Cyberpeace Builders Instytutu Cyberpeace, która usuwa barierę umiejętności w zakresie pomocy technicznej, oferując wsparcie technologiczne dla organizacji wrażliwych, takich jak szpitale czy organizacje humanitarne.

Pandemia COVID-19 zmieniła model pracy, zmuszając organizacje na całym świecie do szybkiego przystosowania się do systemu pracy zdalnej. Znaczna część pracowników rozpoczęła pracę poza biurem. Ten model przyniósł wiele korzyści dla jednostek, jednak przynosi także nowe wyzwania związane z bezpieczeństwem cyfrowym. Widoczny jest wyraźny niedobór podstawowej wiedzy w zakresie cyfrowego BHP i umiejętności praktycznych, takich jak rozumienie struktury danych czy zasady bezpiecznego udostępniania informacji.

REKOMENDACJE

1. Należy promować wiedzę na temat dostępnych szkoleń z zakresu cyberhigieny oraz ułatwić ich dostępność. Narzędzia cyfrowe, takie jak aplikacja M-Obywatel, mogą być efektywnym kanałem informacyjnym, przypominającym o szkoleniach, wydarzeniach i zasobach edukacyjnych. Kampanie informacyjne powinny podkreślać korzyści wynikające z podnoszenia kompetencji w zakresie bezpieczeństwa cyfrowego.

2. Praktyki związane z cyberhigieną powinny być ujęte w przepisach prawa i wdrażane jako standard w ramach obowiązków podmiotów należących do Krajowego Systemu Cyberbezpieczeństwa (KSC). Wprowadzenie regulacji wymagających systematycznych szkoleń z zakresu bezpieczeństwa cyfrowego dla kluczowych sektorów gospodarki jest niezbędne.

3. Szkolenia z cyberhigieny powinny być łatwo dostępne, bezpłatne i obejmować różnorodne poziomy zaawansowania – od podstawowych kursów dla początkujących po zaawansowane programy dla specjalistów IT. Cyfrowe rozwiązania, takie jak platformy e-learningowe, aplikacje mobilne i portale informacyjne, mogą znacząco zwiększyć dostęp do edukacji, wspierając rozwój kompetencji cyberbezpieczeństwa w szerokim zakresie społecznym.

4. Edukacja w zakresie cyberhigieny powinna być prowadzona systematycznie i stale dostosowywana do nowych wyzwań oraz zmieniających się zagrożeń cyfrowych. Treści edukacyjne muszą być stale weryfikowane i aktualizowane, co zapewni ich adekwatność do aktualnej sytuacji. Takie podejście nie tylko zwiększa świadomość społeczeństwa, ale również przyczynia się do budowy odporności na cyberzagrożenia, które stają się coraz bardziej powszechne.

5. Potrzebne jest zintegrowane podejście, które obejmuje zarówno wprowadzenie programów edukacyjnych w szkołach jak i uproszczenie narzędzi oraz praktyk dla użytkowników końcowych. Pracodawcy powinni być zobowiązani ustawowo do organizacji szkoleń, które uwzględniają cyberhigienę i cyfrowe zasady bezpieczeństwa i higieny pracy. W konsekwencji przyczyni się to do zwiększenia odporności organizacji na cyberzagrożenia oraz zniweluje niepożądane skutki prawne i finansowe wynikające chociażby z utraty danych czy atakiem na serwer. Organizacje pozarządowe zajmujące się cyberbezpieczeństwem mogą odgrywać kluczową rolę w opracowaniu materiałów dostosowanych do specyficznych potrzeb różnych grup odbiorców. Szkolenia te powinny być krótkie, ale prowadzone cyklicznie, co ułatwia ich przyswajanie.

6. Dodatkowo, istotne jest wprowadzenie mechanizmów oceny skuteczności działań edukacyjnych w obszarze cyberhigieny. Analiza wyników umożliwi wprowadzanie usprawnień w programach szkoleniowych, co zwiększy ich efektywność.

7. Państwo i organizacje powinny opracować standardowe zasady bezpieczeństwa cyfrowego oraz cyfrowych zasad bezpieczeństwa i higieny pracy, obejmujące zarówno uniwersalne wytyczne, jak i szczegółowe zalecenia dla określonych stanowisk. Obowiązkowe szkolenia oraz testy oparte na praktycznych przykładach powinny być przeprowadzane corocznie. Jak pokazuje doświadczenie Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, takie działania skutecznie podnoszą odporność organizacji nawet o 30%.

TEMAT V:

Współpraca międzysektorowa

Współpraca międzysektorowa odgrywa kluczową rolę w budowaniu odporności na zagrożenia cybernetyczne oraz w rozwoju kompetencji niezbędnych w cyfrowym świecie. Dynamiczne tempo rozwoju technologii wymaga zaangażowania sektora publicznego, prywatnego, edukacyjnego oraz organizacji pozarządowych w tworzenie spójnych strategii i programów, które odpowiadają na bieżące potrzeby rynku. Partnerstwa publiczno-prywatne oraz współpraca z samorządami umożliwiają lepsze wykorzystanie zasobów, wspierają innowacyjne inicjatywy edukacyjne i szkoleniowe oraz pomagają eliminować luki kompetencyjne w społeczeństwie. Efektywne partnerstwa nie tylko zwiększają poziom cyberbezpieczeństwa, ale także wspierają rozwój lokalnych społeczności i ich zdolność do adaptacji w obliczu szybko zmieniających się wyzwań cyfrowych.

WYZWANIA I REKOMENDACJE

WYZWANIA

Budowanie odpornego społeczeństwa wymaga zaangażowania zarówno sektora publicznego, jak i prywatnego w tworzenie spójnych strategii rozwoju kompetencji. Partnerstwa publiczno-prywatne (PPP) okazały się skutecznym modelem takiej współpracy, który można wykorzystać do zwiększenia efektywności programów szkoleniowych i odgrywają istotną rolę w rozwoju kompetencji. Współpraca między różnymi interesariuszami umożliwia lepsze wykorzystanie zasobów i identyfikację specyficznych wymagań związanych z cyberbezpieczeństwem. Partnerstwa te pozwalają na wdrożenie innowacyjnych inicjatyw, takich jak międzypokoleniowe warsztaty czy specjalistyczne programy dla różnych grup społecznych, wspierając rozwój kompetencji w odpowiedzi na szybko zmieniające się środowisko technologiczne.

Instytucje edukacyjne jako liderzy wiedzy, mogą być świadome międzynarodowych badań i trendów, co pozwala im projektować programy nauczania dostosowane do aktualnych wymagań rynku pracy. Jednocześnie, dzięki ścisłej współpracy instytucje edukacyjne i przemysł mogą przewidywać potrzeby i dostosowywać programy szkoleniowe. Partnerstwa te mogą odegrać kluczową rolę w tworzeniu efektywnych programów szkoleniowych w zakresie cyberbezpieczeństwa, zwłaszcza poprzez zaangażowanie różnych grup społecznych oraz instytucji na wszystkich poziomach. Przemysł, instytucje edukacyjne oraz instytucje publiczne odgrywają kluczowe, komplementarne role w identyfikowaniu i zaspokajaniu specyficznych potrzeb związanych z umiejętnościami w cyberbezpieczeństwie. Firmy prywatne pełnią również rolę informacyjną, dostarczając danych o potrzebach rynkowych i technologicznych, co pozwala na bieżące dostosowywanie programów nauczania. Organizacja staży i praktyk przez firmy umożliwiają weryfikację nabytych kompetencji oraz wskazanie braków wymagających uzupełnienia, a także wspiera certyfikacje i szkolenia wewnętrzne. Także współpraca z samorządami, które mogą promować edukację w zakresie cyberbezpieczeństwa, stanowi istotny krok w eliminowaniu luki kompetencyjnej w społeczeństwie. Dzięki temu możliwe będzie efektywne dostosowanie do wyzwań współczesnego świata.

REKOMENDACJE

1. Wprowadzenie platform współpracy umożliwiających firmom przekazywanie informacji zwrotnych ośrodkom akademickim i instytucjom edukacyjnym na temat programów nauczania pozwoli na bieżące dostosowywanie oferty edukacyjnej do wymagań rynku pracy. Wspieranie pętli informacji zwrotnej z przemysłem jest kluczowe, aby programy szkoleniowe w zakresie cyberbezpieczeństwa odzwierciedlały najnowsze zagrożenia i wymagania techniczne. W tym celu należy wprowadzić formalne mechanizmy przekazywania informacji zwrotnych z branży, takie jak udział przedstawicieli sektora prywatnego w radach doradczych instytucji edukacyjnych.

2. Przedsiębiorstwa powinny aktywnie określać swoje bieżące i przyszłe potrzeby, wspierać rozwój kompetencji swoich pracowników oraz promować elastyczne modele edukacyjne, które obejmują zarówno umiejętności techniczne, jak i interpersonalne. Regularne konsultacje dotyczące oczekiwań wobec absolwentów oraz aktualizacja treści programów nauczania to podstawa dostosowania kształcenia do rzeczywistych wyzwań.

3. Partnerstwa publiczno-prywatne (PPP) powinny koncentrować się na oddziaływaniu i zaspokajaniu potrzeb w zakresie umiejętności, z wymiernymi wskaźnikami. Fundacje, organizacje pozarządowe oraz instytucje państwowe mogą wspólnie prowadzić programy edukacyjne i szkoleniowe, dostosowane do potrzeb różnych grup, takich jak seniorzy, dzieci czy osoby z niskim poziomem umiejętności cyfrowych.

4. Istotne jest opracowanie spójnego systemu kształcenia, który umożliwi ciągłe aktualizowanie wiedzy i umiejętności, uwzględniając szybkie tempo rozwoju technologicznego. Priorytetem powinno być wprowadzenie programów nauczania, które rozwijają krytyczne myślenie, analizę danych oraz ocenę ryzyka.

5. Partnerstwa publiczno-prywatne mogą także wspierać budowę lokalnych inicjatyw i struktur cyberbezpieczeństwa, szczególnie poprzez współpracę z samorządami. Takie działania pomogą w rozwoju kompetencji w mniej uprzywilejowanych regionach, które często są niedostatecznie uwzględniane w centralnych strategiach edukacyjnych, co sprawi, że programy będą bardziej elastyczne, dostępne i dostosowane do najnowszych trendów technologicznych.

6. Państwo powinno zapewniać strategiczne wsparcie poprzez finansowanie inicjatyw edukacyjnych, tworzenie regulacji sprzyjających współpracy międzysektorowej. Państwo może wpływać na samorządy, aby wymagały tworzenia struktur cyberbezpieczeństwa oraz wspierały lokalne programy edukacyjne. Działania te zapewniają wspólny język i wspólne zrozumienie między zainteresowanymi stronami, wykorzystując ramy i standardy.

7. Jednocześnie kluczowa jest współpraca z samorządami, które mogą inicjować lokalne programy edukacyjne oraz organizować międzypokoleniowe warsztaty i działania angażujące różne grupy społeczne.

8. Granty edukacyjne, fundusze samorządowe czy wsparcie ze środków unijnych mogą znacząco przyczynić się do realizacji projektów szkoleniowych. Jednocześnie uproszczenie procedur aplikacyjnych i ograniczenie biurokracji pozwolą zwiększyć efektywność wykorzystania dostępnych środków.

9. W ramach jednolitego wdrażania działań edukacyjnych na rzecz kompetencji cyfrowych istotną rolę pełnią skoordynowane inicjatywy wspierające realizację zadań instytucji takich jak ECCC czy ENISA na poziomach krajowych państw UE. Ministerstwo Cyfryzacji powinno rozważyć utworzenie skoordynowanej sieci ośrodków o charakterze informacyjno-edukacyjnym na poziomie krajowym w 16 województwach, których zadaniem będą działania informacyjne, realizacja kampanii informacyjno-edukacyjnych, wsparcie działań Ministerstwa na poziomie wojewódzkim, realizacja zadań edukacyjnych dla uczniów szkół podstawowych i ponadpodstawowych, seniorów, społeczności lokalnej, realizacja specjalistycznych szkoleń dla uczelni wyższych, a także współpraca z jednostkami samorządowymi w zakresie wdrażania działań rozwijających kompetencje cyfrowe oraz wsparcie samorządów w tworzeniu i realizacji strategii dotyczących sektora cyberbezpieczeństwa. Ośrodki mogłyby pełnić rolę informacyjną wobec Ministerstwa, jednocześnie realizując bieżące i systematyczne działania na rzecz podnoszenia kompetencji cyfrowych, w tym kompetencji związanych z cyberbezpieczeństwem i identyfikacją dezinformacji. Inicjatywa byłaby realnym wyrazem współpracy między jednostkami administracji oraz NGO. Zakres działalności ośrodków byłby aktualizowany na corocznych konsultacjach ewaluacyjnych z przedstawicielami sektora prywatnego, co pozwoli na dostosowanie oferty edukacyjnej, a także stworzy realną podstawę do systemowego włączenia edukacji cyfrowej w proces nauczania. Implementacja podobnych rozwiązań w warunkach krajowych państw członkowskich przyczyni się do skutecznego ustalenia i bezpośredniego wdrożenia jednolitych norm kompetencji cyfrowych.

10. Przedsiębiorstwa powinny aktywnie oferować miejsca pracy dla osób dopiero wchodzących na

rynek pracy, co umożliwi rozwój ich umiejętności i zapewni odpowiedź na zapotrzebowanie branży na wykwalifikowaną kadrę.

11. Partnerstwa powinny opierać się na mierzalnych celach, które będą uwzględniały elastyczność i zdolność do adaptacji wobec nowych wyzwań. W miarę jak zmienia się krajobraz technologiczny, należy regularnie aktualizować strategie działania i długoterminowe cele.

12. Aby zapewnić trwałość wielopodmiotowych inicjatyw szkoleniowych, konieczne jest dokumentowanie doświadczeń i efektów współpracy, co pozwala lepiej zarządzać procesami edukacyjnymi i dostosowywać je do zmieniających się wymagań. Wdrażanie modułowych programów, które można modyfikować w zależności od pojawiających się technologii i zagrożeń, zapewni większą aktualność i skuteczność działań.

Podsumowanie kluczowych rekomendacji

Poniżej zebrano najważniejsze rekomendacje, uporządkowane według priorytetów działań:

1. Wyzwania w cyberbezpieczeństwie:

- Stworzenie katalogu kompetencji cyfrowych obejmującego zarówno umiejętności miękkie, jak i twarde.
- Wczesna edukacja w zakresie krytycznego myślenia i cyfrowego BHP.

2. Mapowanie luki kompetencji:

- Regularna identyfikacja luk kompetencyjnych z udziałem sektora prywatnego.
- Tworzenie centralnych punktów informacyjnych wspierających rynek pracy i edukację.

3. Szkolenia w cyberbezpieczeństwie:

- Elastyczne, praktyczne i regularnie aktualizowane programy szkoleniowe.
- Wprowadzenie gier edukacyjnych i symulacji scenariuszy zagrożeń.

4. Praktyki cyberhigieny:

- Włączenie standardów cyberhigieny do regulacji prawnych i obowiązkowych szkoleń pracowników.
- Stworzenie intuicyjnych narzędzi i aplikacji edukacyjnych.

5. Współpraca międzysektorowa:

- Zacieśnienie współpracy PPP oraz z samorządami w zakresie lokalnych programów edukacyjnych.
- Rozwój sieci informacyjno-edukacyjnych na poziomie regionalnym i krajowym.