

MATERIAŁY UZUPEŁNIAJĄCE

DO PROGRAMU SZKOLENIOWO-DORADCZEGO DLA KADRY JST



CZĘŚĆ 2

MICHAŁ CUPIAŁ
ZOFIA DOMARADZKA-GROCHOWALSKA
DOROTA JASTRZĘBSKA
ANNA PAWEŁAS
DOROTA PINTAL
DOROTA TOMASZEWICZ

MATERIAŁY UZUPEŁNIAJĄCE

DO PROGRAMU SZKOLENIOWO-DORADCZEGO DLA KADRY JST

CZĘŚĆ 2

**Michał Cupiał, Zofia Domaradzka-Grochowalska,
Dorota Jastrzębska, Anna Pawełas, Dorota Pintal, Dorota Tomaszewicz**

Autorzy: **Michał Cupiał, Zofia Domaradzka-Grochowalska, Dorota Jastrzębska, Anna Pawełas, Dorota Pintal, Dorota Tomaszewicz**

Redakcja merytoryczna: **Dorota Pintal, Dorota Tomaszewicz**

Redakcja i korekta: **Renata Faron-Radzka**

Projekt okładki, layout, redakcja techniczna i skład : **Piotr Pękała**

© Copyright for this edition by Ośrodek Rozwoju Edukacji, Warszawa 2025

ISBN 978-83-68584-41-7

Wydanie I

Ośrodek Rozwoju Edukacji

Aleje Ujazdowskie 28

00-478 Warszawa

www.ore.edu.pl

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie Autorstwa – Użycie Niekommercyjne (CC BY-NC)

Publikacja została przygotowana w ramach projektu „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST,” realizowanego w partnerstwie Ośrodka Rozwoju Edukacji ze Związkiem Miast Polskich, współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Plus w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027, Priorytet FERS 01.00, Działanie 01.04 Rozwój systemu edukacji.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



OŚRODEK
ROZWOJU
EDUKACJI

Spis treści

Wstęp	7
Materiał 1. Rola i zadania jednostek samorządu terytorialnego w zakresie cyfryzacji oświaty	11
1. Podstawa prawna określająca działania samorządu w obszarze cyfryzacji oświaty.	11
2. Odpowiedzialność samorządu za realizację zadań oświatowych.	12
3. Nadzór jednostki samorządu terytorialnego jako organu prowadzącego.	13
4. Obowiązek wyodrębnienia przez organ stanowiący środków na doskonalenie zawodowe nauczycieli.	17
5. Bezpieczeństwo informacji jako zadanie jednostek sektora finansów	19
6. Propozycja wskaźników możliwych do wykorzystania w analizie ilościowej.	20
7. Definicja roli i zadań organu prowadzącego w zakresie cyfryzacji oświaty.	26
8. Bibliografia.	29
Materiał 2. Rola i zadania jednostek samorządu terytorialnego w zakresie cyfryzacji oświaty	33
1. Wprowadzenie.	33
2. Zadania JST w zakresie cyfryzacji oświaty.	34
Materiał 3. Planowanie strategiczne JST w obszarze cyfrowego rozwoju oświaty	47
Wprowadzenie	47
1. Kierunki rozwoju cyfryzacji oświaty a wytyczne strategicznych dokumentów europejskich i krajowych.	48
2. Kierunek rozwoju kompetencji przyszłości ze szczególnym uwzględnieniem kompetencji cyfrowych.	60
3. Ramy kompetencji cyfrowych dla obywateli o różnym poziomie zaawansowania. Przykładowe narzędzia do samooceny kompetencji informatycznych w obszarze cyfryzacji oświaty.	68
4. Przykładowe działania wspierające rozwój kompetencji cyfrowych jednostek oświatowych i samorządowych.	75
5. Bibliografia.	78
Materiał 4. Zarządzanie bezpieczeństwem informacji i infrastruktury IT	83
Wprowadzenie.	83

1. Obecna sytuacja w jednostkach samorządu terytorialnego.	84
2. Problematyka zarządzania zasobami IT i cyberbezpieczeństwem w jednostkach samorządu terytorialnego.	86
3. Znaczenie zarządzania bezpieczeństwem informacji.	91
4. Wymagania prawne dla systemu zarządzania bezpieczeństwem informacji.	97
Rozporządzenie określające Krajowe Ramy Interoperacyjności	97
Projekt ustawy o krajowym systemie cyberbezpieczeństwa	102
Rozporządzenie ogólne o ochronie danych osobowych (RODO)	107
5. Zarządzanie infrastrukturą informatyczną w trzech wariantach organizacyjnych	108
Wariant 1: Model w pełni zdecentralizowany	108
Wariant 2: Model hybrydowy z jednostką nadrzędną	113
Wariant 3: Model w pełni scentralizowany	117
6. Porównanie wariantów i sugestie	122
7. Zarządzanie infrastrukturą informatyczną z uwzględnieniem modeli zatrudnienia kadry IT.	123
8. Wdrożenie od podstaw infrastruktury informatycznej w jednostce organizacyjnej.	127
Etap 1: Zabezpieczenie dostępu do sieci publicznej	128
Etap 2: Segmentacja sieci wewnętrznej z wykorzystaniem technologii Virtual Local Area Network (dalej VLAN)	131
Etap 3: Konfiguracja urządzeń sieciowych	133
Etap 4: Konfiguracja urządzeń końcowych	135
Etap 5: Zarządzanie aktualizacjami oprogramowania	138
9. Rola i kompetencje kadry zarządzającej.	141
10. Rola i kompetencje kadry informatycznej.	144
Materiał 5. Rozwiązania wspierające jakościowy rozwój cyfryzacji w edukacji	151
Wprowadzenie.	151
1. Kompetencje przekrojowe i podstawowe jako punkt wyjścia do planowania oraz wdrażania zmian w edukacji.	152
2. Cyberedukacja w centrum uwagi.	157
3. Dobre praktyki w zakresie cyfryzacji w zarządzaniu	

placówkami edukacyjnymi.	160
4. Dobre praktyki w jednostkach oświatowych w zakresie wykorzystania cyfryzacji w edukacji.	164
5. Możliwości i wyzwania dla sztucznej inteligencji w edukacji.	170
6. Inspiracje do organizowania procesu edukacyjnego z wykorzystaniem Zintegrowanej Platformy Edukacyjnej.	176
7. Cyberzagrożenia w edukacji.	180
8. Bibliografia.	183
Materiał 6. Zarządzanie cyfryzacją w oświacie w kontekście wyzwań psychospołecznych	
Wprowadzenie	187
1. Funkcja cyfryzacji w oświacie.	188
2. Transformacja cyfrowa a transformacja myślenia.	190
3. Identyfikacja i analiza głównych wyzwań psychospołecznych wyzwań w procesie zarządzania cyfryzacją w oświacie.	193
4. Modele zarządzania cyfryzacją w oświacie wobec transformacji myślenia o współczesnej edukacji.	215
5. Identyfikacja sieci powiązań i odpowiedzialności w kontekście pożądaných kierunków zmiany w edukacji.	219
6. Związek między kompetencjami osób zarządzających jednostkami edukacyjnymi a przebiegiem procesu cyfryzacji.	222
7. Związek między zjawiskiem higieny cyfrowej i dojrzałości cyfrowej.	226
8. Rola profilaktyki i psychoedukacji w świecie rzeczywistym i wirtualnym.	230
9. Związek między kompetencjami osób zarządzających w oświacie a kształtowaniem postaw u dzieci oraz młodzieży.	233
10. Wybrane metody i narzędzia wspierające proces cyfryzacji.	237
11. Bibliografia.	244
Arkusze diagnostyczne do badania stanu cyfryzacji oświaty w jednostkach samorządu terytorialnego	
1. Arkusz do diagnozy wstępnej. Część 1.	248
2. Arkusz do diagnozy wstępnej. Część 2.	251

3. Arkusz do diagnozy wstępnej. Część 3.	261
4. Wzór Harmonogramu Działań Rozwojowych (dalej HDR).....	264
Słownik pojęć	267

WSTĘP



Cyfryzacja oświaty jest zarówno jednym z kluczowych wyzwań, jak i ogromną szansą rozwojową edukacji.

W obliczu dynamicznego postępu technologicznego szkoła lub inna placówka oświatowa nie mogą pozostawać instytucjami wyłącznie zakorzenionymi w tradycyjnych metodach nauczania. Współczesny uczeń funkcjonuje w świecie zdominowanym przez technologię cyfrową, która wyznacza ramy komunikacji, pracy, uczestnictwa w kulturze i życiu społecznym. Oznacza to, że edukacja, chcąc sprostać oczekiwaniom młodego pokolenia oraz przygotować je do wyzwań przyszłości, musi w pełni korzystać z potencjału narzędzi cyfrowych.

Proces ten nie jest jednak nieskomplikowaną modernizacją techniczną skupiającą się wyłącznie na dostarczeniu komputerów czy zapewnieniu dostępu do internetu. Ten mechanizm wymaga całościowej i strategicznej wizji rozwoju, w której technologie traktuje się nie jako cel sam w sobie, ale jako narzędzia wspierające realizację działań edukacyjnych. Cyfrowa transformacja oznacza zatem nie tylko modernizację infrastruktury, ale także rozwój kompetencji nauczycieli, zmianę metod dydaktycznych, wdrażanie nowych modeli zarządzania oświatą oraz podnoszenie świadomości w zakresie cyberbezpieczeństwa. W tym procesie szczególną rolę odgrywają jednostki samorządu terytorialnego (dalej JST), będące organami prowadzącymi dla szkół, przedszkoli i placówek edukacyjnych. To właśnie od decyzji organów samorządowych, które dotyczą alokacji środków, planowania inwestycji czy wyboru priorytetów rozwojowych, zależy tempo i jakość cyfryzacji edukacji w skali lokalnej.

Wyzwania, z jakimi mierzy się polska oświata w obszarze cyfryzacji, zostały szczególnie wyraźnie uwidocznione w czasie pandemii COVID-19. Zaistniała wówczas sytuacja uwypukliła potrzebę systemowego podejścia do rozwoju edukacji cyfrowej, wskazując

na konieczność diagnozy realnych potrzeb i opracowanie takich rozwiązań, które w przyszłości zwiększyłyby w naszym kraju odporność szkolnictwa na ewentualne wyzwania.

W odpowiedzi na te doświadczenia pojawia się konieczność sformułowania roli i zadań JST w obszarze cyfryzacji oświaty. Zgodnie z obowiązującymi przepisami prawa samorządy odpowiadają za zapewnienie warunków do prowadzenia działalności dydaktycznej, wychowawczej i opiekuńczej. Oznacza to odpowiedzialność JST zarówno za utrzymanie budynków oraz finansowanie bieżącej działalności, jak i inwestowanie w nowoczesną infrastrukturę, wspieranie kompetencji kadry pedagogicznej, zapewnienie bezpiecznego środowiska cyfrowego oraz wprowadzanie rozwiązań ułatwiających zarządzanie edukacją na poziomie lokalnym. Coraz większe znaczenie zyskuje przy tym aspekt bezpieczeństwa informacji nie tylko w zakresie ochrony danych osobowych, ale także odporności systemów informatycznych na zagrożenia zewnętrzne.

Cyfryzacja oświaty – zgodnie z krajowymi i europejskimi dokumentami rozwojowymi – wymaga także strategicznego planowania, które uwzględniałoby cele długofalowe. Jednocześnie każde rozwiązanie wprowadzane na poziomie ogólnopolskim musi być odpowiednio dostosowane i wdrożone w konkretnych warunkach lokalnych (w tym obszarze właśnie ujawnia się znacząca rola samorządów).

Transformacja cyfrowa edukacji nie ogranicza się jednak wyłącznie do aspektów technicznych. Ten proces dotyczy także głębokiej zmiany w sposobie myślenia o nauczaniu i uczeniu się. Zgodnie z tym nauczyciel przestaje być jedynym źródłem wiedzy, a staje się przewodnikiem po świecie informacji, wspierając uczniów w krytycznym myśleniu, selekcji treści i rozwijaniu kompetencji kluczowych (np. umiejętności współpracy, kreatywności czy samodzielności). Technologie cyfrowe stwarzają również ogromne możliwości w zakresie personalizacji nauczania, angażowania uczniów i przygotowywania ich do funkcjonowania w gospodarce opartej na wiedzy.

Nie można przy tym pominąć wyzwań psychospołecznych. Intensywne korzystanie z technologii wiąże się z ryzykiem przeciążenia informacyjnego, uzależnień czy osłabienia relacji społecznych. Dlatego obok inwestycji w infrastrukturę i szkolenia równie niezbędne są także profilaktyka, psychoedukacja oraz kształtowanie postaw odpowiedzialnego korzystania z nowych mediów. Zadaniem samorządów, szkół,

przedszkoli i innych placówek oświatowych jest tworzenie bezpiecznego i sprzyjającego rozwojowi środowiska cyfrowego, które wspiera nie tylko kompetencje techniczne, lecz także dobrostan uczniów i nauczycieli.

Materiały szkoleniowe, które zaprezentowano w niniejszym opracowaniu, stanowią próbę całościowego ujęcia problematyki cyfryzacji oświaty w kontekście zadań jednostek samorządu terytorialnego. Celem jest zarówno wskazanie podstaw prawnych oraz ram organizacyjnych, jak i podzielenie się dobrymi praktykami oraz narzędziami zarządczymi, które mogą być wykorzystane w procesie wdrażania zmian. Opracowanie ma charakter praktyczny, koncentruje się na rozwiązaniach możliwych do zastosowania w realiach lokalnych, a ponadto uwzględnia zarówno kwestie infrastrukturalne, jak i rozwój kompetencji cyfrowych kadr oświaty oraz pracowników administracji.

Cyfrowa transformacja edukacji jest procesem długofalowym i wymagającym współpracy wielu podmiotów, począwszy od organów centralnych, przez samorządy, aż po nauczycieli, uczniów i rodziców. Tylko spójne i systemowe działania mogą wpłynąć na to, że szkoła stanie się przestrzenią otwartą na innowacje, a jednocześnie bezpieczną i przyjazną dla wszystkich uczestników procesu edukacyjnego. W tym sensie niniejsze opracowanie ma służyć jako kompendium wiedzy i inspiracji, które wspiera samorządy w podejmowaniu świadomych, odpowiedzialnych decyzji na rzecz nowoczesnej i jakościowej edukacji cyfrowej.

Materiały uzupełniające do programu szkoleniowo-doradczego dla kadry JST stanowią inspirację do realizacji poszczególnych modułów. Każdy materiał zawiera opracowanie teoretyczne z praktycznymi wskazówkami lub narzędziami możliwymi do zastosowania niezależnie od typu organów samorządowych.

Zagadnienia omawiane w niniejszej publikacji:

- 1) Rola i zadania jednostek samorządu terytorialnego w zakresie cyfryzacji oświaty.
- 2) Rola i zadania jednostek samorządu terytorialnego w zakresie cyfryzacji oświaty – opis obszaru wraz ze wskaźnikami.
- 3) Planowanie strategiczne JST w obszarze cyfrowego rozwoju oświaty.
- 4) Zarządzanie bezpieczeństwem informacji i infrastruktury technologii informacyjnej.
- 5) Rozwiązania wspierające jakościowy rozwój cyfryzacji w edukacji.

- 6) Zarządzanie cyfryzacją w oświacie w kontekście wyzwań psychospołecznych.
- 7) Arkusze diagnostyczne do badania stanu cyfryzacji oświaty w JST oraz harmonogram działań rozwojowych (dalej HDR).

MATERIAŁ 1. ROLA I ZADANIA JEDNOSTEK SAMORZĄDU TERYTORIALNEGO W ZAKRESIE CYFRYZACJI OŚWIATY



Anna Pawełas

1. Podstawa prawna określająca działania samorządu w obszarze cyfryzacji oświaty.

Cyfryzacja oświaty jest bardzo istotnym i niezbędnym środkiem do realizacji nadrzędnego celu edukacyjnego, jakim jest rozwój i dobro ucznia oraz nauczyciela. Zjawisko to obejmuje między innymi (dalej m.in.) rozwój technologii informacyjno-komunikacyjnych (dalej TIK), modernizację infrastruktury oraz wzbogacanie treści i zasobów. Transformacja cyfrowa dotyczy wszystkich obszarów życia, w tym także i edukacji. Wraz z wzrostem wykorzystania nowoczesnych technologii zwiększa się zapotrzebowanie na osoby, które będą potrafiły nie tylko z nich korzystać, ale także wykażą się umiejętnością projektowania, wytwarzania i pracowania z wykorzystaniem tych narzędzi. Znaczenie rozwoju kompetencji cyfrowych od wielu lat podkreślają organizacje międzynarodowe. Sytuację diametralnie zmieniła pandemia COVID-19, która dotknęła praktycznie wszystkich krajów na świecie, wymuszając m.in. zamknięcie szkół, przedszkoli, innych placówek edukacyjnych i przedsiębiorstw, a co za tym idzie – przeniesienie zarówno kształcenia, jak i pracy do przestrzeni wirtualnej. Tempo i zasięg rozprzestrzeniania się wirusa przyspieszyły rewolucję cyfrową w obszarze edukacji.

Niebagatelną rolę w tym zakresie odgrywają JST, które są organami prowadzącymi dla szkół, przedszkoli i innych podmiotów oświatowych. Zgodnie z przepisami prawa organy samorządowe sprawują nadzór nad działalnością szkół, przedszkoli i placówek oświatowych w zakresie spraw finansowych i administracyjnych. Szczególne znaczenie mają decyzje dotyczące alokacji środków budżetowych na zadania i działania będące odpowiedzią na zdiagnozowane potrzeby. Jednym z głównych elementów kompetencji przyszłości są umiejętności cyfrowe obywateli. Celowe kształtowanie tych kompetencji w polskim systemie oświaty wymaga cyfrowego środowiska edukacyjnego, które przyczyniałoby się do rozwoju wskazanych umiejętności wśród mieszkańców naszego kraju. Natomiast optymalne cyfrowe środowisko edukacyjne obejmuje zbiór powiązanych z sobą elementów, które dotyczą infrastruktury cyfrowej szkół, przedszkoli i placówek (w tym ich wyposażenia w niezbędny sprzęt z dostępem do bezpłatnych cyfrowych zasobów i narzędzi edukacyjnych). To zaś dopiero stanowi warunek bazowy do rozwoju kompetencji cyfrowych. Obowiązkiem JTS jako organów prowadzących szkoły lub placówki oświatowe jest zatem strategiczne podejście do całościowego zagadnienia, jakim jest cyfryzacja w oświacie na poziomie lokalnym.

2. Odpowiedzialność samorządu za realizację zadań oświatowych.

Odpowiedzialność samorządu za realizację zadań oświatowych wynika wprost z artykułu (dalej art.) 7 ustęp (dalej ust.) 1 ustawy o samorządzie gminnym oraz art. 4 ust 1 ustawy o samorządzie powiatowym. Z przywołanych przepisów wyłaniają się własne zadania samorządu, do których należy edukacja publiczna w zakresie przewidzianym przez Prawo oświatowe. JST zakładają i prowadzą podmioty oświatowe wymienione w art. 2 Ustawy Prawo oświatowe zgodnie z podziałem wykazany w art. 8 Prawa oświatowego, który dotyczy typów jednostek prowadzonych przez organy samorządowe. Zadania i odpowiedzialność JST wynikają również z celów ogólnych zawartych w obowiązujących w polskim systemie edukacyjnym podstawach programowych, które dotyczą nauki w cyfrowym świecie.

3. Nadzór jednostki samorządu terytorialnego jako organu prowadzącego.

Samorząd jako organ prowadzący – zgodnie z art. 57 i art. 58 ustawy Prawo oświatowe – sprawuje nadzór w zakresie działalności finansowej i administracyjnej nad prowadzonymi szkołami, przedszkolami i placówkami oświatowymi. Zajmuje się kontrolą realizacji środków budżetowych przyznanych danej jednostce oświatowej, a także wykorzystaniem przez nią funduszy pochodzących z innych źródeł. Ponadto samorząd rozlicza szkoły, przedszkola i placówki w zakresie przestrzegania przez nie norm prawnych dotyczących organizacji pracy, a także kontroluje prawidłowość zarządzania posiadanym przez nie mieniem. Ważnym zadaniem tego organu prowadzącego jest również monitorowanie, w jaki sposób podległe mu podmioty przestrzegają obowiązujących przepisów bezpieczeństwa i higieny pracy pracowników oraz uczniów.

Przywołane normy prawne wskazują na szeroki zakres zadań wykonywanych przez samorząd w kwestii nadzoru nad finansami oraz administracją szkół i placówek edukacyjnych.

Doprecyzowanie zadań JST w zakresie sprawowanego nadzoru następuje w art. 10 ustawy Prawo oświatowe. W przytoczonym przepisie ustawodawca nałożył obowiązki na organ prowadzący szkołę, przedszkole lub placówkę, które wynikają z faktu przedmiotowego prowadzenia danego podmiotu. Głównym zadaniem JST jest odpowiedzialność za działalność szkoły, przedszkola lub innego podmiotu oświatowego. Ponadto w dokumencie wskazano katalog czynności, których organ prowadzący – na poziomie otwartym – w szczególności musi dopilnować. Należą do nich¹:

- zapewnienie warunków działania szkoły, przedszkola lub placówki, w tym bezpiecznych i higienicznych warunków nauki;

¹ Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 10 marca 2023 roku, w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo oświatowe (Dziennik Ustaw z 2023 roku pozycja 900), zob. D20230900L.pdf [dostęp, online dn. 2.09.2025].

- wychowanie i opieka, czyli zapewnienie warunków umożliwiających stosowanie specjalnej organizacji nauki i metod pracy dla dzieci i młodzieży objętych kształceniem specjalnym;
- wykonywanie remontów obiektów szkolnych oraz zadań inwestycyjnych w tym zakresie;
- zapewnienie obsługi administracyjnej (w tym prawnej), obsługi finansowej, w tym w zakresie wykonywania czynności, o których mowa w art. 4 ust. 3 pkt 2–6 ustawy z dnia 29 września 1994 roku o rachunkowości (Dziennik Ustaw z 2016 roku pozycja 1047 ze zmianami), i obsługi organizacyjnej szkoły lub placówki;
- wyposażenie szkoły lub placówki w pomoce dydaktyczne i sprzęt niezbędny do pełnej realizacji programów nauczania, programów wychowawczo-profilaktycznych, przeprowadzania egzaminów oraz wykonywania innych zadań statutowych;
- wykonywanie czynności w sprawach z zakresu prawa pracy w stosunku do dyrektora szkoły lub placówki.

Wskazany powyżej przepis doprecyzowuje katalog zadań samorządu wobec podmiotów oświatowych, nad którymi sprawuje nadzór. Ponadto, co sugeruje ustawa o samorządzie powiatowym i gminnym, organ prowadzący może zapewnić szkołom, przedszkolom i placówkom oświatowym wspólną obsługę administracyjno-finansową. Poza tym – zgodnie z zarządzeniem ustawowym o finansach publicznych – samorząd sprawuje nadzór nad gospodarką finansową jednostek oświatowych. Zakres monitorowania finansów szkół i placówek oświatowych obejmuje następujące kwestie²:

- kontrolę zarządczą II poziomu i wynikające z tego uprawnienia (art. 69 ust. 1 pkt 2 ustawy o finansach publicznych);
- określenie ram dla planów finansowych jednostek nadzorowanych i zwrócenie uwagi na właściwą realizację przez nie określonych założeń budżetowych (art. 249 ust. 2 i art. 247 ust. 2 ustawy o finansach publicznych);
- przedstawienie harmonogramu realizacji budżetu, w tym planów finansowych jednostek (art. 249 ust. 6 ustawy o finansach publicznych);
- blokowanie planowanych wydatków w sytuacji zagrożenia realizacji budżetu (art. 260 ust. 1 ustawy o finansach publicznych).

² Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 czerwca 2023 roku w sprawie ogłoszenia jednolitego tekstu ustawy o finansach publicznych (Dziennik Ustaw z 2023 roku pozycja 1270), zob. D20231270L.pdf [dostęp, online dn. 2.09.2025].

Art. 10 ustawy Prawo oświatowe określa wiele zadań stojących przed organem prowadzącym szkołę, przedszkole lub placówkę oświatową. Jednym z obowiązków samorządu jest m.in. konieczność wyposażenia tych podmiotów w pomoce dydaktyczne i sprzęt niezbędny zarówno do realizacji programów nauczania (w tym szczególnie podstawy programowej), programów wychowawczo-profilaktycznych, przeprowadzania egzaminów, wykonywania innych zadań statutowych, jak i realizowania czynności z zakresu prawa pracy w stosunku do dyrektora szkoły lub placówki.

Wśród rozporządzeń ustawowych dotyczących realizacji podstawy programowej w różnych typach szkół warto zwrócić uwagę na dwa z nich:

- Rozporządzenie z dnia 14 lutego 2017 roku **w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej** (Dziennik Ustaw z 2022 roku pozycja 609), które dotyczy szkół tak zwanego (dalej tzw.) nowego typu (8-letnia szkoła podstawowa, branżowa szkoła I stopnia, szkoła specjalna przysposabiająca do pracy, szkoła policealna);
- Rozporządzenie z dnia 30 stycznia 2018 roku **w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia** (Dziennik Ustaw z 2018 roku pozycja 467), które dotyczy szkół tzw. nowego typu (4-letnie liceum ogólnokształcące, 5-letnie technikum, branżowa szkoła II stopnia).

Powyższe akty prawne wskazują na rolę placówek edukacyjnych w kształceniu kompetencji cyfrowych uczniów. Szkoła ma za zadanie stworzyć uczniom warunki do nabywania wiedzy i umiejętności z wykorzystaniem metod i technik wywodzących się z informatyki. Podmioty oświatowe powinny kłaść szczególny nacisk na kształcenie uczniów w zakresie:

- logicznego i algorytmicznego myślenia oraz programowania;
- posługiwania się aplikacjami komputerowymi;
- umiejętności wyszukiwania i wykorzystywania informacji pochodzących z różnych źródeł;
- posługiwania się komputerem i podstawowymi urządzeniami cyfrowymi;

- stosowania umiejętności cyfrowych na zajęciach z różnych przedmiotów (m.in. do pracy nad tekstem, wykonywania obliczeń, przetwarzania informacji i ich prezentowania w rozmaitych formach).

Zadania JST w zakresie cyfryzacji oświaty wynikają również z podstawowych kierunków realizacji polityki oświatowej państwa³ w roku szkolnym 2025/2026. Ich publikacja nastąpiła na podstawie rozporządzenia ustawowego o prawie oświatowym – art. 60 ust. 3 pkt 1 ustawy z dnia 14 grudnia 2016 roku (Dziennik Ustaw z 2023 roku pozycja 900).

W dokumencie z 2023 roku wśród obowiązków nałożonych na samorząd wskazano także konieczność:

- promowania higieny cyfrowej i bezpiecznego poruszania się w sieci;
- rozwijania umiejętności krytycznej analizy informacji dostępnych w internecie;
- poprawnego metodycznie wykorzystywania przez nauczycieli nowoczesnych technologii, w szczególności opartych na sztucznej inteligencji oraz korzystanie z zasobów Zintegrowanej Platformy Edukacyjnej (dalej ZPE).

Natomiast z **art. 29 ustawy Karta Nauczyciela** dla organów prowadzących wynika obowiązek zapewnienia szkole podstawowych warunków do realizacji przez nauczyciela zadań dydaktycznych, wychowawczych i opiekuńczych. Na mocy art. 29 ust. 3 przywołanego dokumentu zostało wydane rozporządzenie⁴, gdzie wskazane zostały minimalne wymagania dla sprzętu komputerowego zarówno ucznia i nauczycieli.

³ Podstawowe kierunki realizacji polityki oświatowej państwa w roku szkolnym 2025/2026 – Ministerstwo Edukacji Narodowej – Portal Gov.pl, zob. Podstawowe kierunki realizacji polityki oświatowej państwa w roku szkolnym 2025/2026 - Ministerstwo Edukacji Narodowej - Portal Gov.pl [dostęp, online dn. 2.09.2025].

⁴ Rozporządzenie Ministra Edukacji Narodowej w sprawie podstawowych warunków niezbędnych do realizacji przez szkoły i nauczycieli zadań dydaktycznych, wychowawczych i opiekuńczych oraz programów nauczania (Dziennik Ustaw z 2024 roku pozycja 9), zob. D20240009.pdf [dostęp, online dn. 2.09.2025].

4. Obowiązek wyodrębnienia przez organ stanowiący środków na doskonalenie zawodowe nauczycieli.

Z art. 70a ustawy Karta Nauczyciela⁵ wynika obowiązek dla organów prowadzących wyodrębnienia 0,8 procent (dalej proc.) środków z przeznaczeniem na doskonalenie zawodowe nauczycieli.

Aktywa wskazane w budżetach – zgodnie z przeprowadzoną diagnozą potrzeb – zostaną zapewnione jednostkom oświatowym z przeznaczeniem na podnoszenie kompetencji nauczycieli. Określenie nieodzownych działań w zakresie doskonalenia zawodowego kadry pedagogicznej danej szkoły, przedszkola i placówki należy do obowiązków dyrektora. W ramach zdiagnozowanych potrzeb osoba ta musi uwzględnić następujące kryteria:

- wyniki nadzoru pedagogicznego (nie tylko z ostatniego roku szkolnego);
- wyniki egzaminu ósmoklasisty, egzaminu zawodowego lub egzaminu maturalnego (w zależności od typu danej szkoły);
- realizację podstawy programowej kształcenia ogólnego lub podstaw programowych kształcenia w zawodach szkolnictwa branżowego;
- wymagania wobec szkół, przedszkoli i placówek, określone przez resort edukacji;
- wnioski nauczycieli o dofinansowanie poszczególnych form doskonalenia;
- szkolenia branżowe (szkoły prowadzące kształcenie zawodowe, placówki kształcenia ustawicznego, centra kształcenia zawodowego).
- wymagania wobec szkół i placówek, określone przez resort edukacji;
- wnioski nauczycieli o dofinansowanie poszczególnych form doskonalenia;
- szkolenia branżowe (szkoły prowadzące kształcenie zawodowe, placówki kształcenia ustawicznego, centra kształcenia zawodowego).

W kolejnym etapie dyrektor szkoły, przedszkola lub placówki wnioskuje do organu prowadzącego o dofinansowanie w następnym roku kalendarzowym doskonalenia

⁵ Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 12 kwietnia 2023 roku w sprawie ogłoszenia jednolitego tekstu ustawy – Karta Nauczyciela (Dziennik Ustaw z 2023 roku pozycja 984 wraz z jednolitym tekstem ustawy z dnia 26 stycznia 1982 roku – Karta Nauczyciela (Dziennik Ustaw z 2021 roku pozycja 1762), zob. D20230984L.pdf [dostęp, online dn. 2.09.2025].

zawodowego nauczycieli. Wnioski przygotowuje dyrektor danej jednostki oświatowej na podstawie zdiagnozowanych uprzednio potrzeb. W bieżącym roku kalendarzowym taką prośbę o dofinansowanie rozwijania kompetencji zawodowych kadry pedagogicznej należy złożyć do samorządu **do dnia 31 października danego roku**.

Organ prowadzący – na podstawie wniosków złożonych przez dyrektora danej szkoły do 31 stycznia – określi plan dofinansowania form doskonalenia zawodowego nauczycieli. Jest on ustalany po przeprowadzeniu procedury określonej w rozporządzeniu Ministerstwa Edukacji Narodowej (dalej MEN) z 23 sierpnia 2019 roku⁶. Plan dofinansowania form doskonalenia zawodowego uwzględnia:

- wnioski dyrektorów szkół;
- wyniki egzaminu ósmoklasisty, egzaminu zawodowego lub egzaminu maturalnego;
- podstawowe kierunki realizacji polityki oświatowej państwa;
- stopień realizacji harmonogramu szkoleń branżowych.

Realizacją założeń finansowania form doskonalenia nauczycieli zajmuje się organ wykonawczy na szczeblu terenowym, którym może być wójt gminy, burmistrz miasta, prezydent miasta, starosta powiatowy, marszałek województwa. Co znalazło potwierdzenie w uzasadnieniu wyroku ogłoszonego przez Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 30 listopada 2021 roku (sygnatura III SA/Łd 679/21), w którym napisano: „W konsekwencji to wykonawczy organ gminy jest właściwy w zakresie podziału środków (...), opracowania planu dofinansowania form doskonalenia zawodowego nauczycieli (...), czy ustalenia maksymalnej kwoty dofinansowania opłat oraz określenia specjalności i form kształcenia (...)”.Warto również pamiętać, że plan dofinansowania form doskonalenia nauczycieli wymaga uwzględnienia opinii związków zawodowych.

W kontekście cyfrowego rozwoju szkoły, przedszkola i jednostki edukacyjnej zadanie dotyczące prawidłowej alokacji środków, które są adekwatne do potrzeb danej placówki oświatowej, ma niezwykle istotne znaczenie.

⁶ Rozporządzenie Ministra Edukacji Narodowej z dnia 23 sierpnia 2019 r. w sprawie dofinansowania doskonalenia zawodowego nauczycieli, szczegółowych celów szkolenia branżowego oraz trybu i warunków kierowania nauczycieli na szkolenia branżowe (Dz. U. z 2023 r. poz. 2628)

5. Bezpieczeństwo informacji jako zadanie jednostek sektora finansów

Zabezpieczenie informacji w oświacie przed nieautoryzowanym dostępem, manipulacją lub kradzieżą jest niezbędne dla ochrony danych uczniów, nauczycieli i personelu szkolnego. Zapewnienie bezpieczeństwa danych edukacyjnych pomaga również w utrzymaniu zaufania społeczności szkolnej, a także w zachowaniu integralności procesów edukacyjnych.

Ponadto dochowanie staranności w tym zakresie wspiera przestrzeganie przepisów prawa dotyczących ochrony danych osobowych. Podstawy prawne dla zabezpieczenia przepływu informacji w oświacie regulują zarówno przepisy krajowe (ustawa o ochronie danych osobowych), jak i przepisy międzynarodowe (w Unii Europejskiej jest to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE; dalej RODO⁷).

Bezpieczeństwo informacji w jednostkach oświatowych wynika z respektowania następujących aspektów:

- **ochrony danych osobowych**⁸ (szkoły, przedszkola i instytucje edukacyjne muszą przestrzegać regulacji dotyczących ochrony danych osobowych, czyli RODO, które określa zasady gromadzenia, przetwarzania i przechowywania danych osobowych);
- **prawa do prywatności** (dostęp do informacji uczniów, nauczycieli i personelu szkolnego musi być ograniczony do osób uprawnionych, aby chronić prywatność każdego zainteresowanego);
- **zasady bezpieczeństwa technologii informatycznych**, dalej IT (wdrażanie odpowiednich środków technicznych i organizacyjnych – w tym zabezpieczenia

⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich informacji oraz uchylenia dyrektywy 95/46/WE/(RODO), zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016_679 z dnia 27 kwietnia (1).pdf [online, dostęp dn. 2.09.2025].

⁸ Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dziennik Ustaw z 2018 roku pozycja 1000), zob. D20181000L.pdf [dostęp, online dn. 2.09.2025].

sieci, zapory ogniowe, systemy antywirusowe i szkolenia z zakresu bezpieczeństwa informatycznego – aby zapobiec naruszeniom bezpieczeństwa danych);

- **zapewnienie ciągłości działania** (planowanie awaryjne i procedury odzyskiwania danych w przypadku incydentów bezpieczeństwa, takich jak cyberatak lub awaria systemu, aby minimalizować zakłócenia w procesie nauczania i uczenia się);
- **edukacja i świadomość** (szkolenie nauczycieli, uczniów i personelu szkolnego w zakresie podstawowych zasad bezpieczeństwa informacji, aby zwiększyć świadomość zagrożeń oraz promowanie odpowiedzialnego korzystania z technologii).

Zadania jednostek administracji publicznej w tym zakresie wynikają również z ust. 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności (dalej KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji w jednostkach sektora finansów publicznych, w tym w JST, wynika bezpośrednio z przepisów prawa. Potwierdzenie zgodności i skuteczności działania systemu zarządzania bezpieczeństwem informacji można uzyskać w wyniku przeprowadzonego audytu wewnętrznego.

6. Propozycja wskaźników możliwych do wykorzystania w analizie ilościowej.

Pandemia COVID-19 oraz konieczność szybkiego uruchomienia zdalnego nauczania sprawiły, że szkoły, przedszkola i placówki musiały poradzić sobie z zaskakującą sytuacją. Nie było czasu, aby w odpowiedni sposób przygotować się do funkcjonowania w rzeczywistości zdeterminowanej przez rozprzestrzeniający się wirus SARS-CoV-2. Dlatego konieczne stało się wprowadzanie rozwiązań doraźnych.

Największym wyzwaniem, przed jakim stanęli nauczyciele, uczniowie, dyrektorzy i organy prowadzące szkoły lub placówki, było przystosowanie form i metod pracy oraz zarządzania jednostkami oświatowymi do nowej sytuacji. Te nadzwyczajne

okoliczności wymagały podejmowania decyzji angażujących środki publiczne. Warunki pandemiczne nie pozwalały zarówno na możliwość stopniowego dostosowania się do zmian, jak i dokonanie ewaluacji – wprowadzanych na bieżąco – rozwiązań organizacyjnych i metodycznych. Dotychczas stosowane środki zaradcze, które polegały na administrowaniu szkolnymi systemami informatycznymi przez nauczycieli informatyki, okazały się nieefektywne (m.in. poprzez wysokie koszty, brak kompetencji do zarządzania urządzeniami sieciowymi oraz danymi w chmurze, przestarzałą strukturę szkolnych sieci). Analizy systemów zarządzania prowadzone przez JST uwidoczniły na poziomie lokalnym wiele różnorodnych wyzwań w zakresie cyfryzacji edukacji. Wśród nich warto wymienić⁹:

- konieczność wyrównywania standardów technologicznych w szkołach, przedszkolach i placówkach oświatowych prowadzonych przez JST, w zakresie sprzętowym (np. konieczność sukcesywnej wymiany sprzętu, uruchamianie nowych serwerowni, doprowadzenie łącz światłowodowych) oraz programowym;
- konieczność wyrównania poziomu umiejętności cyfrowych kadry JST podejmującej decyzje zarządcze w tym zakresie;
- możliwość wdrożenia darmowego oprogramowania dla szkół lub placówek;
- konieczność zabezpieczania danych (bezpieczeństwo danych osobowych, zabezpieczenia software’owe);
- potrzebę scentralizowania zarządzania informatycznego na terenie JST.

Zidentyfikowano także problem związany z brakiem odpowiednich kompetencji kadry wśród pracowników JST. Zauważono również niedobór narzędzi niezbędnych do wdrażania systemowych działań, które mogłyby stanowić odpowiedź na zapotrzebowania wskazane powyżej.

Przywołane potrzeby znalazły odzwierciedlenie w „Diagnozie Technologii Informatyczno-Komunikacyjnych”, która została przeprowadzona przez Fundację EdTech Poland w dniach 1–12 grudnia 2022 roku. Patronat nad tym badaniem objął Instytut Badań Edukacyjnych¹⁰ (dalej IBE). Badanie wykazało niewystarczające wyposażenie polskich szkół w urządzenia sieciowe stwarzające ryzyko m.in. dla możliwości rozwinięcia ciągłych działań edukacyjnych w chmurze w ramach różnych

⁹ Załącznik do uchwały numer 15 Komitetu Monitorującego. Program „Fundusze europejskie dla rozwoju społecznego 2021–2027” z dnia 15 marca 2023 roku, zob. [Zal_do_uchwaly_nr_15_MEiN_Dzialanie_01_04_ORE_pilotaz_15_03_2023.pdf](#) (rozwojspoleczny.gov.pl) [online, dostęp dn. 02.09.2025].

¹⁰ Informacja z badania ankietowego „Diagnoza Technologii Informatyczno-Komunikacyjnych” (Grudzień 2022), Warszawa: Fundacja edTech Poland, patronat Instytut Badań Edukacyjnych, zob. Informacja z badania ankietowego pt. Diagnoza Technologii Informatyczno-Komunikacyjnych - Fundacja EdTech Poland [online, dostęp dn. 2.09.2025].

przedmiotów szkolnych. W częściej niż co drugiej szkole internet dostępny jest tylko dla komputerów mieszczących się w pracowniach informatycznych i pokojach administracji, zaś rzeczywista przepustowość sieci w salach odległych od lokalizacji punktu dostępu jest poniżej 100 megabitów na sekundę (dalej Mb/s) i wymaga modernizacji sieci szkolnej. Zaleca się osiągnięcie referencji dostępności 1 punktu dostępu na 30 użytkowników, czyli na jeden oddział lub salę lekcyjną. Obecnie 1 punkt przypada średnio na 70 użytkowników. Wyposażenie szkół w sprzęt komputerowy jest niewystarczające, co wyraża się nie tylko w jego dostępności, ale także w wieku sprzętu, jego możliwości wykorzystania do pracy zdalnej. Zasadne byłoby uzupełnienie zasobu szkół, przedszkoli i innych jednostek edukacyjnych w sprzęt wysokiej jakości o uniwersalnym zastosowaniu.

Diagnoza wykazała niewystarczające wyposażenie polskich szkół, przedszkoli i placówek w urządzenia sieciowe, które umożliwiałyby możliwość rozwinięcia prowadzenia w chmurze regularnych działań edukacyjnych w ramach różnych przedmiotów szkolnych. Przeprowadzona analiza dowiodła, że niemal w każdej jednostce oświatowej internet jest dostępny tylko w miejscach, w których znajdują się pracownie informatyczne oraz pokoje administracji szkół i placówek. Co ciekawe, rzeczywista przepustowość sieci w pomieszczeniach odległych od lokalizacji punktu dostępu wynosi poniżej 100 Mb/s i wymaga modernizacji sieci szkolnej. Dlatego zaleca się wdrożenie wytycznych dla dostępności sieciowej i osiągnięcie referencji dostępności 1 punktu dostępu do zasobów internetowych na 30 użytkowników (czyli na jeden oddział klasowy / jedną salę lekcyjną). Obecnie 1 punkt przypada średnio na 70 użytkowników.

Wyposażenie szkół w sprzęt komputerowy jest niewystarczające i przestarzałe. Co znacznie utrudnia przystosowanie takich narzędzi do pracy zdalnej. Stąd też rodzi się konieczność, aby podmioty oświatowe były wyposażone w sprzęt komputerowy (w tym w komputery stacjonarne, laptopy, tablety) umożliwiający w pełni wykorzystywać technologie cyfrowe przy realizacji zadań dydaktycznych, wychowawczych i opiekuńczych. Wymagania wobec takich urządzeń są minimalne i określono je w załączniku do przywołanego rozporządzenia.

Tym bardziej więc wydaje się zasadne, aby jednostki oświatowe otrzymały (lub uzupełniły swoje zasoby) sprzęt wysokiej jakości o uniwersalnym zastosowaniu.

„Brak jasno określonych reguł organizacji zdalnego nauczania i ograniczone wsparcie z zewnątrz spowodowało duże obciążenie psychiczne nauczycieli wynikające z presji i oczekiwań społeczeństwa oraz organów zarządzających. Wzrosło też ich obciążenie fizyczne związane z koniecznością dostosowania materiałów edukacyjnych do dostępnych kanałów kształcenia w jak najkrótszym czasie. Jak sugerują wyniki badań¹¹ ponad jednej trzeciej przebadanych szkół nauczyciele sami decydowali z jakich narzędzi korzystają i jak pracują [...]”¹². Opisy i wyniki badań określających związek między deklaracjami dyrektorów szkół i placówek oświatowych na temat wykorzystania narzędzi i platform cyfrowych w okresie pandemii COVID-19 a stanem faktycznym dobitnie ukazują wiele rozbieżności. Doskonale tę sytuację obrazują Tomasz Gajderowicz i Maciej Jakubowski w publikacji „Cyfrowe wyzwania stojące przed polską edukacją”. Autorzy ci przedstawiają najważniejsze wnioski wynikające z przeprowadzonej przez nich analizy¹³:

- „Pandemia COVID-19 ujawniła brak odpowiednich kompetencji nauczycieli i uczniów w zakresie korzystania z narzędzi cyfrowych w edukacji. Wyniki badań pokazują, że rzeczywistość znacznie odbiega od deklaracji dyrektorów szkół sprzed pandemii na temat wykorzystywania platform edukacyjnych. Konieczne jest położenie nacisku na rozwój i ewaluację umiejętności nauczycieli.
- Nierówny dostęp do infrastruktury, bariery techniczne i konieczność współdzielenia sprzętu powodują wzrost luki edukacyjnej na korzyść osób będących w lepszej sytuacji ekonomicznej i z wyższymi umiejętnościami.
- Dostęp do komputera i łącza internetowego jest w Polsce lepszy niż w innych krajach, jednak w nauczaniu w pandemii dostęp może być ograniczony ze względu na konieczność współdzielenia sprzętu. Problemem może być także brak odpowiednich umiejętności cyfrowych rodziców.
- W wyniku zamknięcia placówek edukacyjnych pogorszeniu uległy relacje między uczniami oraz nauczycielem i uczniami.
- Możliwość monitorowania aktywności uczniów jest ograniczona, co ma negatywny wpływ na ich uczestnictwo w zajęciach i spadek zaangażowania.

¹¹ Sobiesiak-Penszko P., Pazderski F., (2020), „Dyrektorzy do zadań specjalnych – prezentacja wyników badania”, Warszawa: Fundacja Orange, zob. Webinarium Edukacja zdalna w szkołach Wyniki badania dyrektorów (lekcjaenter.pl) [dostęp, online dn. 2.09.2025].

¹² Gajderowicz T., Jakubowski M., (2020), „Cyfrowe wyzwania stojące przed polską edukacją”, Warszawa: WNE UW i Evidence Institute, s. 7, zob. PIE-6(2020)_Cyfrowe_wyzwania.indd [online, dostęp dn. 2.09.2025].

¹³ Ibidem, s. 6.

- Nauczanie zdalne wymagało dużego zaangażowania rodziców w edukację dzieci, co częściowo wynikało z przyjętej przez nauczycieli strategii prowadzenia zajęć, sprowadzającej się do zlecania zadań do samodzielnej realizacji.
- Głównym kryterium wyboru narzędzia do prowadzenia zajęć online powinna być jego dostępność, prostota i znajomość zasad korzystania przez uczniów oraz możliwość organizacji zajęć w czasie rzeczywistym wzmacniających interakcję i zaangażowanie uczniów.
- Kompleksowa diagnoza straty edukacyjnej jest niezbędna do skonstruowania programów naprawczych. Konieczne jest też przeprowadzenie wystandaryzowanych badań na dużą skalę.
- Kształcenie zdalne wymaga zmiany metodyki nauczania i metod oceniania uczniów.
- Niezbędne jest przygotowanie planów wprowadzenia hybrydowej formy nauczania uwzględniającej zarówno zajęcia stacjonarne, jak i zdalne”.

Tomasz Gajderowicz i Maciej Jakubowski w swoim raporcie zamieszczają zestawienie liczbowe pozwalające rzetelnie ocenić, jak w okresie pandemii wyglądało przygotowanie i uczestniczenie uczniów oraz nauczycieli w zajęciach online, a także w jaki sposób obie te grupy wykorzystywały narzędzia cyfrowe¹⁴:

- „Tylko 5 proc. nauczycieli określiło swoje przygotowanie do prowadzenia zdalnych zajęć jako bardzo dobre, a około 40 proc. czuło się przygotowanych w stopniu małym lub umiarkowanym.
- Zaledwie 8 proc. uczniów oceniało umiejętności swoich nauczycieli na wysokim poziomie, a 26 proc. oceniało je źle.
- Aż 85 proc. nauczycieli deklarowało brak wcześniejszego doświadczenia w wykorzystaniu narzędzi edukacji zdalnej.
- Tylko 35 proc. polskich piętnastolatków miało dostęp do platformy edukacyjnej w szkole, a jedynie 15 proc. przyznało, że urządzenia cyfrowe były stosowane do nauczania przed pandemią”.

Podczas pandemii COVID-19 organizacja pracy szkół i przedszkoli, zdalne nauczanie i praca w systemie hybrydowym stały się nie lada wyzwaniem. Dlatego istotne jest działanie mające na celu podnoszenie kompetencji zarówno nauczycieli w zakresie technologii informacyjno-komunikacyjnych, jak i pracowników zatrudnionych w urzędach. Równie ważną kwestią stanowi konieczność doposażenia polskich szkół

¹⁴ Ibidem, s. 4–5.

i placówek oświatowych w sprzęt komputerowy dobrej jakości, który pozwoli na wdrożenie centralnych narzędzi i zasobów cyfrowych zarówno do zarządzania, jak i do wykorzystania w nauczaniu.

Wnikliwa analiza przepisów określających zadania i obowiązki JST w zakresie cyfryzacji oświaty w czasie ostatniej pandemii, uwidocznione przy tej okazji problemy polskiej edukacji, a także wnioski zamieszczone w publikacji „Cyfrowe wyzwania stojące przed polską edukacją” podkreślają jedną istotną kwestię. Zwracają uwagę, że decyzje podejmowane przez organy prowadzące szkoły, przedszkola i placówki oświatowe powinny odpowiadać na zidentyfikowane potrzeby oraz trudności związane z cyfrowym rozwojem oświaty w danym samorządzie. Rozpoznanie problemów powinno wynikać z rzetelnie przeprowadzonej diagnozy stanu zastanego w jednostce oświatowej, a następnie wiązać się z inwentaryzacją posiadanego sprzętu, a także weryfikacją posiadanych zasobów. Samorząd – po dokonaniu oceny stanu zastanego w zakresie cyfryzacji (po weryfikacji sprzętu, zasobów i kompetencji) w danej szkole lub placówce – powinien określić swoje cele, a także dokonać alokacji środków budżetowych na zadania i działania niezbędne do osiągnięcia założonego efektu.

Do wskaźników kontroli zarządczej w szkołach, przedszkolach i placówkach oświatowych należą:

- liczba przeprowadzonych audytów w jednostkach oświatowych prowadzonych przez JST;
- liczba doposażonych pracowni w szkołach i placówkach oświatowych;
- liczba wdrożonych narzędzi informatycznych do centralnego zarządzania oświatą;
- liczba przeszkolonych nauczycieli w zakresie TIK;
- liczba przeprowadzonych szkoleń w zakresie wykorzystania technologii TIK w edukacji;
- liczba nauczycieli prowadzących zajęcia przy wykorzystaniu zasobów cyfrowych i narzędzi informatycznych;
- liczba godzin zajęć dydaktycznych prowadzonych z wykorzystaniem zasobów cyfrowych i narzędzi informatycznych;
- liczba komputerów w szkole przypadająca na ucznia.

7. Definicja roli i zadań organu prowadzącego w zakresie cyfryzacji oświaty.

Zarówno odpowiednio przygotowani nauczyciele, nowoczesne wyposażenie szkół, przedszkoli i placówek oświatowych, podstawa programowa, jak i właściwie skonstruowane programy nauczania są czynnikami, które stanowią bazę do kształtowania kompetencji cyfrowych uczniów. Dlatego rola JST w zakresie cyfryzacji oświaty ma istotne znaczenie. Bowiem bez wsparcia lokalnych władz i bez odpowiednich środków finansowych nie uda się skutecznie zrealizować projektu cyfryzacji we wszystkich jednostkach oświatowych.

Współcześnie – wobec zmieniających się nieustannie okoliczności geopolitycznych, społecznych czy zdrowotnych, dzięki różnorodności dostępnych narzędzi technologicznych, obecności nowych sposobów nauczania i konieczności aktualizacji wiedzy nauczycieli – warto uzmysłwić sobie zarówno konieczność rozwijania wszystkich zagadnień związanych z cyfryzacją polskiej edukacji, jak i traktowanie tej kwestii jako całości. Podstawa programowa, system organizacji procesu kształcenia, metodyka nauczania, kompetencje nauczycieli, zasoby sprzętowe i edukacyjne, a także infrastruktura sieciowa szkół, przedszkoli i placówek oświatowych wymagają cyklicznych przeglądów oraz dostosowywania do aktualnych potrzeb w zakresie kształcenia cyfrowej. Samorządy podejmują działania mające na celu doposażenie jednostek oświatowych w sprzęt niezbędny do realizacji procesu edukowania uczniów i nauczycieli w tym zakresie.

Nie ulega wątpliwości, że rozwijanie kompetencji cyfrowych powinno być prowadzone na zajęciach równoległe w połączeniu z kształtowaniem również innych umiejętności (zarówno osobistych, społecznych, obywatelskich, jak i w zakresie uczenia się, przedsiębiorczości, myślenia krytycznego, rozwiązywania problemów oraz pracy zespołowej). W świetle wymogów przepisów prawa kształtują się następujące

zadania JST w zakresie cyfryzacji oświaty, które zostały zdiagnozowane jako obszary wymagające interwencji¹⁵.

Wśród tych zadań można wskazać:

- Wspieranie rozwoju infrastruktury cyfrowej szkół, przedszkoli i placówek oraz wyposażanie ich w niezbędny sprzęt

Cyfryzacja szkół, przedszkoli i placówek oświatowych wymaga doposażenia ich w odpowiedni sprzęt. Z przeprowadzonych diagnoz i badań wynika, że obecny stan, liczba i jakość urządzeń informatycznych w polskich szkołach, przedszkoli i podmiotach edukacyjnych nie są zadowalające. Na skutek dotychczasowych inwestycji, zrealizowanych przede wszystkim w ramach pilotażu programu „Cyfrowa Szkoła”, jedynie około 500 szkół w Polsce jest przygotowanych do pracy w modelu „jeden uczeń na jeden komputer”.

Brak swobodnego dostępu do internetu jest kolejną barierą, która ogranicza postęp cyfryzacji w edukacji. W wielu jednostkach oświatowych problemem jest brak dostępu do odpowiedniej infrastruktury sieciowej. Ograniczenia te sprawiają, że w tych szkołach i placówkach oświatowych zarówno zasoby edukacyjne, jak i metody oraz narzędzia pracy wymagające odpowiednich łączów komunikacyjnych i sieci, nie są w ogóle wykorzystywane lub w dużym stopniu ograniczone.

- Dostarczanie szkołom i placówkom cyfrowych zasobów i narzędzi edukacyjnych

Zaopatrywanie przez JST szkół, przedszkoli i placówek oświatowych w zasoby cyfrowe i narzędzia informatyczne jest niezwykle ważne. Takie działanie bowiem wspiera edukację i podnosi jakość nauczania.

Przykładowe sposoby dostarczania szkołom i placówkom oświatowym przez JST zasobów cyfrowych i narzędzi informatycznych:

- **zakup i dystrybucja sprzętu komputerowego** (JST mogą zakupywać komputery, laptopy, tablety oraz inne urządzenia elektroniczne i dystrybuować je zarówno do szkół, przedszkoli, jak i placówek oświatowych; w ten sposób uczniowie i nauczyciele mają dostęp do sprzętu niezbędnego im do nauki oraz pracy);
- **tworzenie infrastruktury sieciowej** (JST mogą inwestować zarówno w budowę infrastruktury sieciowej, w tym sieci internetowej o wysokiej prędkości, sieci

¹⁵ Załącznik do uchwały numer 15 Komitetu Monitorującego. Program „Fundusze europejskie dla rozwoju społecznego 2021–2027”, Op. cit.

lokalnej w szkołach i placówkach oświatowych, jak i zapewnić dostęp do bezprzewodowego internetu na terenie placówek oświatowych);

- **zakup licencji na oprogramowanie edukacyjne** (JST mogą nabywać licencje na różnorodne oprogramowanie edukacyjne, np. programy do nauki języków obcych, edytory graficzne, narzędzia do tworzenia prezentacji czy platformy e-learningowe; mogą one być potem wykorzystywane przez nauczycieli i uczniów);
- **wspieranie projektów e-learningowych** (JST mogą wspierać szkoły, przedszkola i placówki oświatowe w realizacji projektów rozmaitych planów e-learningowych, np. zakupu kursów online, organizację szkoleń dla nauczycieli z zakresu wykorzystania technologii w edukacji czy rozwój platformy do zdalnej nauki);
- **tworzenie zasobów cyfrowych** (JST mogą inwestować w tworzenie zasobów cyfrowych, np. platform e-booków, baz wiedzy online czy repozytoriów zasobów multimedialnych, które mogą być wykorzystywane przez nauczycieli i uczniów w procesie nauczania i uczenia się).

Rozwijanie umiejętności cyfrowych uczniów i nauczycieli

JST mogą organizować zarówno szkolenia i warsztaty dla nauczycieli z zakresu wykorzystania technologii informatycznych w pracy dydaktycznej, jak i edukować społeczność lokalną na temat korzyści płynących z wykorzystania cyfrowych narzędzi w edukacji. Dostarczanie szkołom, przedszkolom i placówkom oświatowym cyfrowych zasobów i narzędzi informatycznych przez organ prowadzący wymaga skoordynowanego działania, wsparcia finansowego, a także odpowiedniej infrastruktury technicznej. Jest to istotny element wspierania rozwoju edukacji cyfrowej i zapewnienia równego dostępu do nowoczesnych technologii uczniom i nauczycielom.

Cyfryzacja polskiej edukacji wymaga strategicznej wizji, w której nadrzędną rolę odgrywają cele związane z kształceniem. Szerokopasmowy dostęp, nowoczesny sprzęt czy zasoby sieciowe są jedynie środkami do celu, jakim powinno być dobro uczniów i nauczycieli oraz jakość edukacji. Warto też pamiętać o tym, że równie niezbędne jest podejście systemowe, które zakłada równoczesny rozwój czterech opisanych przez nas obszarów: infrastruktury, sprzętu, zasobów oraz kompetencji nauczycieli. Kwestią mniej istotną jest wówczas skoncentrowanie się tylko na jednym z wskazanych aspektów.

8. Bibliografia.

Dziubińska A., (2018), „Rola systemów informatycznych w zarządzaniu placówką oświatową”, „Zarządzanie Publiczne” nr 42(3), s. 67–80.

Gajderowicz T., Jakubowski M., (2020), „Cyfrowe wyzwania stojące przed polską edukacją”, Warszawa: WNE UW oraz Evidence Institute, zob. PIE-6(2020)_Cyfrowe_wyzwania.indd [online, dostęp dn. 2.09.2025].

Grzelak M., (2020), „Rola technologii informacyjno-komunikacyjnych w doskonaleniu zarządzania oświatą w Polsce”, „Zarządzanie Publiczne” nr 47(2), s. 185–198.

Informacja z badania ankietowego „Diagnoza Technologii Informacyjno-Komunikacyjnych”, (Grudzień 2022), Warszawa: Fundacja edTech Poland, patronat Instytut Badań Edukacyjnych, zob. Informacja z badania ankietowego pt. Diagnoza Technologii Informacyjno-Komunikacyjnych - Fundacja EdTech Poland [online, dostęp dn. 2.09.2025].

Janicki R., (2018), „Systemy informatyczne w zarządzaniu placówkami oświatowymi: analiza możliwości i ograniczeń”, „Zarządzanie Publiczne” nr 45(4), s. 377–391.

Kozłowska A., (2019), „Ewaluacja systemów informatycznych w zarządzaniu oświatą: wyzwania i perspektywy dla polskich szkół”, „Edukacja Informatyczna” nr 21(2), s. 89–102.

Krawczyk M., Zięba A., (2017), „Wykorzystanie systemów informatycznych w zarządzaniu szkołą na przykładzie polskich placówek oświatowych”, „Edukacja Techniczna i Informatyczna” nr 1(1), s. 45–58.

Mazur K., (2018), „Zastosowanie systemów informatycznych w zarządzaniu placówką oświatową: wybrane problemy i perspektywy rozwoju”, „Zarządzanie i Finanse” nr 16(1), s. 25–39.

Nowak P., Wiśniewski M., (2017), „Znaczenie systemów informatycznych w procesie zarządzania placówkami oświatowymi w Polsce”, „Edukacja Techniczna i Informatyczna” nr 2(2), s. 67–78.

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 10 marca 2023 roku, w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo oświatowe (Dziennik Ustaw z 2023 roku pozycja 900), zob. D20230900L.pdf [dostęp, online dn. 2.09.2025].

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 czerwca 2023 roku w sprawie ogłoszenia jednolitego tekstu ustawy o finansach publicznych (Dziennik Ustaw z 2023 roku pozycja 1270), zob. D20231270L.pdf [dostęp, online dn. 2.09.2025].

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 12 kwietnia 2023 roku w sprawie ogłoszenia jednolitego tekstu ustawy – Karta Nauczyciela (Dziennik Ustaw z 2023 roku pozycja 984 wraz z jednolitym tekstem ustawy z dnia 26 stycznia 1982 roku – Karta Nauczyciela (Dziennik Ustaw z 2021 roku pozycja 1762), zob. D20230984L.pdf [dostęp, online dn. 2.09.2025].

Podstawowe kierunki realizacji polityki oświatowej państwa w roku szkolnym 2023/2024, zob. Podstawowe kierunki realizacji polityki oświatowej państwa w roku szkolnym 2023/2024 - Ministerstwo Edukacji Narodowej - Portal Gov.pl (www.gov.pl) [dostęp, online dn. 2.09.2025].

Płusa A., (2023), „Nauka w cyfrowym świecie transformacji technologicznej i globalnych wyzwań”, Warszawa: Ośrodek Rozwoju Edukacji.

Raport Najwyższej Izby Kontroli, „Informacja o wynikach kontroli. Cyfryzacja szkół”, KNO.40.007.00.2016 Nr ewid. 62/2017/P/16/025/KNO, zob. kno~p_16_025_201611221355141479822914~02.pdf [dostęp, online dn. 2.09.2025].

Ratajczak M., (2019), „Wykorzystanie systemów informatycznych w zarządzaniu szkołą na przykładzie polskich placówek oświatowych”, „Edukacja Informatyczna” nr 20(3), s. 123–137.

Rozporządzenie z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dziennik Ustaw z 2017 roku pozycja 2247), zob. D20172247.pdf (sejm.gov.pl) [dostęp, online dn. 2.09.2025].

Rozporządzenie Ministra Edukacji Narodowej w sprawie podstawowych warunków niezbędnych do realizacji przez szkoły i nauczycieli zadań dydaktycznych, wychowawczych i opiekuńczych oraz programów nauczania (Dziennik Ustaw z 2024 roku pozycja 9), zob. D20240009.pdf [dostęp, online dn. 2.09.2025].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich informacji oraz uchylenia dyrektywy 95/46/WE/(RODO), zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016_679 z dnia 27 kwietnia (1).pdf [online, dostęp dn. 2.09.2025].

Rozporządzenie Ministra Edukacji Narodowej z dnia 23 listopada 2023 roku w sprawie podstawowych warunków niezbędnych do realizacji przez szkoły i nauczycieli zadań dydaktycznych, wychowawczych i opiekuńczych oraz programów nauczania (Dziennik Ustaw z 2024 roku pozycja 9), zob. Dz. U. z 2024 r. poz.9 [dostęp, online dn. 2.09.2025].

Śliwerski B., (2019), „Wykorzystanie technologii informacyjno-komunikacyjnych w zarządzaniu placówkami oświatowymi”, „Edukacja i Dialog” nr 11, s. 111–123.

Szymańska A., (2020), „Systemy informatyczne w zarządzaniu szkołą: wyzwania i perspektywy”, „Nowa Edukacja” nr 3(45), s. 73–86.

Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dziennik Ustaw z 2018 roku pozycja 1000), zob. D20181000L.pdf [dostęp, online dn. 2.09.2025].

Wyrwa F., (2021), „Centralizacja zarządzania informatycznego w gminie Margonin. Karta opisu dobrej praktyki”, Warszawa: Ośrodek Rozwoju Edukacji, zob. centralizacja-zarzadzania-informatycznego-w-gminie-margonin (3).pdf [dostęp, online dn. 2.09.2025].

Załącznik do uchwały numer 15 Komitetu Monitorującego. Program „Fundusze europejskie dla rozwoju społecznego 2021–2027” z dnia 15 marca 2023 roku, zob. Zal_do_uchwaly_nr_15_MEiN_Dzialanie_01_04_ORE_pilotaz_15_03_2023.pdf (rozwojspoeczny.gov.pl) [dostęp, online dn. 2.09.2025].

MATERIAŁ 2. ROLA I ZADANIA JEDNOSTEK SAMORZĄDU TERYTORYALNEGO W ZAKRESIE CYFRYZACJI OŚWIATY



Michał Cupiał, Zofia Domaradzka-Grochowalska, Dorota

Jastrzębska, Anna Pawełas, Dorota Pintal, Dorota Tomaszewicz

1. Wprowadzenie.

Skuteczna cyfryzacja oświaty wymaga nie tylko inwestycji w sprzęt i infrastrukturę, ale także wdrażania narzędzi zarządczych i wspierania personalnego rozwoju organizacji. W Materiale 1., koncentrującym się na roli i zadaniach oświaty, w sposób obszerny przedstawiono potrzeby i trudności samorządów w odniesieniu do cyfryzacji szkół oraz placówek oświatowych. Poza tym w tym fragmencie szczegółowo opisano obowiązki JST wynikające z przepisów prawa.

Poza tym – jak podaje raport¹⁶ Związku Miast Polskich, który sporządzono na podstawie badań przeprowadzonych w szkołach podstawowych i ponadpodstawowych w 2024 roku w ramach projektu „Cyfrowy rozwój oświaty

¹⁶ Ośrodek Rozwoju Edukacji, (2023), „Cyfrowy rozwój oświaty w ramach samorządu terytorialnego”, Warszawa: Ośrodek Rozwoju Edukacji, zob. (<https://www.ore.edu.pl/category/projekty-fers/cyfrowy-rozwoj-oswiaty-w-jednostkach-samorządu-terytorialnego-szkolenie-i-doradztwo-dla-kadr-jst/cyfrowy-rozwoj-oswiaty-w-jednostkach-samorządu-terytorialnego-szkolenie-i-doradztwo-dla-kadr-jst-aktualności/>) [dostęp, online dn. 2.09.2025].

w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST” – w kwestii cyfryzacji szkół i placówek pojawiają się kolejne wnioski:

- JST powinny mieć za zadanie systematyczne ocenianie dostępnej infrastruktury cyfrowej i kompetencji, aby móc podejmować planowane działania, które odpowiadają rzeczywistym potrzebom;
- JST zarówno w wymiarze strategicznym, jak i praktycznym wymagają specjalnych programów szkoleniowych i wsparcia doradczego w zarządzaniu cyfryzacją;
- działania w zakresie cyfryzacji muszą być skoordynowane z aktywnym udziałem lokalnych interesariuszy, a ponadto powinny wspierać procesy dialogu i współpracy;
- tworzenie sieci samorządów, które dzielą się doświadczeniami, jest niezwykle istotne, dlatego warto wspierać zarówno powstawanie takich grup, jak i systematyczne dokumentowanie oraz promowanie skutecznych rozwiązań;
- JST powinny monitorować ryzyko wykluczenia cyfrowego i podejmować działania wyrównawcze poprzez dostarczanie sprzętu, łącza internetowego, a także oferowanie wsparcia kompetencyjnego;
- zadania JST powinny obejmować inwentaryzację i racjonalne wykorzystanie infrastruktury cyfrowej, a także skierować się ku rozwiązaniom wykorzystującym zasoby cyfrowe (w tym e-materiały i platformy edukacyjne).

Odpowiedzi na zidentyfikowane potrzeby, wnioski i realizację zadań oświatowych w zakresie cyfryzacji zostały omówione w części „Rola i zadania JST w zakresie cyfryzacji oświaty”. W materiale tym przedstawiono również polecane narzędzia zarządcze i rozwiązania wspierające personalny rozwój organizacji, które mogą być implementowane w różnego rodzaju samorządach.

2. Zadania JST w zakresie cyfryzacji oświaty.

Zadanie 1. Wdrożenie narzędzi cyfrowych umożliwiających zdalne nauczanie z wykorzystaniem technologii cyfrowych na poziomie JST, szkół, przedszkoli i placówek oświatowych.

Lekcje prowadzone w formie stacjonarnej umożliwiają w sposób nieograniczony stosowanie technik i narzędzi edukacyjnych. Dlatego przy wyborze platform

edukacyjnych tak istotne jest określenie ich funkcjonalności i możliwości. Istnieje oczywiście opcja wdrożenia bardzo zróżnicowanych narzędzi cyfrowych wykorzystywanych przy nauczaniu, jednak w dalszej konsekwencji może to doprowadzić do niepotrzebnego chaosu i bezpośrednio wpłynąć na jakość nauczania. Z tego powodu ważnym zagadnieniem jest wprowadzenie odpowiednich narzędzi umożliwiających zdalne nauczanie we wszystkich szkołach podlegających danej JST. Zanim jednak ten proces rozpocznie się, powinno się konkretnie określić potrzeby poszczególnych szkół i placówek edukacyjnych w zakresie funkcjonalności platformy.

Wśród podstawowych elementów, jakie powinna uwzględniać platforma edukacyjna, można wskazać m.in.:

- możliwość wyświetlania prezentacji i szybkie przełączanie się między ekranami;
- możliwość publikacji i pobrania plików (np. kart pracy, zeszytu ćwiczeń czy innych materiałów dydaktycznych dla uczniów oraz nauczycieli);
- możliwość zaangażowania uczniów poprzez dyskusję, zadania, pracę w grupach;
- możliwość sprawdzenia wiedzy uczniów w formie testów, quizów lub egzaminów.

Zadanie 2. Wdrożenie narzędzi informatycznych wspomagających zarządzanie oświatą.

Dokumenty finansowe – raporty, arkusze organizacji, System Informacji Oświatowej (dalej SIO) – które gromadzi się na potrzeby analiz, są elementem planowania strategicznego. Umożliwia ono podejmowanie trafnych decyzji w zakresie optymalizacji organizacji i racjonalizacji finansów oświaty. Efektywne połączenie planowania strategicznego z narzędziami informatycznymi zmniejsza wysiłek organizacyjny związany z budżetowaniem, a także usprawnia kontrolowanie realizacji założeń budżetowych.

Można wskazać trzy główne grupy korzyści płynących z zastosowania narzędzi informatycznych przy planowaniu, realizacji i wykonaniu założeń finansowych:

- **korzyści zarządcze** – w tym przypadku szczególne znaczenie ma łatwość analizowania danych, zarówno tych organizacyjnych (arkusze organizacji), jak i ekonomicznych (racjonalizacja wydatków oświatowych), które są zgromadzone w jednym miejscu;
- **korzyści organizacyjne** – to dzięki nim dostęp do informacji znajduje się na poziomie szczegółowości ustanowionym przez organ (budżet sprowadzony do

poziomu pozycji klasyfikacyjnej). Ponadto uzyskane z systemu informacje są rzetelne i powiązane ze sobą na każdym etapie procesu budżetowego;

- **korzyści ekonomiczne** – one są najbardziej istotne, ponieważ wynikają z funkcjonowania systemu. Wykorzystanie narzędzi informatycznych umożliwia, podejmowanie trafnych decyzji zarządczych, które są efektem rzetelnej analizy danych, a ponadto prowadzą do zracjonalizowania wydatków oświatowych. Poza tym narzędzia cyfrowe pozwalają zaoszczędzić czas i zużycie materiałów biurowych niezbędnych w procesie zbierania danych.

Warto też pamiętać o tym, że decyzje podejmowane są szybko i nie są przypadkowe, a proces zbierania danych (jednolitych) usprawnia zarządzanie oświatą. Tym samym takie działanie stwarza możliwość racjonalizacji kosztów. Dzięki narzędziom informatycznym można łatwo zarówno wyliczyć wskaźniki służące do analizy, jak i te dające możliwość tworzenia zestawień. Planowanie budżetu z uwzględnieniem szczegółowych pozycji pozwala z powodzeniem przeprowadzać przetargi centralne. Nie można też zapomnieć o jeszcze innym korzystnym aspekcie, czyli o środkach finansowych zaplanowanych w budżetach poszczególnych JST. Kwoty te nie są przypadkowe. Wynikają bowiem z arkuszy organizacji oraz umów zawartych w wyniku zamówienia publicznego przeprowadzonego centralnie przez organ prowadzący. Opisy dobrych praktyk doskonale ilustrują praktyczne zastosowanie wskazanych narzędzi.

Zadanie 3. Inwentaryzacja posiadanych zasobów cyfrowych (obejmujących software i hardware) w szkołach, przedszkolach lub placówkach oświatowych.

Z prawnego punktu widzenia proces inwentaryzacji IT jest formalnym obowiązkiem każdej szkoły lub placówki oświatowej. Polega on na sporządzeniu wykazu wszystkich dostępnych sprzętów informatycznych oraz oprogramowania dostępnego w danej jednostce. Choć zazwyczaj przegląd systemów informatycznych przeprowadza się ostatniego dnia każdego roku obrotowego, to jednak warto pamiętać, że termin ten jest elastyczny. Przed doposażeniem szkół, przedszkoli i placówek oświatowych w sprzęt komputerowy – w celu realizacji zadań przez JST w zakresie cyfryzacji – warto dokonać inwentaryzacji posiadanych zasobów cyfrowych, określić ich stan i ewentualnie wskazać braki.

Zapewnienie bieżącej (pozwalającej określić posiadane zasoby w dowolnym momencie) inwentaryzacji zasobów IT – zarówno sprzętowych (hardware), jak

i programowych (software) – jest ważne z kilku powodów (szczególnie w kontekście rozwoju cybernarzędzi w edukacji oraz bezpieczeństwa przetwarzanych danych).

Bieżący przegląd pozwala na identyfikację i zarządzanie zasobami, co jest fundamentem dla bezpieczeństwa informacji. Pozwala to na ochronę przed zagrożeniami i atakami (np. malware czy ransomware), które mogą wykorzystać niezabezpieczone lub przestarzałe systemy oraz aplikacje. Zarówno dobre praktyki, jak i aktualne regulacje prawne wymagają od organizacji prowadzenia bieżącej ewidencji zasobów przetwarzających dane osobowe. Dzięki prowadzeniu takiej ewidencji podmioty edukacyjne mogą lepiej spełniać wymogi związane z bezpieczeństwem informacji, a tym samym zminimalizować ryzyko naruszeń w zakresie bezpieczeństwa danych i uniknąć sankcji finansowych.

Inwentaryzacja pozwala także na efektywne zarządzanie zasobami, umożliwiając odpowiednią alokację i wykorzystanie sprzętu oraz oprogramowania. W kontekście szkół, przedszkoli i placówek oświatowych, w których budżety często są ograniczone, optymalne wykorzystanie dostępnych zasobów informatycznych może znacząco wpłynąć na jakość nauczania i dostęp do nowoczesnych narzędzi edukacyjnych. Bieżąca ewidencja potencjału IT umożliwia szybkie identyfikowanie systemów, które wymagają aktualizacji lub konserwacji. To z kolei zarówno pomaga w zapobieganiu awariom mogącym zakłócić proces nauczania, jak i chroni przed eksploatacją znanych podatności (luk w zabezpieczeniach systemów informatycznych) przez cyberprzestępców. Inwentaryzacja pozwala również na identyfikację zbędnych lub rzadko używanych zasobów, co umożliwia ich lepsze wykorzystanie lub wycofanie. Takie działanie przyczynia się do redukcji kosztów.

Zarządzanie zasobami IT stało się jeszcze bardziej istotne w dobie pandemii COVID-19 oraz wzrostu popularności zdalnego nauczania. Prowadzenie regularnego przeglądu pozwala na lepsze zrozumienie architektury sieciowej i systemów informatycznych. A to z kolei jest niezbędne do skutecznego planowania realizacji zadań edukacyjnych w odniesieniu do aktualnych potrzeb, dostępu do niezbędnych narzędzi i zasobów, a także przygotowania zabezpieczeń przed potencjalnymi problemami lub niebezpieczeństwami typowymi dla IT.

Bieżąca inwentaryzacja może być także podstawą do wzrostu zapotrzebowania na niezbędny sprzęt i oprogramowanie. A te z kolei będą wykorzystywane w centralnym zarządzaniu oświatą. Przeprowadzanie ewidencji wpływa korzystnie

na efektywne wdrożenie tych zasobów cyfrowych. Proces ten powinien obejmować zautomatyzowane mechanizmy identyfikowania i ewidencjonowania posiadanych urządzeń oraz oprogramowania. W szczególności inwentaryzacja posiadanych zasobów IT powinna obejmować następujące rodzaje urządzeń:

- przyłącza internetowe;
- zabezpieczenia brzegowe (router lub zintegrowane zarządzanie zagrożeniami, czyli Unified Threat Management (dalej UTM));
- sieci informatyczne;
- zabezpieczenia fizyczne danych;
- zabezpieczenia softwarowe;
- dostępność sieci bezprzewodowej;
- komputery nauczycieli;
- serwery oraz dyski sieciowe;
- drukarki;
- oprogramowanie.

Dostęp do informacji o aktualnie posiadanych zasobach i adekwatne zarządzanie tymi elementami są niezbędne do zapewnienia efektywnego wykorzystania technologii cyfrowych w edukacji. A to z stanowi ważny element zarówno dla samego procesu nauczania, ale także dla bezpieczeństwa informacji w szkołach i placówkach edukacyjnych.

Zadanie 4. Weryfikacja posiadanych zasobów pod kątem wykorzystania technologii cyfrowych przez szkoły, przedszkola lub innej placówki oświatowej.

Popularność zasobów cyfrowych w szkołach, przedszkolach i placówkach edukacyjnych wzrasta z każdym rokiem. I choć materiały tego typu same w sobie nie przyczyniają się do poprawy efektów nauczania, to jednak warto zwrócić uwagę na inny pozytywny aspekt. Wzrasta bowiem nie tylko poziom wykorzystania zasobów cyfrowych w codziennej praktyce, ale także rozwijają się umiejętności nauczycieli w zakresie korzystania z takich narzędzi. Dlatego warto przeprowadzić badanie wśród grona pedagogicznego (np. w formie ankiety) pod kątem wykorzystania technologii cyfrowych w pracy szkoły lub placówki oświatowej. Podstawowymi zagadnieniami ankietowymi mogłyby być następujące kwestie:

- stopień wykorzystania przez nauczycieli dostępnych w sieci cyfrowych zasobów do realizacji podstawy programowej;

- uzasadnienie oceny przez nauczyciela i ewentualnie podanie pozytywnego lub negatywnego przykładu ilustrującego stan wykorzystania zasobów cyfrowych w codziennej praktyce;
- wyrażenie przez nauczycieli ogólnej opinii w sprawie wykorzystania zasobów cyfrowych w placówce zatrudnienia.

Równie istotnym działaniem, które weryfikuje stan wykorzystania zasobów cyfrowych podczas zajęć edukacyjnych, byłoby przeprowadzenie takiego badania wśród uczniów. Kolejny krok stanowiłoby porównanie wyników ankiety nauczycielskiej z opiniami dzieci i młodzieży.

Zadanie 5. Finansowanie doskonalenia nauczycieli w zakresie cyfrowej transformacji szkoły, przedszkola lub innej placówki oświatowej.

Efektywny proces dydaktyczny wymaga praktycznej znajomości odpowiednich narzędzi cyfrowych oraz stałego rozwijania kompetencji nauczycieli. Poziom ich umiejętności i przygotowania do organizacji procesów edukacyjnych z włączeniem TIK, jak i przeprowadzanie nauczania zdalnego wpływają na skuteczność działań w zakresie rozwijania kompetencji cyfrowych uczniów.

Współczesny nauczyciel w codziennej pracy z uczniami świadomie wykorzystuje technologie cyfrowe. Tym samym angażuje i motywuje dzieci i młodzież do czynnego udziału w zajęciach.

JST mają wpływ na jakość doskonalenia nauczycieli poprzez planowanie wydatków zgodnie z potrzebami danej szkoły lub placówki edukacyjnej. Ważnym elementem w procesie doskonalenia umiejętności cyfrowych nauczycieli jest odchodzenie od incydentalnych form na rzecz wspomagania długofalowego, które jest procesem uwzględniającym diagnozowanie, planowanie, wdrażanie i monitorowanie działań oraz ocenę efektów.

Zadanie 6. Planowanie i budowa infrastruktury IT.

Planowanie i budowa infrastruktury informatycznej są kluczowe dla zapewnienia stabilności, wydajności oraz bezpieczeństwa sieci zarówno w placówkach edukacyjnych, jak i JST. Proces ten obejmuje kilka istotnych etapów, które zapewniają odpowiednie dostosowanie infrastruktury IT do specyficznych potrzeb organizacyjnych i wymogów bezpieczeństwa. Fundamentem efektywności i bezpieczeństwa jest projektowanie

architektury sieci, czyli określenie jej najlepszej topologii w zależności od potrzeb organizacyjnych i potencjalnych zagrożeń. Właściwie zaprojektowana architektura sieci zapewnia optymalne wykorzystanie zasobów, minimalizuje opóźnienia i zwiększa przepustowość. Tym samym przyczynia się do płynnego działania narzędzi edukacyjnych i aplikacji administracyjnych. Zastosowanie odpowiedniego sprzętu sieciowego zgodnie z wymaganiami wydajności i bezpieczeństwa jest kolejnym krokiem do zapewnienia niezawodności i bezpieczeństwa sieci. Wybór nowoczesnych i odpowiednio zabezpieczonych urządzeń (np. routerów, przełączników oraz punktów dostępowych) wpływa na stabilność i bezpieczeństwo całej infrastruktury IT.

Ważnym elementem jest także przeprowadzenie testów wydajności i bezpieczeństwa nowo utworzonej infrastruktury, co pozwala na identyfikację i eliminację potencjalnych problemów, zanim będą miały one wpływ na codzienne funkcjonowanie szkoły, przedszkola i placówki edukacyjnej.

Dobrze zaplanowana topografia sieci, która uwzględni strefy zdemilitaryzowane, pozwoli skutecznie i efektywnie zaplanować zabezpieczenia i prawidłowo umieścić elementy cyberbezpieczeństwa m.in.:

- urządzenia UTM;
- firewall;
- system zapobiegania włamaniom, czyli Intrusion Prevention System (dalej IPS);
- system wykrywania włamań, czyli Intrusion Detection System (dalej IDS);
- elementy monitorujące ruch sieciowy.

Zabezpieczenia te pozwolą chronić sieć przed nieautoryzowanym dostępem, atakami rozproszonej usługi, czyli Distributed Denial of Service (dalej DDoS) oraz innymi zagrożeniami. A to z kolei korzystnie wpływa na bezpieczeństwo uczniów i pracowników szkoły, przedszkola oraz placówki oświatowej.

Zapewnienie efektywnego planowania i budowy infrastruktury IT jest istotne zarówno dla płynnego funkcjonowania narzędzi edukacyjnych i zarządczych, jak i dla ochrony danych i zasobów informatycznych przed różnego rodzaju zagrożeniami. Poprzez odpowiednie projektowanie, wybór sprzętu, wdrażanie zabezpieczeń, testowanie oraz monitorowanie, placówki edukacyjne mogą zapewnić stabilne, bezpieczne i wydajne środowisko IT, które wspiera proces nauczania i zarządzania.

Zadanie 7. Analiza ryzyka dla zasobów IT.

Zarządzanie bezpieczeństwem informacji i zapewnienie ciągłości realizacji zadań edukacyjnych i zarządczych jest nierozzerwalnie związane z analizą ryzyka, którą przeprowadza się wobec zasobów IT wykorzystywanych w danej szkole, przedszkolu czy placówce oświatowej. Proces wymaga zidentyfikowania potencjalnych zagrożeń, co pozwala na wskazanie możliwych źródeł ryzyk mogących wpływać na urządzenia, systemy informatyczne i przetwarzane w nich dane. Analiza ewentualnych niebezpieczeństw pozwala także ustalić podatności, które mogą być wykorzystane przez cyberprzestępców albo stać się przyczyną zwykłych awarii uniemożliwiających realizację zadań.

Kolejnym krokiem jest ustalenie potencjalnego wpływu realnych zagrożeń na jednostkę oświatową lub JST. Ta ocena z jednej strony pozwala zrozumieć konsekwencje wynikające z wystąpienia ewentualnych niebezpieczeństw, ale też wskazuje na konieczność posiadania odpowiednich zasobów pomocnych w ich usunięciu.

Na podstawie tych ocen szkoła, przedszkole i placówka oświatowa lub JST mogą zaprojektować zabezpieczenia, czyli mechanizmy minimalizujące potencjalne ryzyka. Opracowanie strategii zarządzania w sytuacji naruszenia systemu informatycznego danej jednostki edukacyjnej jest kluczowe dla minimalizowania potencjalnych zagrożeń oraz ich skutków. Umożliwia to planowanie i wdrażanie działań prewencyjnych, co jest nie tylko niezbędne dla bezpieczeństwa zasobów informatycznych i informacji, ale także zapewnia ciągłość działania systemów informatycznych.

W dalszym etapie monitorowanie zidentyfikowanych ryzyk pozwala na bieżące dostosowywanie strategii zarządzania bezpieczeństwem informacji do zmieniających się warunków i nowych zagrożeń. Tym samym korzystnie wpływa na utrzymanie wysokiego poziomu bezpieczeństwa informacji w szkole, przedszkolu i placówce oświatowej czy siedzibie JST.

Zadanie 8. Dobór zabezpieczeń.

Efektem poprzednich zadań jest nieodzowne dokonanie doboru adekwatnych zabezpieczeń do zidentyfikowanych zagrożeń. Proces ten jest nie tylko dobrą praktyką, ale stanowi również wymóg prawny wynikający z przepisów unijnych:

RODO i Dyrektywy o Bezpieczeństwie Sieci i Systemów Informacyjnych 2 (dalej NIS2), polskich aktów prawnych: ustawy o krajowym systemie cyberbezpieczeństwie

(Dziennik Ustaw 2018 pozycja 1560) i rozporządzenie w sprawie KRI (Dziennik Ustaw 2024 pozycja 773), a także minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Błyskawicznie rozwijająca się cyfryzacja nie omija JST czy szkół, przedszkoli lub placówek edukacyjnych. Powinno się pamiętać, aby każdy podmiot świadomie zarządzał zabezpieczeniami w najistotniejszych obszarach. Ochrona transferu danych powinna uwzględniać wdrożenie w szczególności technologii szyfrowania danych przesyłanych w sieci, a także identyfikacji podmiotów uczestniczących w tym procesie. Wprowadzanie środków szyfrowania zapewnia ochronę danych podczas ich przesyłania przed nieautoryzowanym dostępem. Kolejnym elementem jest zabezpieczenie punktu styku zasobów IT danej placówki z siecią internetową. Obszar ten obejmuje gwarancję zabezpieczeń w postaci aktywnych urządzeń brzegowych (np. UTM, bramy sieciowe trzeciej generacji) oraz zapewnienie im aktualnych polityk bezpieczeństwa (np. poprzez wykupienie odpowiednich licencji lub zapewnienie wykwalifikowanego personelu zarządzającego).

Ponadto warto sobie uzmysłować, że regularne aktualizacje urządzeń sieciowych oraz podstawowego oprogramowania układowego – wbudowanego na stałe w pamięć urządzeń elektronicznych, odpowiadającego za ich podstawową funkcjonalność i sterowanie pracą sprzętu – (dalej firmware) są konieczne. Pozwalają zabezpieczyć zasoby cyfrowe przed nowymi zagrożeniami i podatnościami. Wdrożenie narzędzi do monitorowania stanu i wydajności urządzeń sieciowych pozwala zarówno na bieżące śledzenie ich funkcjonowania, jak i szybkie reagowanie na wszelkie nieprawidłowości.

W aspekcie kontaktu zasobów IT danej placówki z siecią zewnętrzną nie można pominąć analizy ruchu sieciowego. Jego monitorowanie obejmuje wprowadzenie systemów wykrywania i zapobiegania włamaniom (m.in. IDS / IPS), które monitorują sieć i reagują na podejrzany ruch. Regularne przeglądy i analizy ruchu sieciowego pomagają identyfikować nieautoryzowane próby dostępu i inne nieprawidłowości. Zapisywanie i analiza identyfikatorów graficznych – (dalej loga sieciowe) – są kluczowe w procesie śledzenia, identyfikowania, badania i reagowania na wszelkie próby zmierzające do zniszczenia systemów cyfrowych danej placówki oświatowej lub JST.

Innym aspektem bezpieczeństwa jest – zasygnalizowana wcześniej – topografia sieci. Pozwala ona na utworzenie stref zdemilitaryzowanych (dalej DMZ) dla systemów

narażonych na dostęp z internetu. W ten sposób topografia sieci pomaga izolować krytyczne zasoby od bezpośredniego kontaktu z siecią zewnętrzną.

Dla użytkowników wyjątkowo istotna jest polityka zarządzania uprawnieniami. Mechanizmy kontroli dostępu do systemów lub urządzeń na podstawie zaplanowanego procesu nadawania ról i upoważnień zapewniają danej osobie poziom dostępu, których jest adekwatny do powierzonych jej zadań. Systemy te zapobiegają także nieuprawnionej eskalacji nadawanych uprawnień.

Kolejnym obszarem jest zabezpieczenie urządzeń końcowych poprzez instalację oprogramowania antywirusowego i firewall. Niemniej istotne jest w tym aspekcie utrzymywanie aktualnej wersji oprogramowania i systemów operacyjnych, aby chronić urządzenia przed znanymi lukami bezpieczeństwa. Z punktu widzenia ochrony jest ważne zapewnienie możliwości zdalnego zarządzania urządzeniami końcowymi poprzez implementację nowoczesnych systemów monitorujących lub audytowych. Ponadto wprowadzenie pełnego szyfrowania dysków na urządzeniach końcowych zapewnia, że przechowywane tam dane są chronione w przypadku utraty lub kradzieży tych sprzętów.

Równie ważne jest także zastosowanie oprogramowania monitorującego wykorzystanie urządzeń IT w danej placówce oświatowej lub JST. Dzięki temu możliwe jest monitorowanie wszelkich zdarzeń w kontekście bezpieczeństwa i zapewnienia ciągłości działania określonej jednostki.

Stale zmieniające się warunki cyberprzestrzeni wymagają także wykwalifikowanego personelu informatycznego. Zadania w tym zakresie mogą być realizowane zarówno przez pracowników danego podmiotu, jak i – w formie zlecenia określonych zadań – jakąś osobę spoza danej szkoły, przedszkola, placówki oświatowej czy JST.

Trzeba sobie uzmysłowić, że niezależnie od tego, kto zapewni ciągłość działania i zagwarantuje bezpieczeństwo zasobów IT, to odpowiedzialność za sprawdzenie kwalifikacji tej osoby spoczywa na organach prowadzących daną placówkę.

Powyższe elementy stanowią minimum, które trzeba uwzględnić w jednostkach oświatowych i JST w celu zapewnienia kompleksowej ochrony systemów i danych. Takie podejście jest zgodne z aktualnymi wymogami prawa, dobrymi praktykami, międzynarodową normą standaryzującą systemy zarządzania bezpieczeństwem

informacji (dalej ISO 27001) lub – zalecanymi w sektorze publicznym – wytycznymi amerykańskiego Narodowego Instytutu Standardów i Technologii (dalej NIST).

Kompleksowe podejście do bezpieczeństwa informacji wpływa na ochronę danych, bezpieczeństwo infrastruktury IT, zgodność z przepisami prawnymi oraz ciągłość nauczania. Zapewnia zabezpieczenie przed złośliwym oprogramowaniem i edukuje społeczność danej szkoły, przedszkola, placówki oświatowej lub JST na temat zagrożeń cybernetycznych oraz najlepszych praktyk w zakresie bezpieczeństwa informatycznego.

Zadanie 9. Planowanie i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji.

Projektowanie i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) z uwzględnieniem planów ciągłości działania i procedur przywracania funkcjonalności mechanizmów informatycznych na skutek zniszczenia zapory bezpieczeństwa zasobów cyfrowych jest niezbędne dla zapewnienia stabilności oraz odporności danego podmiotu na różne zagrożenia. Poza tym SZBI umożliwia także spełnienie wymagań prawnych wynikających ze rozporządzenia w sprawie KRI, przepisów określających Krajowy System Cyberbezpieczeństwa (dalej KSC) z uwzględnieniem wymagań dyrektywy NIS2 oraz ogólnego rozporządzenia o ochronie danych.

Planowanie SZBI zaczyna się od identyfikacji krytycznych zasobów i funkcji biznesowych, co pozwala na identyfikację głównych elementów niezbędnych dla ciągłości działania danej szkoły, przedszkola, placówki edukacyjnej czy JST. Następnie tworzy się szczegółowe mechanizmy postępowania podczas zarządzania bezpieczeństwem IT oraz przygotowuje się procedury reagowania uwzględniające – w ramach planów ciągłości działania lub sposobów odzyskiwania systemów po awarii – różne scenariusze awaryjne. Mechanizmy te powinny uwzględniać także przeprowadzanie testów, symulacji ataków i awarii w celu sprawdzenia zaplanowanej strategii awaryjnej. Takie działanie jest niezbędne do weryfikacji skuteczności tych planów, a w razie potrzeby także do gotowości ich użycia.

Ciągła ewaluacja i aktualizacja procedur (w odniesieniu do zmieniających się warunków operacyjnych i technologicznych) są niezwykle ważne dla utrzymania ich aktualności i skuteczności. Proces ten obejmuje również regularne szkolenia dla pracowników z zakresu obowiązujących sposobów reagowania na awarie

i mechanizmów zapewnienia ciągłości postępowania. Przygotowanie personelu w tym zakresie zapewnia, że wszyscy pracownicy w przypadku awarii są świadomi swoich ról i odpowiedzialności. A to z kolei stanowi niezwykle ważny aspekt dla skutecznego zrealizowania zadań w przypadku wystąpienia incydentu informatycznego.

Szkoły, przedszkola, placówki oświatowe oraz JST – dzięki kompleksowemu podejściu do przygotowania i wdrażania SZBI z uwzględnieniem planów nieprzerwanego działania i odzyskiwania danych na skutek uszkodzenia systemu informatycznego – są dobrze przygotowane na różne scenariusze awaryjne. To podejście pozwala na minimalizowanie zakłóceń w działalności, ochronę krytycznych zasobów i funkcji biznesowych oraz szybką i skuteczną reakcję na incydenty. A to z kolei jest niezbędnym czynnikiem dla utrzymania nieprzerwanego działania systemu cyfrowego, ochrony danych oraz prawidłowego funkcjonowania infrastruktury IT.

Obecnie istotny element SZBI stanowi kierowanie zdarzeniami bezpieczeństwa informacji (czyli rozmaitymi sytuacjami sugerującymi możliwość lub faktyczne naruszenie ochrony informacji w danej placówce edukacyjnej lub samorządowej). Każda jednostka oświatowa i JST, które spełniają wymogi prawne określone w krajowym systemie cyberbezpieczeństwa i ogólnym rozporządzeniu o ochronie danych, powinny mieć opracowane i wdrożone procedury działania na wypadek incydentów informatycznych.

Zadanie 10. Realizacja audytów bezpieczeństwa informacji.

Ostatnim kluczowym elementem zapewnienia skuteczności wdrożonego SZBI jest realizacja audytów bezpieczeństwa informacji. Gwarantuje ona zgodność z przepisami prawa oraz normami, a co najważniejsze pozwala zweryfikować faktyczny poziom bezpieczeństwa danych w szkołach, placówkach oświatowych czy JST.

Realizacja audytów bezpieczeństwa informacji we wskazanych jednostkach przynosi wiele korzyści, które mają bezpośredni wpływ na ochronę danych i skuteczność zarządzania bezpieczeństwem informacji. Przede wszystkim taka kontrola pozwala na dokładne zidentyfikowanie słabych punktów i potencjalnych zagrożeń, co umożliwia wczesne podjęcie działań korygujących i zapobiegawczych. Dzięki temu szkoły, przedszkola, placówki oświatowe i samorządowe mogą znacząco zwiększyć poziom ochrony danych osobowych uczniów, rodziców i pracowników. Taki mechanizm

jest szczególnie istotny w kontekście wymogów RODO i przepisów dotyczących bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa.

Audyt bezpieczeństwa informacji pomaga również w zapewnieniu zgodności ze stosowanymi normami i przyjętymi procedurami bezpieczeństwa, co jest ważne dla spełnienia zarówno wymagań prawnych, jak i minimalnych wyznaczników przypisanych systemom teleinformatycznym, które określono w KRI. Regularne kontrole umożliwiają bieżące monitorowanie i dostosowywanie procedur bezpieczeństwa do zmieniających się warunków i nowych zagrożeń, co zwiększa odporność placówek wobec ewentualnych incydentów zaburzających bezpieczeństwo zasobów cyfrowych.

Dzięki takim audytom poprawiana jest również efektywność zarządzania zabezpieczeniami IT, co przekłada się na lepszą ochronę infrastruktury teleinformatycznej i danych przed atakami cybernetycznymi. Ponadto specjalistyczne kontrole mogą zwiększać świadomość pracowników i uczniów na temat znaczenia bezpieczeństwa informacji oraz najlepszych praktyk w tym zakresie. Regularne szkolenia i edukacja w ramach audytów pomagają w jednostkach oświatowych i budżetowych w budowaniu kultury bezpieczeństwa. Tym samym obniżają ryzyko incydentów spowodowanych przez błędy ludzkie.

Warto też podkreślić, że – zgodnie z par. 20 ust. 2 pkt 14 rozporządzenia z dnia 12 kwietnia 2012 roku w sprawie KRI (Dziennik Ustaw z 2012 roku pozycja 526) oraz w świetle w art. 32 ogólnego rozporządzenia RODO – w aktualnym łańdźu prawnym audyt bezpieczeństwa informacji jest obowiązkowy zarówno w szkołach / placówkach oświatowych i samorządowych.

Ważne!

Przedstawione powyżej zadania stanowiły punkt wyjścia do opracowania arkuszy diagnostycznych w obszarze cyfryzacji oświaty.

- Arkusz do diagnozy wstępnej. Część 1. odnosi się do zadań 1–5.
- Arkusz do diagnozy wstępnej. Część 2. odnosi się do zadań 6–10 umożliwiających określenie stopnia wdrożenia narzędzi i rozwiązań zarządczych.
- Arkusz do diagnozy wstępnej. Część 3 odnosi się do zadań 1–10 dotyczących stosowania narzędzi personalnego rozwoju organizacji.

Diagnoza wstępna musi być przeprowadzona z wykorzystaniem wszystkich arkuszy stanowiących załącznik do niniejszego opracowania.

MATERIAŁ 3. PLANOWANIE STRATEGICZNE JST W OBSZARZE CYFROWEGO ROZWOJU OŚWIATY

Dorota Tomaszewicz

Ważne!

Materiał 3. stanowi – zarówno na etapie diagnozy wstępnej oraz pogłębionej, jak i w kontekście przygotowania Harmonogramu Działań Rozwojowych (dalej HDR) – wsparcie dla JST w zakresie planowania strategicznego. HDR pełni rolę niezwykle ważnego dokumentu, który jest ukierunkowany na rozwój cyfryzacji oświaty w JST w powiązaniu ze średnio i długookresowymi europejskimi oraz krajowymi pismami strategicznymi. Wzór HDR stanowi załącznik do niniejszego opracowania. Dodatkowo poleca się zapoznanie z planami działań rozwojowych w zakresie cyfryzacji oświaty, które zostały opracowane w pilotażu projektu HDR. Obecnie harmonogramy te są zamieszczonymi na stronie Ośrodka Rozwoju Edukacji (dalej ORE)¹⁷.

Wprowadzenie

Cyfryzacja edukacji stanowi jeden z kluczowych kierunków rozwoju społeczno-gospodarczego w Polsce i w całej Unii Europejskiej. Transformacja cyfrowa nie jest już wyłącznie odpowiedzią na wyzwania technologiczne, lecz staje się fundamentem budowania nowoczesnego społeczeństwa opartego na wiedzy i innowacjach. W tym kontekście szkoła, jako instytucja przygotowująca kolejne pokolenia do życia i pracy w zmieniającej się rzeczywistości, odgrywa szczególną rolę. Jej zadaniem jest nie tylko

¹⁷ Ośrodek Rozwoju Edukacji, (2025), „Harmonogramy działań rozwojowych w zakresie cyfryzacji oświaty w JST”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu.pl/2025/07/harmonogramy-dzialan-rozwojowych-w-zakresie-cyfryzacji-oswiaty-w-jst/> [dostęp, online dn. 2.09.2025].

zapewnienie dostępu do narzędzi i infrastruktury, lecz także kształtowanie kompetencji cyfrowych, które warunkują aktywne uczestnictwo w życiu zawodowym i społecznym.

Strategiczne dokumenty europejskie i krajowe wyznaczają kierunki działań w obszarze cyfryzacji, kładąc nacisk na rozwój infrastruktury, umiejętności cyfrowych oraz świadome i odpowiedzialne korzystanie z nowych technologii. W Polsce działania te znajdują swoje odzwierciedlenie w licznych programach i inicjatywach – od Ogólnopolskiej Sieci Edukacyjnej i programów szkoleniowych dla nauczycieli, po projekty wspierające samorządy w procesie transformacji cyfrowej.

Materiał ten stanowi próbę kompleksowego spojrzenia na proces cyfryzacji oświaty. Prezentuje on zarówno uwarunkowania strategiczne, jak i konkretne rozwiązania wspierające szkoły oraz jednostki samorządu terytorialnego w realizacji polityki cyfrowej. Celem publikacji jest nie tylko przybliżenie najważniejszych dokumentów i projektów, lecz także wskazanie, jak poprzez rozwój kompetencji przyszłości – w tym kompetencji cyfrowych – możliwe jest podniesienie jakości kształcenia, wzmocnienie kapitału ludzkiego i społecznego oraz budowanie konkurencyjnej, nowoczesnej gospodarki.

1. Kierunki rozwoju cyfryzacji oświaty a wytyczne strategicznych dokumentów europejskich i krajowych.

Rozwój cyfryzacji oświaty jest głównym elementem strategii zarówno na poziomie europejskim, jak i krajowym. Ramy strategiczne Unii Europejskiej (dalej UE) zawierają plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027. Główne kierunki działań dotyczą wspierania rozwoju ekosystemu edukacji cyfrowej, a w szczególności koncentrują się na tworzeniu infrastruktury i narzędzi wspierających nauczanie cyfrowe oraz rozwijaniu kompetencji w tym zakresie, promowania ich wśród uczniów i nauczycieli (w tym programowanie i cyberbezpieczeństwo). Do 2030 roku krajowa polityka cyfryzacji obszaru edukacji jest skoncentrowana na wzroście dostępności i jakości edukacji cyfrowej, rozwoju kompetencji cyfrowych wśród dzieci i młodzieży oraz kadry pedagogicznej.

Wśród głównych inicjatyw podejmowanych w ostatnich latach na rzecz rozwoju cyfryzacji oświaty są:

- Ogólnopolska Sieć Edukacyjna (dalej OSE) – program pozwalający szkołom, przedszkolom i placówkom oświatowym z całej Polski na dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Inicjatywa ta odpowiada na wyzwania współczesnej edukacji tj. podnoszenie poziomu cyfrowych kompetencji uczniów i otwarcie ich na nowe technologie. Ponadto OSE ma na celu wspomaganie procesu kształcenia w szkołach poprzez umożliwienie dostępu do zasobów edukacyjnych oraz promowanie zasad bezpiecznego korzystania z technologii cyfrowych¹⁸.
- „Lekcja:Enter” – program szkoleniowy dla nauczycieli w zakresie wykorzystania technologii cyfrowych w nauczaniu. Wspiera szkoły w dostosowaniu się do zmieniającego się świata. W ramach cykli szkoleniowych nauczyciele otrzymali pomoc w zakresie metod pracy na lekcji, tworzenia dla uczniów warunków pozwalających im na aktywne włączanie się w proces nauczania oraz uczenia się (m.in. dzięki wykorzystaniu technologii oraz ogólnodostępnych narzędzi cyfrowych)¹⁹.
- „Lekcja:AI” – program (realizowany przez Fundację Orange we współpracy z Fundacją Rozwoju Społeczeństwa Informacyjnego oraz firmą No Input Signal sp. z o.o.) ma na celu rozwój kompetencji nauczycieli w obszarze sztucznej inteligencji (dalej AI). Szkolenia przeprowadzane w ramach tego projektu są bezpłatne i obejmują trzy poziomy zaawansowania (począwszy od podstawowego, przez średni, aż po zaawansowany). Dzięki temu mogą być dopasowane do różnych potrzeb i stopnia przygotowania uczestników. Podczas kursów, które są prowadzonych zarówno online, jak i stacjonarnie, nauczyciele zdobywają wiedzę o mechanizmach funkcjonowania AI, jej codziennych zastosowaniach, a także o szansach i zagrożeniach związanych z rozwojem tej technologii. Istotnym elementem programu jest praktyczne wykorzystanie narzędzi AI w dydaktyce i życiu osobistym, a w modułach bardziej zaawansowanych uczestnicy przygotowują własne scenariusze lekcji lub projekty edukacyjne z wykorzystaniem tego narzędzia. Projekt kładzie również nacisk na kwestie społeczne i etyczne, ucząc świadomego i odpowiedzialnego podejścia do nowych technologii. Projekt „Lekcja:AI” stanowi więc ważny krok w kierunku modernizacji polskiej szkoły i przygotowania kadry

¹⁸ Ogólnopolska Sieć Edukacyjna, zob. <https://ose.gov.pl/> [dostęp, online, dn. 2.09.2025].

¹⁹ „Edukacja cyfrowa w szkołach”. Raport z badań prowadzonych w ramach projektu „Lekcja:Enter” (2021), Warszawa: Fundacja Orange, Fundacja Rozwoju Społeczeństwa, zob. <https://lekciaenter.pl/> [dostęp, online dn. 2.09.2025].

pedagogicznej do pracy w erze cyfrowej. Bowiemy wyposaża nauczycieli w wiedzę i praktyczne umiejętności, które pozwolą nie tylko efektywniej korzystać z narzędzi AI, ale także kształtować u uczniów postawy krytycznego, etycznego i twórczego wykorzystania nowatorskich rozwiązań technologicznych. Dzięki temu szkoła może lepiej odpowiadać na wyzwania współczesności i przygotowywać młodych ludzi do funkcjonowania w świecie, w którym AI odgrywa coraz większą rolę²⁰.

- Centrum Mistrzostwa Informatycznego (dalej CMI) – projekt, którego celem było podniesienie kompetencji kadry dydaktycznej (osób prowadzących zajęcia pozalekcyjne rozwijające zainteresowania informatyczne), a także aktywizacji młodzieży uzdolnionej informatycznie, pobudzania kreatywności oraz promowania współpracy zespołowej w ramach kół informatycznych. Projekt skierowany był do nauczycieli szkół podstawowych, ponadpodstawowych, nauczycieli akademickich oraz innych osób dorosłych wykazujących predyspozycje oraz zainteresowania do pracy z wybitnie uzdolnioną młodzieżą, czyli uczniami z klas IV–VI, klas VII–VIII szkół podstawowych, uczniami szkół średnich (w tym liceów ogólnokształcących i techników oraz szkół branżowych I i II stopnia)²¹.
- „Cyberbezpieczny Samorząd” – to projekt zwiększający poziom bezpieczeństwa informacji JST poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Grupą docelową programu są pracownicy administracji publicznej. Dzięki wsparciu grantowemu JST „Cyberbezpieczny Samorząd” umożliwi właściwym organom – w ramach swej organizacji – wdrożenie lub aktualizację SZBI, środków zarządzania ryzykiem w cyberbezpieczeństwie, mechanizmów i czynników zwiększających odporność na ataki z cyberprzestrzeni, podniesienia poziomu wiedzy i kompetencji personelu wdrożonego w urzędzie. Ponadto SZBI przykładą wiele uwagi do podniesienia poziomu wiedzy i kompetencji personelu samorządowego (wdrożonego w urzędzie), traktując te działania jako punkt wyjścia do uzyskania wyższego poziomu odporności na cyberzagrożenia²².
- Projekt „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST” stanowi kolejną inicjatywę w zakresie

²⁰ „Lekcja:AI.” Projekt bezpłatnych szkoleń o sztucznej inteligencji (2025), Warszawa: Fundacja Orange, Fundacja Rozwoju Społeczeństwa Informacyjnego, No Input Signal sp. z o.o., zob. <https://lekciaai.pl/> [dostęp, online dn. 2.09. 2025].

²¹ Centrum Mistrzostwa Informatycznego (CMI), zob. <https://cmi.edu.pl/> [dostęp, online, dn. 2.09. 2025].

²² Centrum Projektów Polska Cyfrowa (CPPC), NASK – Państwowy Instytut Badawczy, (2023), „Cyberbezpieczny samorząd”, NASK: Warszawa, zob. <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd2> [dostęp, online dn. 2.09.2025].

wsparcia organów samorządowych. Program ten jest realizowany przez ORE w Warszawie. Cel tej inicjatywy stanowi opracowanie koncepcji szkoleń i doradztwa wspomagającego JST w zarządzaniu cyfryzacją, a także ich przetestowanie. Projekt koncentruje się na wsparciu kadry samorządowej w procesie tworzenia warunków i wdrażania innowacyjnych rozwiązań strategicznych sprzyjających rozwojowi lokalnych systemów oświaty²³.

Obecnie odpowiedzi na to, w jakim kierunku podąża rozwój cyfryzacji edukacji, znajdują się w krajowych dokumentach strategicznych. Mają one służyć podejmowaniu i realizowaniu działań w celu zapewnienia trwałego i zrównoważonego rozwoju oraz zachowania spójności społeczno-gospodarczej i przestrzennej. Poniżej zilustrowano układ dokumentów strategicznych kraju.



Rysunek 1. Hierarchiczny układ dokumentów strategicznych kraju. Opracowanie własne.

Dokumenty strategiczne kraju są powiązane z dokumentami europejskimi i stanowią punktem wyjścia do planowania strategicznego na szczeblach: lokalnym, wojewódzkim, regionalnym i krajowym.

²³ „Cyfrowy rozwój oświaty w ramach samorządu terytorialnego”, (2023), op. cit.

Raport „Długookresowa Strategia Rozwoju Kraju. «Polska 2030. Trzecia Fala Nowoczesności» (URM z 5 lutego 2013 roku)”²⁴ składa się z dwóch części.

- **Pierwszą** stanowi wstęp wraz z diagnozą i opisem kontekstu społecznego, gospodarczego i międzynarodowego Strategii (w tym szkicu zaproponowano rozwiązania w trzech obszarach strategicznych), a także oraz prezentacja ram makroekonomicznych rozwoju Polski do 2030 roku.
- **Drugą** tworzy charakterystyka proponowanych kierunków interwencji (czyli działań wskazanych do podjęcia w perspektywie 2030 roku, które przyczyniają się do osiągnięcia celu głównego przyjętej strategii), a także opis zasad monitorowania i ewaluacji wdrażania projektu Polska 2030. Dokument ten wytycza podstawowe kierunki analizy i charakteryzuje zarówno warunki niezbędne dla rozwoju Polski w kluczowych obszarach na tle UE, jak i procesów gospodarczych zachodzących w świecie. W materiale tym określono trzy obszary zadaniowe. Poniżej na rysunku zilustrowano kluczowy cel ogólny i wspomniane obszary.

CEL GŁÓWNY: poprawa jakości życia Polaków (wzrost PKB na mieszkańca w relacji do najbogatszego państwa UE i zwiększenie spójności społecznej) dzięki stabilnemu, wysokiemu wzrostowi gospodarczemu, co pozwala na modernizację kraju

Makroekonomiczne warunki rozwoju Polski do 2030 roku

obszar konkurencyjności
i innowacyjności
gospodarki
(modernizacji)

Nastawiony na zbudowanie nowych przewag konkurencyjnych Polski opartych o wzrost KI (wzrost kapitału ludzkiego, społecznego, relacyjnego, strukturalnego) i wykorzystanie impetu cyfrowego, co daje w efekcie większą konkurencyjność

obszar równoważenia
potencjału rozwojowego
regionów (dyfuzji)

Zgodnie z zasadami rozbudzania potencjału rozwojowego odpowiednich obszarów mechanizmami dyfuzji i absorpcji oraz polityką spójności społecznej, co daje w efekcie zwiększenie potencjału konkurencyjności Polski

obszar efektywności
i sprawności państwa
(efektywności)

Usprawniający funkcje przyjaznego i pomocnego państwa (nie nadodpowiedzialnego) działającego efektywnie w kluczowych obszarach interwencji

Rysunek 2. Kluczowy cel ogólny oraz trzy obszary zadaniowe dla Polski 2030.

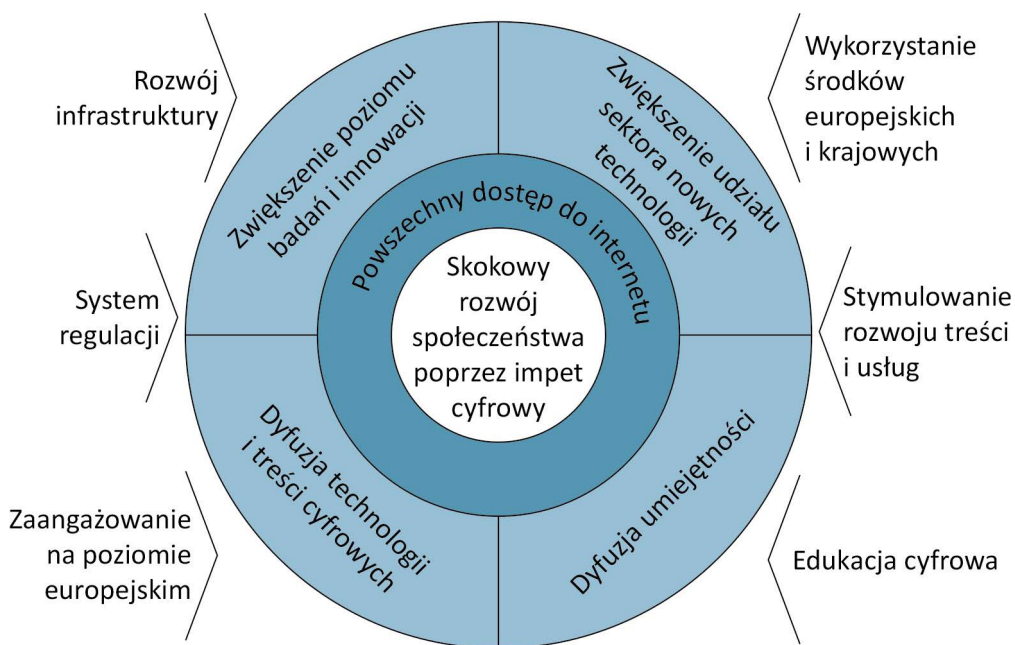
²⁴ Ministerstwo Cyfryzacji, (2013), „Długookresowa strategia Rozwoju Kraju. «Polska 2030. Trzecia fala nowoczesności»” (DSRK), Warszawa, zob. <https://mac.gov.pl/files/wp-content/uploads/2013/02/Strategia-DSRK-PL2030-RM.pdf> [dostęp, online dn. 2.09.2025].

Przywołanym trzem obszarom zadaniowym podporządkowano cele strategiczne oraz kierunki interwencji w podziale tematycznym. Co znalazło odzwierciedlenie poniżej.



Rysunek 3. Cele strategiczne i kierunki interwencji w odniesieniu do trzech obszarów zadaniowych – Polska 2030.

W dokumencie „**Długookresowa Strategia Rozwoju Kraju. «Polska 2030. Trzecia fala nowoczesności»**” podkreśla się wzajemne przenikanie się obszarów strategicznych. Poza tym zwrócono uwagę, że kluczem do poprawy konkurencyjności i innowacyjności gospodarki jest przejście od modelu społeczeństwa informacyjnego do społeczeństwa cyfrowego, a także wykorzystywanie nowych technologii w odniesieniu do wszystkich czynników rozwojowych. Strategia się dowodzi również, że cyfryzacja ma sens tylko jako podejście kompleksowe polegające na zwiększeniu dostępności do internetu oraz jego użytkowania poprzez rozwój i udostępnianie treści (zasobów publicznych) oraz zwiększenie kompetencji cyfrowych społeczeństwa. Opisuje się to jako świadome wykorzystanie impetu cyfrowego.



Rysunek 4. Dynamika cyfrowa niezbędna do rozwijania wszystkich czynników determinujących rozwój Polski.

Jednym z celów projektu „Długookresowa Strategia Rozwoju Kraju. «Polska 2030. Trzecia fala nowoczesności»” jest stworzenie Polski Cyfrowej poprzez podjęcie następujących kierunków interwencji:

- Wspieranie inwestycji w infrastrukturę szerokopasmową w celu zapewnienia powszechnego, wysokiej jakości dostępu do internetu.
- Budowanie kompetencji cyfrowych osób nauczających (m.in. nauczycieli, pracowników innych instytucji edukacyjnych i kultury, pracowników organizacji pozarządowych) i wdrożenie powszechnej edukacji cyfrowej oraz stworzenie nowoczesnej sieciowej infrastruktury i zasobów edukacyjnych.
- Zwiększenie ilości zasobów publicznych (m.in. zasobów edukacyjnych, zbiorów dziedzictwa, publikacji naukowych i treści mediów publicznych) dostępnych w sieci, w celu zapewnienia podaży treści wysokiej jakości.
- Stworzenie dogodnych warunków prawnych dla rozwoju rynku usług elektronicznych.
- Gromadzenie, przechowywanie, zabezpieczanie oraz udostępnianie danych i dokumentów elektronicznych oraz udostępnianie i zabezpieczanie w postaci

elektronicznej dotychczasowych zasobów w postaci tradycyjnej, w tym udostępnienie za pośrednictwem internetu treści objętych domeną publiczną.

Proponowane kierunki interwencji rozwoju Polski Cyfrowej mają znaczenie dla osiągnięcia pozostałych celów strategicznych związanych z kapitałem ludzkim, kapitałem społecznym oraz sprawnym państwem.

Kolejnym istotnym programem jest „**Strategia na rzecz Odpowiedzialnego Rozwoju kraju do roku 2020 (z perspektywą do 2030 roku)**”²⁵ (dalej SOR). Określa ona nowy model rozwoju – suwerenną wizję strategiczną, zasady, cele i priorytety rozwoju kraju w wymiarze gospodarczym, społecznym i przestrzennym do 2020 roku oraz w perspektywie do 2030 roku. Ze względu na swoją rolę i przypisane jej zadania Strategia stanowi instrument elastycznego zarządzania głównymi procesami rozwojowymi w kraju.

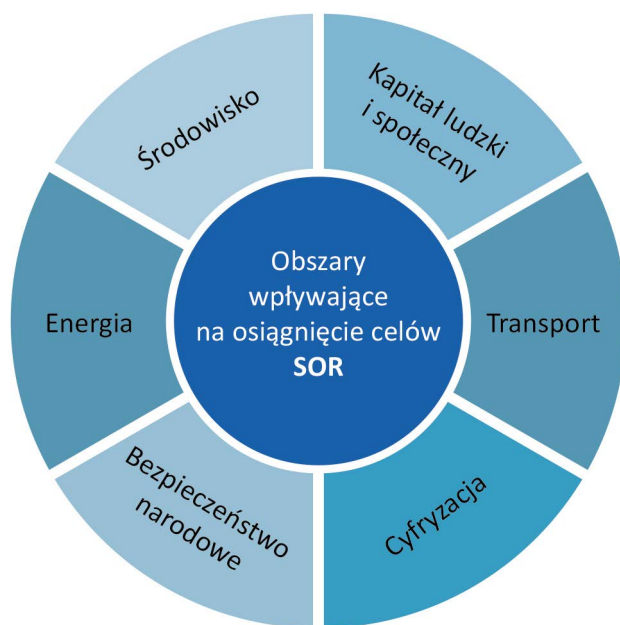
SOR jest aktualizacją średniookresowej procedury rozwoju kraju („Strategii Rozwoju Kraju 2020”), która została przyjęta uchwałą Rady Ministrów 25 września 2012 roku, zgodnie z wymogami ustawy z dnia 6 grudnia 2006 roku o zasadach prowadzenia polityki rozwoju. Ten plan gospodarczy stanowi jednocześnie podstawę do określenia nowego systemu dokumentów strategicznych, który zostanie zaprezentowany w zaktualizowanym systemie zarządzania rozwojem Polski oraz znajdzie odzwierciedlenie w nowelizacji ustawy z dnia 6 grudnia 2006 roku o zasadach prowadzenia polityki rozwoju. SOR wyznacza jednocześnie zakres aktualizacji obowiązujących procedur (w tym dziewięć strategii zintegrowanych) i programów oraz innych dokumentów wdrożeniowych, zgodnie z przyjętą koncepcją rozwojową. Głównym celem SOR jest tworzenie warunków dla wzrostu dochodów mieszkańców Polski, przy jednoczesnym wzroście spójności w wymiarze społecznym, ekonomicznym środowiskowym i terytorialnym. W dokumencie tym określono trzy cele szczegółowe:

- **Pierwszy cel szczegółowy** obejmuje trwały wzrost gospodarczy oparty coraz silniej na wiedzy, danych i doskonałości organizacyjnej.
- **Drugi cel szczegółowy** stanowi rozwój społecznie wrażliwy i terytorialnie zrównoważony.

²⁵ Uchwała nr 8 Rady Ministrów z dnia 14 lutego 2017 roku w sprawie przyjęcia „Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 roku)”, zob. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20170000260> [dostęp, online dn. 2.09.2025].

- **Trzeci cel szczegółowy** koncentruje się na budowaniu skutecznego państwa oraz instytucji służących zarówno wzrostowi, jak i włączeniu społecznemu, a także gospodarstwu.

W SOR określono również główne obszary koncentracji działań w obrębie poszczególnych celów szczegółowych. Ponadto scharakteryzowano obszary wpływające na osiągnięcie celów przyjętej strategii. Obszary te obrazuje poniższy rysunek.



Rysunek 5. Obszary wpływające na osiągnięcie celu głównego i celów szczegółowych SOR.

Wśród obszarów wpływających na osiągnięcie celów SOR znajdują się zarówno kapitał ludzki i społeczny, jak i cyfryzacja. Przez kapitał ludzki należy rozumieć zasób wiedzy, umiejętności oraz potencjał zawarty w każdym człowieku i w społeczeństwie jako całości. Ponadto ta teoria ekonomiczna określa zdolności do pracy, adaptowania się do zmian w otoczeniu oraz możliwości tworzenia nowych rozwiązań. W perspektywie SOR kluczowym pojęciem dla rozwoju kapitału ludzkiego są umiejętności jednostek i grup społecznych. W badaniu ewaluacyjnym „Diagnoza społeczna. Analiza kwalifikacji i kompetencji kluczowych dla zwiększenia szans absolwentów na rynku pracy”, będącego wnikliwym

badaniem nad stanem kapitału ludzkiego w Polsce, główną rolę przypisano rozwojowi i wzmocnieniu wybranych umiejętności. Raport ten wskazuje na następujące rodzaje umiejętności:

- **Umiejętności uniwersalne** pozwalają na pełnienie funkcji, ról społecznych i zawodowych w różnych kontekstach, które są niezależne od danego sektora, branży czy zawodu. Umiejętności te są wykorzystywane w różnych sytuacjach (np. kompetencje językowe, komunikacyjne, przedsiębiorczość).
- **Umiejętności cyfrowe** są niezbędne do funkcjonowania we współczesnym świecie bez względu na wiek czy sprawność fizyczną, pozwalają na poznawanie treści cyfrowych i ocenę ich wiarygodności, użycie ich w życiu codziennym, rozszerzanie bazy popytowej dla e-usług świadczonych przez podmioty publiczne i gospodarcze. Kompetencje te tym samym przyczyniają się do rozwoju gospodarczego i realizacji celów SOR.
- **Umiejętności zawodowe** są pożądane, ponieważ brak wykwalifikowanych pracowników może uniemożliwić lub utrudnić rozwój w priorytetowych sektorach gospodarki i znaczących dla kraju branżach.

Wyzwaniem dla rozwoju społeczno-gospodarczego kraju jest niski poziom kapitału społecznego w Polsce (tzw. kapitału pomostowego) jako czynnika tworzącego dodatkowe koszty związane z ograniczonym zaufaniem na linii państwo – obywatel. Dla wzmocnienia roli dialogu społecznego i obywatelskiego szczególnie istotne jest szeroko rozumiane partnerstwo pomiędzy instytucjami administracji publicznej i organizacjami pozarządowymi, oparte na wzajemnym zaufaniu i współpracy. Z jednej strony będzie ono wzmocniać potencjał państwa, a z drugiej rozwijać kapitał społeczny. Czynnikiem odgrywającymi kluczową rolę w tym zakresie są: kultura współpracy, kreatywność, tolerancja, zaufanie, gotowość do tworzenia zinstytucjonalizowanych i niesformalizowanych sieci współpracy oraz partnerstwa pomiędzy różnymi podmiotami życia publicznego. Kolejny znaczący obszar stanowi cyfryzacja, ponieważ gospodarka wchodzi obecnie w etap czwartej rewolucji przemysłowej (tzw. „Przemysłu 4.0”), która opiera się na nowoczesnych sieciach telekomunikacyjnych (stacjonarnych i mobilnych), bez których nie ma szansy na dalszy rozwój technologii cyfrowej, innowacyjności, przyspieszenia gospodarki czy zwiększenia efektywności wykorzystania zasobów. Rozwój technologii informacyjno-

-komunikacyjnych (dalej ICT) stymuluje dynamiczny rozwój i wnosi nową wartość we wszystkich segmentach gospodarki (w przemyśle, energetyce, administracji publicznej,

edukacji, ochronie zdrowia, inteligentnych miast, budynków i pojazdów, transporcie i logistyce, rolnictwie, bankowości). Dynamika zmian w otaczającym świecie wymusza zmiany tradycyjnych modeli nauczania. Obecnie wiedza i kompetencje nabyte w procesie edukacji dezaktualizują się w szybkim tempie. Dlatego też Polska potrzebuje takiego modelu nauki, który umożliwia ciągłą aktualizację wiedzy i dostosowanie jej do potrzeb rynku pracy. Wyzwaniem dla naszego kraju – już na etapie szkoły podstawowej – jest więc budowa cyfrowego systemu edukacyjnego. SOR zakłada przejście do koncepcji gospodarki opartej na wiedzy. Nie będzie to jednak możliwe bez wykorzystania kompetencji cyfrowych, które w XXI wieku będą stanowić o przewadze konkurencyjnej Polski na tle innych krajów.

Wśród dokumentów strategicznych odnajdziemy również **„Krajową Strategię Rozwoju Regionalnego 2030”**²⁶ (dalej KSRR 2030). Głównym jej celem jest efektywne wykorzystanie wewnętrznych potencjałów terytoriów i ich specjalizacji dla osiągnięcia zrównoważonego rozwoju naszego państwa. Co w dalszej konsekwencji przyczyni się do wzrostu dochodów mieszkańców Polski przy jednoczesnym osiągnięciu spójności w wymiarze społecznym, gospodarczym, środowiskowym i przestrzennym. Dookreśla to drugi cel szczegółowy SOR – Rozwój społecznie wrażliwy i terytorialnie zrównoważony. Do 2030 roku głównym dążeniem polityki regionalnej będzie – realizowany na podstawie trzech uzupełniających się celów szczegółowych – zwiększenie spójności rozwoju kraju w wymiarze społecznym, gospodarczym, środowiskowym i przestrzennym, wzmacnianie regionalnych przewag konkurencyjnych, a także podniesienie jakości zarządzania i wdrażania polityk ukierunkowanych terytorialnie. W SKRR uznano, że cyfryzacja jest podstawowym czynnikiem stymulującym dostęp obywateli do usług wraz z płynącymi z nich korzyściami natury ekonomiczno-społecznej. Strategia wyznacza wobec tego kierunki rozwoju i modernizacji infrastruktury teleinformatycznej i telekomunikacyjnej, a także zakłada stworzenie nowoczesnej infrastruktury łączności elektronicznej przy wdrożeniu bezprzewodowych sieci nowej generacji (technologia 5G). Ponadto KSRR określa zadania do wykonania w ramach dalszej informatyzacji gospodarki oraz zwiększenia przepustowości sieci. Strategia ta – w ramach wzmocnienia szans rozwojowych obszarów zagrożonych trwałą marginalizacją – jako priorytet dąży do zapewnienia jak największej grupie

²⁶ Ministerstwo Funduszy i Polityki Realnej (2019), „Krajowa Strategia Rozwoju Regionalnego”, Warszawa, zob. Krajowa Strategia Rozwoju Regionalnego - Ministerstwo Funduszy i Polityki Regionalnej - Portal Gov.pl [dostęp, online dn. 2.09.2025].

odbiorców szerokopasmowego dostępu do internetu W odniesieniu do wyzwania, jakim jest zapewnienie kadry dla nowoczesnej gospodarki, główne dążenie stanowić będzie zwiększenie liczby osób posiadających podstawowe umiejętności cyfrowe. Edukacja w tym zakresie ma umożliwić obywatelom korzystanie z nowych rozwiązań informatycznych ułatwiających realizację procedur administracyjnych, a przedsiębiorcom pozyskiwanie pracowników gotowych do działania w nowych realiach gospodarczych.

W przywołanych dokumentach strategicznych kraju szczególną uwagę zwraca się na aspekt cyfryzacji, w tym rozwijania kompetencji cyfrowych obywateli. „Dziewięć zintegrowanych strategii rozwoju kraju”²⁷ uszczegóławiających SOR potwierdza wagę zagadnienia i doprecyzowuje zakres działań w tym zakresie.



Rysunek 6. Dziewięć zintegrowanych strategii rozwoju kraju.

Dla przykładu w „Strategii Rozwoju Kapitału Ludzkiego 2030” odnajdujemy cztery cele szczegółowe. Pierwszy z nich mówi wprost o podniesieniu poziomu kompetencji oraz kwalifikacji obywateli (w tym umiejętności cyfrowych). Wśród opisanych kierunków interwencji przedstawiono działania ukierunkowane na technologie cyfrowe w zakresie rozwoju potencjału ludzkiego. Oto kilka z nich:

²⁷ Ministerstwo Funduszy i Polityki Realnej (2020), „Czym jest zarządzanie rozwojem”, Warszawa, zob. <https://www.gov.pl/web/fundusze-regiony/czym-jest-zarzadzanie-rozwojem> [dostęp, online dn. 2.09.2025].

- dostarczanie usług publicznych z wykorzystaniem nowoczesnych technologii informacyjnych;
- zapewnienie wyposażenia i infrastruktury dla doskonalenia systemu edukacji;
- podnoszenie kompetencji technologicznych w zakresie TIK wśród uczniów i nauczycieli;
- prowadzenie kampanii edukacyjno-informacyjnych na rzecz upowszechnienia korzyści z wykorzystania technologii cyfrowych.

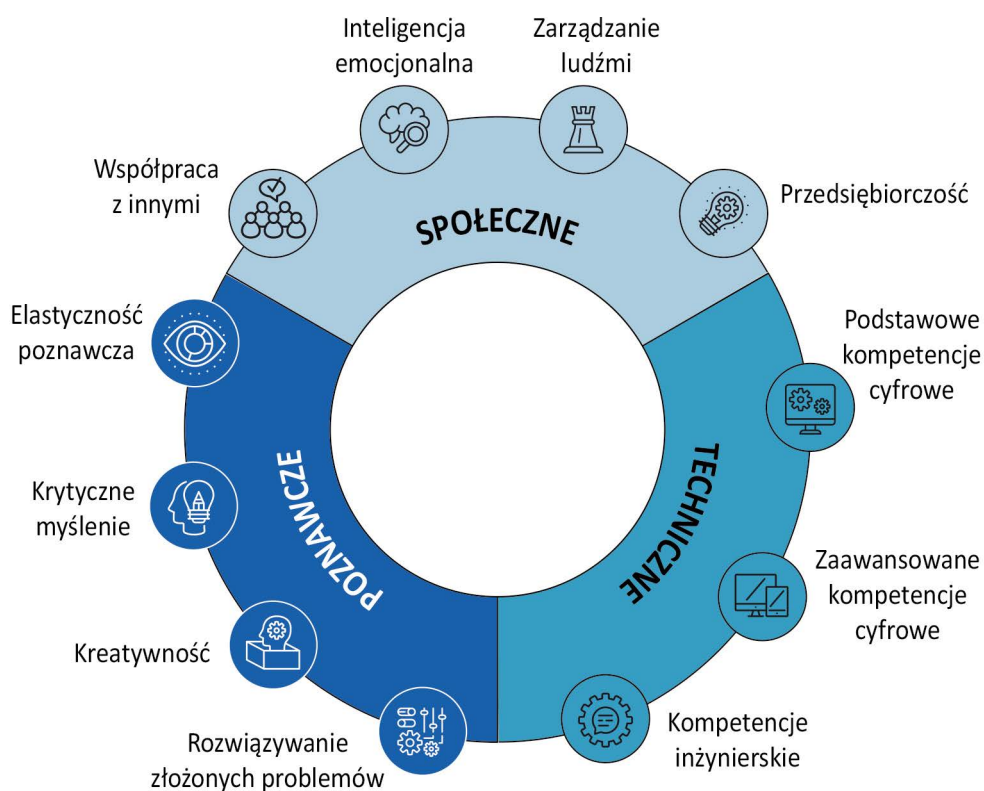
Natomiast w SRKS podkreśla się, że digitalizacja, cyfrowa rekonstrukcja i udostępnianie zbiorów dziedzictwa kulturowego za pomocą Internetu należą do najważniejszych przedsięwzięć prowadzących do rozwoju kultury cyfrowej w Polsce.

2. Kierunek rozwoju kompetencji przyszłości ze szczególnym uwzględnieniem kompetencji cyfrowych.

Na kompetencje przyszłości składają się umiejętności, które w nadchodzących latach będą szczególnie cenione na rynku pracy. W obliczu dynamicznych zmian technologicznych i społecznych te kompetencje stają się priorytetowe dla osiągnięcia sukcesu zawodowego i osobistego.

Do kompetencji przyszłości zalicza się:

- kompetencje techniczne (tworzą podstawowe i zaawansowane umiejętności cyfrowe oraz umiejętności inżynierskie);
- kompetencje poznawcze (pozwalające na rozwiązywanie złożonych problemów, kreatywność, myślenie krytyczne, elastyczność poznawcza);
- kompetencje społeczne (obejmują komunikację i kooperację, inteligencję emocjonalną, zarządzanie ludźmi, przedsiębiorczość);
- postawy ułatwiające funkcjonowanie w warunkach przyspieszonej zmiany społecznej i gospodarczej (w tym elastyczność, wytrzymałość oraz nastawienie na uczenie się przez całe życie).



Rysunek 7. Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne²⁸.

W obecnych czasach każdy człowiek potrzebuje – rozwijanych w perspektywie uczenia się przez całe życie – kompetencji kluczowych, które stanowią dynamiczną kombinację wiedzy, umiejętności i postaw. Są one niezbędne do samorealizacji i rozwoju osobistego, zatrudnienia, włączenia społecznego czy satysfakcjonującego życia. Do **kompetencji kluczowych** Rada Europejska – na podstawie „Zalecenia z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie” – zalicza:

- kompetencje w zakresie doboru i tworzenia informacji w języku ojczystym i językach obcych;
- umiejętności matematyczne, przyrodnicze i cyfrowe;
- kompetencje osobiste, społeczne i obywatelskie;

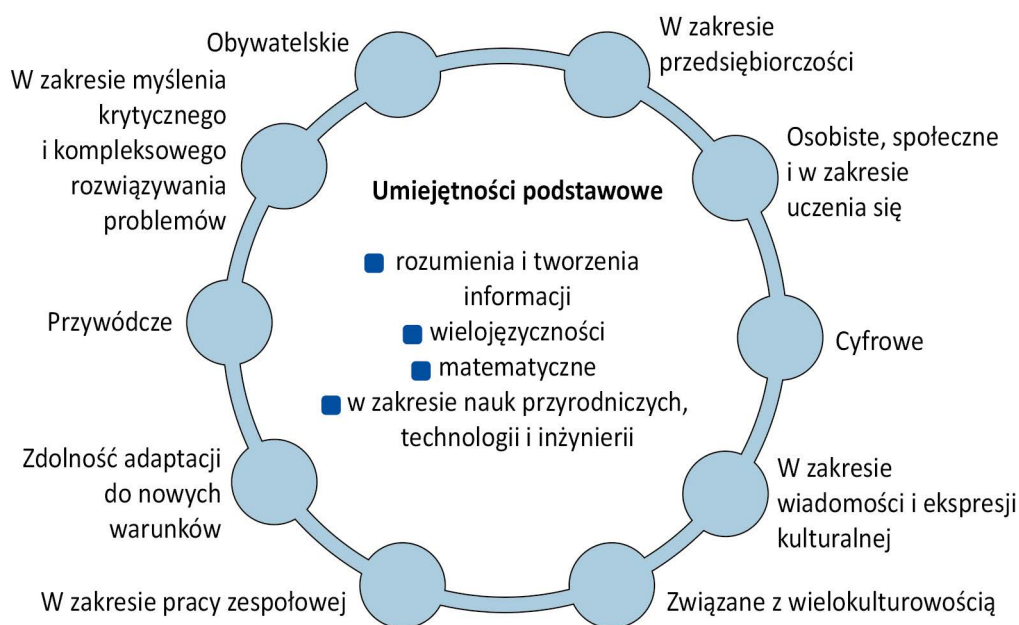
²⁸ Śledziewska K., Włoch R., (2019), „Kompetencje przyszłości. Jak je kształtować w elastycznym ekosystemie edukacyjnym”, Warszawa: DELab Uniwersytet Warszawski, zob. <https://delab.uw.edu.pl/raporty/kompetencje-przyszlosci-jak-je-ksztaltowac-w-elastycznym-ekosystemie-edukacyjnym/> [dostęp, online dn. 2.09.2025].

- umiejętności w zakresie przedsiębiorczości oraz świadomości i ekspresji kulturalnej²⁹).

W przywołanym dokumencie Komisja Europejska (dalej KE) w ramach kompetencji kluczowych wyróżnia także dwa inne typy:

- Umiejętności podstawowe – mające zastosowanie w wielu zawodach. Te kompetencje zwiększają wydajność pracowników, pozwalają osobom poszukującym pracy ubiegać się o stanowiska u większej liczby pracodawców, a więc tym samym poprawiają szansę na zdobycie zatrudnienia. Umiejętności podstawowe stanowią także punkt wyjścia do rozwijania pozostałych kompetencji. Dzięki swojej uniwersalności ułatwiają funkcjonowanie w warunkach niepewności, w których dynamiczne zmiany technologiczne skutkują szybkimi modyfikacjami standardów kwalifikacji i kompetencji zawodowych.
- Umiejętności przekrojowe obejmują także kompetencje cyfrowe rozumiane jako:
 - » pewne, krytyczne i odpowiedzialne korzystanie z technologii informatycznych, a także interesowanie się nimi w celach edukacyjnych, zawodowych i społecznych;
 - » zdolność korzystania z informacji i danych, komunikowanie się i współpraca, biegłość w korzystaniu z mediów, tworzenie treści cyfrowych (w tym programowanie);
 - » bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem);
 - » kwestie dotyczące własności intelektualnej, rozwiązywanie problemów i krytyczne myślenie.

²⁹ Rada Europejska, (2018), „Zalecenie Rady z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie”, „Dziennik Urzędowy Unii Europejskiej” nr 2018/C 189/01, zob. <https://op.europa.eu/pl/publication-detail/-/publication/6fda126a-67c9-11e8-ab9c-01aa75ed71a1> [dostęp, online dn. 2.09.2025].



Rysunek 8. Umiejętności podstawowe i przekrojowe (ZSU 2030)³⁰.

„Zintegrowana Strategia Umiejętności 2030 (dalej ZSU 2030)” wpisuje się w SOR, a także uzupełnia i rozwija cele oraz kierunki działań projektowane w „Strategii Rozwoju Kapitału Ludzkiego 2020 (z perspektywą do 2030 roku)”, nawiązując również do pozostałych ośmiu horyzontalnych zintegrowanych strategii rozwoju.

W związku z tym, że działania na rzecz tworzenia i realizacji programów wspierających rozwój cyfryzacji w Polsce (w tym rozwijania kompetencji cyfrowych) są podejmowane przez różne podmioty (np. resorty, ministerstwa, organizacje, instytucje), dlatego moment obecnie nie ma jednego wiodącego lidera koordynującego prace w tym zakresie. Tym bardziej warto zwrócić uwagę na proponowane rozwiązania i podejmowane działania przez Ministerstwo Cyfryzacji³¹. Na stronie tego resortu znajduje się definicja kompetencji cyfrowych: „Uznajemy, że kompetencje cyfrowe to harmonijna kompozycja wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym, tj. społeczeństwie wykorzystującym w życiu codziennym i pracy technologie cyfrowe.

³⁰ Ministerstwo Edukacji Narodowej. Departament Innowacji i Rozwoju, (2020), „Zintegrowana Strategia Umiejętności 2030”, zob. <https://zsu2030.mein.gov.pl/#zu> [dostęp, online dn. 2.09.2025].

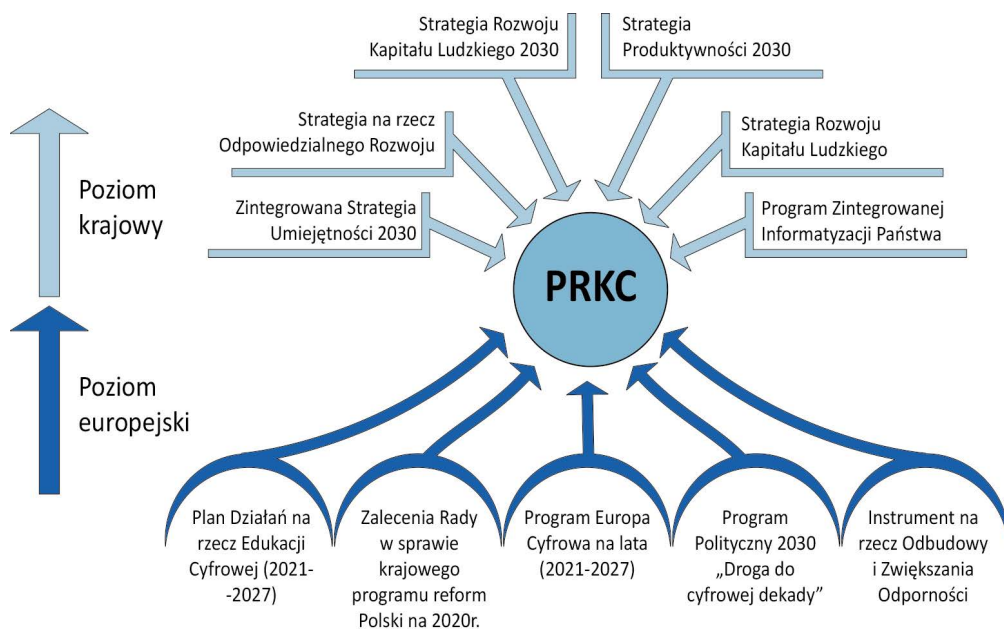
³¹ Ministerstwo Cyfryzacji, (2025), „Cyfryzacja”, Warszawa, zob. <https://www.gov.pl/web/cyfryzacja> [dostęp, online dn. 2.09.2025].

Wiemy, że w skład tych umiejętności wchodzi:

- kompetencje informatyczne obejmujące posługiwanie się komputerem i innymi urządzeniami elektronicznymi, bezpieczne korzystanie z internetu, aplikacji i oprogramowania, nowych inteligentnych technologii cyfrowych oraz umiejętność stosowania metod pochodzących z informatyki przy programowaniu i tworzeniu rozwiązań informatycznych dla problemów z różnych dziedzin (myślenie komputacyjne);
- kompetencje informacyjno-komunikacyjne polegające na umiejętności wyszukiwania informacji, rozumienia jej, a także selekcji i oceny krytycznej, jak również komunikowania się na odległość za pomocą technologii cyfrowych;
- kompetencje funkcjonalne, czyli realne wykorzystanie powyższych kompetencji w różnych sferach codziennego życia (np. finansach, pracy i rozwoju zawodowym, utrzymywaniu relacji, zdrowiu, hobby, zaangażowaniu obywatelskiemu, życiu duchowemu) zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych”.

Ważnym krokiem wspierającym działania na rzecz rozwoju cyfryzacji (w tym rozwoju kompetencji cyfrowych) było przeprowadzenie diagnozy sytuacji w obszarze kompetencji cyfrowych w Polsce, analizowanie występujących trendów cyfryzacyjnych, a także problemów i wyzwań kraju oraz Europy. Wiele dokumentów strategicznych (zarówno krajowych jak i europejskich) oraz wyniki przeprowadzonej diagnozy stanowiły podstawę do opracowania **„Programu Rozwoju Kompetencji Cyfrowych”³²** (dalej PRKC). Jego celem jest stały wzrost poziomu kompetencji cyfrowych przez **zapewnienie każdemu w Polsce możliwości ich rozwoju stosownie do potrzeb.**

³² Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 roku w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych” (Dziennik Ustaw z dnia 30 marca 2023 roku pozycja 318), zob. <https://eli.gov.pl/eli/MP/2023/318/ogl> [dostęp, online dn. 2.09.2025].



Rysunek 9. Kluczowe dokumenty strategiczne na poziomie krajowym i unijnym uwzględnione w PRKC.

Przygotowanie PRKC poprzedziły liczne spotkania i warsztaty z wieloma interesariuszami i ekspertami działającymi na rzecz rozwoju kompetencji cyfrowych. Projekt Programu został przekazany w III kwartale 2022 roku do konsultacji publicznych, opiniowania, a także dwukrotnie do konsultacji międzyresortowych. Zamyśl PRKC uzyskał pozytywną opinię Komisji Wspólnej Rządu i Samorządu Terytorialnego oraz Komitetu Rady Ministrów do spraw Cyfryzacji. Następnie 21 lutego 2023 roku Rada Ministrów przyjęła uchwałę w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych”³³. Ten projekt w ramach swoich kompleksowych założeń przewiduje rozwój powszechnych kompetencji cyfrowych wśród obywateli, począwszy od etapu edukacji przedszkolnej i wczesnoszkolnej do wieku senioralnego. Wsparcie w ramach PRKC będzie kierowane do wszystkich pragnących podnosić swoje kompetencje cyfrowe (w tym do nauczycieli, przedsiębiorców, pracowników wszystkich sektorów gospodarki oraz urzędników, jak również osób utalentowanych cyfrowo, które zasilą w przyszłości zasób specjalistów ICT o najwyższych kompetencjach). Równolegle zaplanowano działania na rzecz integracji cyfrowej. Mają one likwidować wykluczenie cyfrowe poprzez propagowanie i zwiększenie dostępności cyfrowych

³³ Zob. <https://www.dziennikustaw.gov.pl/MP/2023/318> [dostęp, online dn. 2.09.2025].

stron internetowych i aplikacji mobilnych dla osób z niepełnosprawnościami. W programie tym znajdują się również inicjatywy mające na celu zwiększenie świadomości dotyczącej korzystania z technologii cyfrowych oraz propagowanie higieny cyfrowej. W PRKC wyróżniono cztery priorytety. W ramach każdego z nich opracowano zadania wyznaczające obszar interwencji przewidzianych do realizacji działań i projektów.

Priorytet I	Wzmocnienie zarządzania rozwojem kompetencji cyfrowych
Realizacja wskazanego priorytetu ma zapewnić systemowe podejście do rozwoju kompetencji cyfrowych w Polsce, które w szczególności wzmocni: koordynację działań na rzecz realizacji PRKC, monitorowanie realizacji PRKC i rozwoju kompetencji cyfrowych w naszym kraju, współdziałanie administracji na poziomie centralnym i regionalnym, współpracę międzysektorową między administracją publiczną, biznesem oraz organizacjami pozarządowymi, a także współtworzenie i współdzielenie wiedzy, dobrych praktyk i zasobów edukacyjnych.	
Priorytet II	Rozwój edukacji cyfrowej
Realizacja wskazanego priorytetu ma zapewnić na wszystkich etapach kształcenia systemowe podejście do rozwijania kompetencji cyfrowych oraz wykorzystania zasobów i narzędzi w dydaktyce. Ten priorytet opiera się na wzmocnieniu kompetencji w zakresie dydaktyki cyfrowej nauczycieli, nauczycieli akademickich i umiejętności pracowników Klubów Rozwoju Cyfrowego (jako edukatorów cyfrowych), a także kompetencji cyfrowych studentów stosownie do kierunku kształcenia i wybranej ścieżki kariery.	
Priorytet III	Zapewnienie każdemu możliwości rozwoju kompetencji cyfrowych
Realizacja tego priorytetu ma zapewnić dostęp do informacji, poradnictwa i szkoleń dla wszystkich, którzy chcą zbudować lub podnieść swoje kompetencje cyfrowe w Klubach Rozwoju Cyfrowego, czyli lokalnych placówkach zorganizowanych w gminach na bazie istniejących instytucji, np. bibliotek publicznych, Lokalnych Ośrodków Wiedzy i Edukacji (dalej LOWE), szkół lub innych instytucji kultury, edukacji lub kształcenia ustawicznego, centr usług społecznych, uniwersytetów ludowych, kół gospodyń wiejskich lub podmiotów systemu nauki i szkolnictwa wyższego. Działania promocyjne mają przyczynić się do wzrostu zainteresowania rozwojem kompetencji cyfrowych wśród osób dorosłych, aktywizacji cyfrowej sektora małych i średnich przedsiębiorstw (dalej MŚP) oraz wzmacniania postaw procyfrowych w administracji publicznej. Tym samym ma to prowadzić do ograniczenia wykluczenia cyfrowego związanego zarówno z deficytem motywacji do korzystania z technologii cyfrowych, jak i z brakiem umiejętności w tym zakresie.	

Priorytet IV	Wsparcie kompetencji cyfrowych na rynku pracy
Realizacja wskazanego priorytetu ma zapewnić adekwatny do potrzeb napływ pracowników o oczekiwanych kompetencjach cyfrowych. Sytuacja ta przyczyni się zarówno do wzrostu wydajności pracy w Polsce, jak i konkurencyjności na rynku pracy, a w dalszej konsekwencji wpłynie pozytywnie na jakość życia. Ma to również spowodować większe wykorzystanie technologii cyfrowych w sektorze MŚP, a w konsekwencji przyczynić się do wzrostu konkurencyjności polskiej gospodarki. Zakłada się również wzrost kompetencji cyfrowych pracowników instytucji publicznych, a tym samym poprawę jakości usług e-administracji oraz ich cyfrową dostępność dla osób z niepełnosprawnościami. Rynek pracy ma wzbogacić się o nowy zasób dobrze wykształconych specjalistów ICT, którzy są potrzebni we wszystkich branżach gospodarki.	

Z kolei na stronie MEN³⁴ znajdują się informacje o jednym z kamieni milowych Krajowego Planu Odbudowy, czyli o przyjęciu przez Radę Ministrów uchwały w sprawie polityki cyfryzacji obszaru edukacji. Rozporządzenie ma charakter dokumentu programowego i strategicznego o nazwie „Polityka Cyfrowej Transformacji Edukacji” (dalej PCTE), stanowi podstawę do zmian w systemie edukacji i realizacji inwestycji w nowe technologie. Ponadto określała kierunki cyfryzacji systemu edukacji w perspektywie krótko- i długoterminowej.

Myślą przewodnią PCTE jest **Dekalog cyfrowej transformacji edukacji skoncentrowany wokół następujących zagadnień:**

- I. Ewaluacja stanu edukacji cyfrowej.
- II. Rewizja obowiązującej podstawy programowej.
- III. Wpływ nowych technologii (w tym AI) na szkołę.
- IV. Metody kształcenia, dydaktyka informatyki, dydaktyka cyfrowa.
- V. Kształcenie i doskonalenie nauczycieli.
- VI. Wyposażenie uczniów, nauczycieli i szkół.
- VII. Kształcenie cyfrowych specjalistów.
- VIII. Cyfrowe bezpieczeństwo.
- IX. Zmiana organizacji pracy szkoły.
- X. Koordynacja realizacji nakreślonych celów.

³⁴ Uchwała nr 98 Rady Ministrów z dnia 12 września 2024 roku w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji” (Dziennik Ustaw z dnia 17 września 2024 roku), pozycja 812, zob. <https://dziennikustaw.gov.pl/M2024000081201.pdf> [dostęp, online dn. 2.09.2025].

3. Ramy kompetencji cyfrowych dla obywateli o różnym poziomie zaawansowania. Przykładowe narzędzia do samooceny kompetencji informatycznych w obszarze cyfryzacji oświaty.

DigComp³⁵ – Ramy kompetencji cyfrowych dla obywateli

Europejskie „Ramy kompetencji cyfrowych dla obywateli” (dalej DigComp 2.0) są narzędziem stworzonym w celu poprawy kompetencji cyfrowych obywateli. Zostało ono opracowane przez Wspólne Centrum Badawcze KE i po raz pierwszy opublikowane w 2013 roku, a następnie zaktualizowane w 2016 roku. Obecnie obowiązuje nowa wersja – jest nią DigComp 2.2 – która została wydana przez KE – Wspólne Centrum Badawcze – © Unia Europejska, 2022, a jej autorami są: Riina Vuorikari, Stefano Kluzera, Yves Punie. To narzędzie rozwoju kompetencji cyfrowych zawiera nowe przykłady wiedzy, umiejętności i postaw. DigComp 2.2 składa się z 21 kompetencji podzielonych na pięć obszarów obejmujących różne aspekty korzystania z technologii cyfrowych. Pierwsze trzy obszary dotyczą umiejętności, które można powiązać z określonymi działaniami i zastosowaniami. Z drugiej strony obszary czwarty i piąty (Bezpieczeństwo i rozwiązywanie problemów) są „przekrojowe”, ponieważ dotyczą każdego rodzaju działalności prowadzonej za pomocą środków cyfrowych. W szczególności elementy rozwiązywania problemów są obecne we wszystkich kompetencjach, ale zdefiniowano konkretny obszar, aby podkreślić znaczenie tego aspektu przy korzystaniu z technologii i praktyk cyfrowych.

Poniżej zamieszczono charakterystykę każdego obszaru (wymiar 1) uzupełnionego o opisane kompetencje (wymiar 2).

³⁵ Vuorikari R., Kluzer S., Punie Y., (2022), „DigComp 2.2. Ramy kompetencji cyfrowych dla obywateli – nowe przykłady wiedzy, umiejętności i postaw”, Luksemburg: Urząd Publikacji Unii Europejskiej, zob. <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415> [dostęp, online dn. 2.09.2025].

Obszar 1. Umiejętność korzystania z informacji i z danych:

- 1) **Przeglądanie, wyszukiwanie i filtrowanie danych, informacji i treści cyfrowych.** Umiejętność skutecznego wyszukiwania informacji w internecie oraz filtrowania wyników. Tworzenie i aktualizowanie własnych strategii wyszukiwania.
- 2) **Ocena danych, informacji i treści cyfrowych.** Umiejętność oceny wiarygodności i jakości informacji, źródeł danych i treści cyfrowych. Analiza, interpretacja i krytyczna ocena danych, informacji i treści cyfrowych.
- 3) **Zarządzanie danymi, informacjami i treściami cyfrowymi.** Umiejętność organizowania, przechowywania i odzyskiwania danych, informacji i treści w środowisku cyfrowym.

Obszar 2. Komunikacja i współpraca:

- 1) **Komunikacja z wykorzystaniem technologii cyfrowych.** Umiejętność komunikowania się za pomocą różnych narzędzi cyfrowych (e-mail, komunikatory, media społecznościowe).
- 2) **Dzielenie się informacjami i zasobami z wykorzystaniem technologii cyfrowych.** Umiejętność dzielenia się z innymi – przy użyciu odpowiednich narzędzi informatycznych – informacjami i treściami cyfrowymi, a także w zakresie stosowania odnośników i przypisów.
- 3) **Aktywność obywatelska z wykorzystaniem technologii cyfrowych:** Uczestniczenie w życiu społecznym poprzez wykorzystanie publicznych i prywatnych usług cyfrowych. Poszukiwanie możliwości usamodzielnienia się i działań obywatelskich poprzez odpowiednie technologie cyfrowe.
- 4) **Współpraca z wykorzystaniem technologii cyfrowych.** Umiejętność współpracy z innymi osobami za pomocą narzędzi cyfrowych oraz wspólne tworzenie wiedzy i treści.
- 5) **Netykieta.** Znajomość zasad etykiety w komunikacji online. Dostosowanie strategii komunikacyjnych do konkretnych odbiorców oraz uświadomienie sobie różnorodności kulturowej i pokoleniowej w środowisku cyfrowym.
- 6) **Zarządzanie tożsamością cyfrową.** Umiejętność zarządzania swoją tożsamością, danymi wytworzonymi przy użyciu różnych informatycznych narzędzi, środowisk i usług.
- 7) **Umiejętność zarządzania danymi wytworzonymi przy użyciu różnych cyfrowych narzędzi, środowisk i usług.**

Obszar 3. Tworzenie treści cyfrowych:

- 1) **Tworzenie treści cyfrowych.** Umiejętność tworzenia w różnych formatach nowych treści cyfrowych (teksty, obrazy, wideo). Zdolność ekspresji przy wykorzystaniu środków cyfrowych.
- 2) **Integracja i przetwarzanie treści.** Umiejętność wprowadzania zmian, udoskonalania, poprawiania i integrowania informacji oraz treści z posiadanym zasobem wiedzy w celu tworzenia nowych, oryginalnych i rzetelnych treści oraz wiedzy.
- 3) **Przestrzeganie prawa autorskiego i licencji:** Znajomość zasad dotyczących praw autorskich i licencji na treści cyfrowe.
- 4) **Programowanie:** Podstawowa umiejętność programowania i tworzenia aplikacji.

Obszar 4. Bezpieczeństwo:

- 1) **Narzędzia służące ochronie.** Umiejętność zabezpieczania urządzeń i treści cyfrowych przed zagrożeniami (wirusy, malware). Rozumienie ryzyka i zagrożeń w środowisku cyfrowym. Wiedza dotycząca środków bezpieczeństwa i ochrony, a także uwzględnienie wiarygodności i prywatności.
- 2) **Ochrona danych osobowych i prywatności.** Umiejętność ochrony swoich danych osobowych i prywatności w środowisku cyfrowym. Dostrzeżenie, jak używać i udostępniać dane osobowe, zapewniając sobie i innym ochronę przed szkodą. Rozumienie, że w usługach cyfrowych stosowana jest „Polityka prywatności”, aby informować o sposobie wykorzystania danych.
- 3) **Ochrona zdrowia fizycznego, psychicznego i dobrostanu przed zagrożeniami wynikającymi z korzystania z technologii informacyjno-komunikacyjnych.** Umiejętność unikania zagrożeń zdrowotnych i zagrożeń dla dobrostanu fizycznego i psychicznego podczas korzystania z technologii cyfrowych. Zdolność chronienia siebie i innych przed ewentualnymi zagrożeniami w środowisku cyfrowym (np. wirtualnym nękanie). Świadomość znaczenia technologii cyfrowych dla dobrostanu społecznego i integracji społecznej.
- 4) **Ochrona środowiska.** Świadomość wpływu technologii cyfrowych na środowisko i umiejętność ich wykorzystywania.

Obszar 5. Rozwiązywanie problemów:

- 1) **Rozwiązywanie problemów technicznych.** Umiejętność diagnozowania i rozwiązywania problemów technicznych związanych z użytkowaniem urządzeń i wykorzystywaniem środowisk cyfrowych.
- 2) **Rozpoznawanie potrzeb i narzędzi niezbędnych do rozwiązywania problemów:** Zdolność oceny potrzeb oraz identyfikacja, oszacowanie, wybór i użytkowanie narzędzi cyfrowych oraz możliwych rozwiązań technologicznych w celu rozwikłania problemów. Zmiana i dostosowanie środowisk cyfrowych do indywidualnych potrzeb (np. dostępności).
- 3) **Twórcze wykorzystywanie technologii cyfrowych.** Umiejętność kreatywnego i innowacyjnego korzystania z narzędzi i technologii cyfrowych w celu tworzenia wiedzy i wprowadzania innowacji do procesów i produktów.
- 4) **Rozpoznawanie braków w zakresie kompetencji cyfrowych:** Rozpoznanie obszarów, które wymagają podnoszenia i aktualizacji swoich własnych kompetencji cyfrowych. Umiejętność wspierania innych w rozwoju ich kompetencji cyfrowych. Poszukiwanie możliwości samorozwoju i bieżące śledzenie. Umiejętność ciągłego doskonalenia swoich umiejętności cyfrowych.

Wymiar 3. modelu stanowią poziomy zaawansowania kompetencji, które są wyrażone w formie 8-stopniowej skali (poziom podstawowy 1–2, poziom średniozaawansowany 3–4, poziom zaawansowany 5–6 i poziom wysoce specjalistyczny 7–8). Uzupełnieniem modelu (dla lepszego zrozumienia) jest wymiar 4 opisany w formie przykładów w odniesieniu do wiedzy, umiejętności i postaw. Natomiast wymiar 5 zawiera przykłady odnoszące się do scenariusza zatrudnienia (korzystanie w celu rozwoju kariery zawodowej) oraz scenariusza uczenia się (korzystanie w celu poprawy umiejętności).

Decydenci używają DigComp 2.2 do formułowania polityki wspierającej rozwój kompetencji cyfrowych oraz do planowania inicjatyw edukacyjnych i szkoleniowych. Poleca się wykorzystanie tej platformy do diagnozy poziomu umiejętności cyfrowych każdego obywatela. W ramach projektu podczas prowadzonej diagnozy pogłębionej i wdrażania narzędzi personalnego rozwoju organizacji sugeruje się wykonanie testu umiejętności cyfrowych dla kadry JST oraz nauczycieli³⁶. Każda osoba, która na platformie wykonana bezpłatny test i uzyska swój indywidualny wynik (podawany

³⁶ Komisja Europejska, „Narzędzie do oceny umiejętności cyfrowych”, zob. Digital Skills Assessment Tool [dostęp, online dn. 2.09.2025].

jest w 6-stopniowej skali) w odniesieniu do poszczególnych obszarów kompetencji cyfrowych.

Wykonanie indywidualnej diagnozy poziomu kompetencji cyfrowych jest zaproszeniem do autorefleksji oraz świadomego planowania rozwoju w zakresie podnoszenia kompetencji cyfrowych. Anonimowe zebranie (z wykorzystaniem formularzy Google lub Forms platformy Microsoft 365) wyników indywidualnych pracowników JST lub nauczycieli czy kadry zajmującej się oświatą pozwoliłoby na szybkie wygenerowanie wyniku grupowego. Tym samym – w odniesieniu do rzeczywistego poziomu kompetencji cyfrowych w każdym z pięciu badanych obszarów – pozwoliłoby na uzyskanie informacji na temat panujących tendencji. Na tej podstawie można w sposób świadomy zaplanować doskonalenie i rozwijanie kompetencji cyfrowych pracowników JST, nauczycieli czy kadr zarządzających oświatą.

SELFIE ocena potencjału cyfrowego szkoły

Selfie jest to bezpłatne narzędzie opracowane przez KE, które pomaga szkołom ocenić ich potencjał cyfrowy poprzez zbieranie anonimowych opinii uczniów, nauczycieli i kadry zarządzającej na temat wykorzystania technologii cyfrowych w nauczaniu i uczeniu się. Narzędzie to zapewnia:

- **Anonimowość.** Opinie są zbierane anonimowo, co zapewnia szczerość odpowiedzi.
- **Dostosowanie:** Narzędzie można dostosować do specyficznych potrzeb szkoły.
- **Wizualizacja wyników:** Wyniki są prezentowane w formie wizualnej, co ułatwia ich analizę.
- **Planowanie działań:** Na podstawie wyników szkoły mogą opracować plan działania wspierający rozwój cyfryzacji w szkole.

SELFIE skłania uczniów, nauczycieli i kadrę kierowniczą szkół do wspólnej refleksji na temat korzystania z technologii. Na podstawie zebranych informacji narzędzie to pozwala odpowiedzieć na następujące pytania:

- 1) W jakich obszarach szkoła skutecznie korzysta z technologii, a w jakich może zoptymalizować ich stosowanie?
- 2) Czy szkoła ma plan, w jaki sposób chce korzystać z technologii? Jeśli tak, to czy plan ten jest znany pracownikom szkoły i uczniom.
- 3) Które ze szkoleń są zdaniem nauczycieli najbardziej przydatne?
- 4) Na co należy przeznaczyć fundusze?

SELFIE może pomóc w rozpoczęciu dialogu w szkole na temat ośmiu obszarów, które mogą potencjalnie wymagać poprawy. Poniżej zamieszczono opis sfer, do których odnosi się badanie. Pytania, które w nim zamieszczono, są dostosowane dla wszystkich typów szkół i placówek edukacyjnych i nie mogą być zmienione. Koordynator szkoły może zrezygnować z części pytań dodatkowych po dokonaniu oceny, czy mają znaczenie dla tej konkretnej jednostki oświatowej. Jeżeli koordynator szkoły lub innej jednostki oświatowej uważa, że jakiegoś pytania brakuje, może zdecydować się na dodanie kolejnych dodatkowych (maksymalnie do dziesięciu pytań), które odzwierciedlałyby rzeczywistości tej placówki edukacyjnej. Niemal wszystkie pytania zadawane w ramach SELFIE wymagają udzielenia odpowiedzi przy użyciu pięciostopniowej skali³⁷.

Obszar A: Kierownictwo	Ten obszar w całej szkole dotyczy roli kierownictwa w integracji technologii cyfrowych i ich skutecznego wykorzystania w głównej sferze działalności placówki (tj. w nauczaniu i uczeniu się).
Obszar B: Współpraca i tworzenie sieci kontaktów	Obszar ten jest związany ze środkami uwzględnianymi do wprowadzenia przez szkoły w celu wspierania kultury współpracy i komunikacji. Ponadto środki te służą wymianie doświadczeń i przyczyniają się do skutecznego uczenia się w ramach placówki i poza nią.
Obszar C: Infrastruktura i sprzęt	Ten obszar dotyczy posiadania odpowiedniej, niezawodnej i bezpiecznej infrastruktury (np. sprzętu, oprogramowania, zasobów informacyjnych, połączenia z internetem, wsparcia technicznego lub przestrzeni fizycznej). Taka infrastruktura umożliwia i ułatwia stosowanie innowacyjnych praktyk w zakresie nauczania, uczenia się i oceny.
Obszar D: Ustawiczne doskonalenie zawodowe. Część 1 i 2	Ten obszar dotyczy kwestii, czy szkoła ułatwia ustawiczne doskonalenie zawodowe swoich pracowników na wszystkich poziomach oraz inwestuje w takie doskonalenie. Ustawiczny rozwój może pozytywnie wpływać na integrację nowych metod nauczania i uczenia się, które wykorzystują technologie cyfrowe, aby uzyskać lepsze wyniki w nauce.

³⁷ Komisja Europejska, „SELFIE – narzędzie badania wspierające naukę w erze cyfrowej”, zob. <https://education.ec.europa.eu/pl/selfie> [dostęp, online dn. 2.09.2025].

Obszar E: Pedagogika: wsparcie i zasoby	Obszar ten związany jest z przygotowaniem do wykorzystywania technologii cyfrowych do nauczania przez wprowadzenie aktualizacji oraz innowacji w dziedzinie praktyk nauczania i uczenia się.
Obszar F: Pedagogika: wdrażanie w klasie	Obszar ten związany jest z wdrażaniem w klasie technologii cyfrowych do nauczania przez wprowadzenie aktualizacji oraz innowacji w dziedzinie praktyk nauczania i uczenia się.
Obszar G: Praktyki w zakresie oceny	Ten obszar dotyczy środków, które szkoły mogą rozważyć, aby stopniowo przejść od oceny tradycyjnej do bardziej kompleksowego wachlarza praktyk (np. obejmując praktykę w zakresie oceny), które opierają się na technologii oraz są ukierunkowane na ucznia, spersonalizowane i autentyczne.
Obszar H: Kompetencje cyfrowe uczniów	Ten obszar dotyczy zestawu umiejętności, wiedzy i postaw, które umożliwiają uczniom kreatywne korzystanie z technologii cyfrowych z zachowaniem pewności siebie i krytycznej postawy.

Od momentu uruchomienia badania jest siedem dni na udzielenie odpowiedzi. Po tym czasie sesje zamykają się automatycznie i system tworzy raport z badania. Oprócz sprawozdania ogólnego można pobrać więcej szczegółowych analiz, które będą pomocne w wyciąganiu wniosków i rekomendacji.

W ramach projektu – w trakcie prowadzonej diagnozy pogłębionej i wdrażania narzędzi personalnego rozwoju organizacji – zaleca się wykonanie badania SELFIE. Przed rozpoczęciem badania wybrać koordynatora szkolnego, który we współpracy z kadrą zarządzającą przygotuje uczniów i nauczycieli do udziału w badaniu oraz skutecznie je przeprowadzi. Osoby odpowiedzialne w szkole za zaplanowanie i realizację badania mogą skorzystać z materiału SELFIE krok po kroku, w którym znajduje się opis listy kontrolnej dotyczącej konfiguracji tego narzędzia (w tym wskazówki do konfiguracji profilu szkoły, korzystania z platformy, przeprowadzenia badania, tworzenia raportu oraz wykorzystania wyników).

Szkoły mogą wykorzystać raport SELFIE jako podstawę refleksji i debaty z udziałem całej społeczności szkolnej. Na tej podstawie można zaplanować adekwatny plan działania ukierunkowany na wdrażanie zmian w odniesieniu do obszarów wymagających interwencji.

4. Przykładowe działania wspierające rozwój kompetencji cyfrowych jednostek oświatowych i samorządowych.

Warto też zapoznać się z kilkoma działaniami, które można wykorzystać w ramach prowadzonych diagnoz czy spotkań doradczych w JST lub na etapie opracowania Harmonogramu Działań Rozwojowych (dalej HDR) dotyczącego cyfryzacji oświaty.

- **Spotkania dialogowe** – to forma rozmowy, w której uczestnicy mają możliwość wyrażenia swoich opinii i perspektyw oraz wysłuchania innych w wybranym obszarze tematycznym.

Dobrze zorganizowane spotkanie dialogowe powinno mieć:

- **Określony cel:** Ważne jest, aby jasno określić cel spotkania. Czy ma to być wymiana opinii, poszukiwanie rozwiązań, wspólne określenie priorytetów.
- **Przemyślany wybór uczestników:** Dobór odpowiednich osób jest kwestią niebagatelną. Powinni to być uczestnicy, którzy są otwarci na dialog i gotowi do konstruktywnej rozmowy. Warto również zadbać o różne grupy interesariuszy (np. kadra zarządzająca, uczniowie, nauczyciele, przedstawiciele JST, przedstawiciele instytucji i organizacji współpracujących ze szkołami).
- **Przygotowaną agendę oraz zaplanowany przebieg z adekwatnym doбором metod i sposobów pracy:** Plan musi zawierać główne tematy do omówienia oraz uwzględniać czas na swobodną dyskusję. Ważne jest stworzenie takiego klimatu do pracy, aby każdy uczestnik miał możliwość aktywnego włączenia się w dyskusję, podzielenie spostrzeżeniami czy zaproponowanie rozwiązań.

Kilka wskazówek do przebiegu spotkania dialogowego:

- Na początku spotkania warto przedstawić cel i zasady dialogu. Można również zachęcić uczestników do krótkiego przedstawienia się.
- Podczas fazy głównej trzeba dać przestrzeń do omówienia głównych tematów. Warto, aby nad całością przebiegu spotkania czuwał jeden lub kilku moderatorów. Ich zadaniem jest efektywne zarządzanie czasem, zadawanie pytań pobudzających

dyskusję oraz tworzenie warunków oraz przestrzeni dla każdej osoby biorącej udział w wydarzeniu.

- Na koniec warto podsumować najważniejsze wnioski i ustalić dalsze kroki. Można również zapytać uczestników o ich wrażenia i sugestie na przyszłość.

Wymiana doświadczeń

Wymiana doświadczeń to cenna praktyka, która pozwala na wzajemne uczenie się i rozwijanie umiejętności. Może dotyczyć różnych dziedzin (np. edukacji, biznesu, czy codziennego życia). Warto zaplanować spotkania grup JST, kadry zarządzającej, nauczycieli, uczniów oraz tworzyć przestrzeń do dzielenia się sprawdzonymi rozwiązaniami, doświadczeniem, metodami nauczania, aby poprawiać jakość podejmowanych dotychczas działań i prowadzić do wdrażania ciekawych i sprawdzonych praktyk. Wymienianie się własnymi przeżyciami może być również inspiracją do wdrażania nowatorskich praktyk w zarządzaniu oświatą oraz wprowadzenia innowacji. Dzielenie się doświadczeniami – w zależności od kontekstu i potrzeb – może odbywać się na różne sposoby.

Przykłady wymiany doświadczeń:

- Nauczyciele mogą dzielić się swoimi metodami nauczania, materiałami dydaktycznymi i strategiami zarządzania klasą. Dzięki temu mogą poprawić jakość organizacji procesów edukacyjnych.
- Społeczności lokalne mogą organizować wymianę doświadczeń między różnymi regionami czy gminami. Dzięki temu mogą powstawać nowe inicjatywy, projekty, które będą przynosić sprawdzone rozwiązania z możliwością dostosowania do potrzeb danej społeczności lokalnej.
- Profesjonalne sieci współpracy i samodoskonalenia są przestrzeniami, w których – zgodnie z potrzebami – mogą odbywać się różnorodne spotkania. (np. warsztaty z ekspertem zewnętrznym lub wewnętrznym). Celem takich przedsięwzięć jest dzielenie się wiedzą i doświadczeniami, a także poszukiwanie wspólnego rozwiązywania problemów, opracowania projektów, tworzenia partnerstwa na rzecz rozwoju edukacji.

Warto docenić również narzędzia wspierające wymianę doświadczeń. Są one następujące:

- baza wiedzy (zorganizowane zbiory dokumentów, materiałów) dostępna dla wszystkich członków grup wymiany doświadczeń;

- media społecznościowe, czyli platformy umożliwiające komunikację i współpracę w czasie rzeczywistym;
- intranet, czyli wewnętrzna sieć w ramach jednej organizacji umożliwiająca członkom danej organizacji dzielenie się informacjami i zasobami.

Wizyty studyjne

Wizyty studyjne to zorganizowane odwiedziny osób z jednej lub kilku szkół / placówek edukacyjnych lub organów samorządowych w innej jednostce funkcjonującej w podobnym obszarze. Celem takiej wymiany jest obserwacja, nauka nowych rozwiązań, wymiana doświadczeń oraz rozwijanie kompetencji. Wizyty studyjne mogą trwać od jednego do kilku dni i zwykle obejmują małe (kilkuosobowe) grupy osób. Korzyści z spotkań studyjnych obejmują zdobywanie nowej wiedzy i umiejętności, zwiększenie otwartości na innowacje, budowanie długotrwałych relacji oraz pomoc w planowaniu strategicznym.

Przykłady wizyt studyjnych:

- **Wizyty studyjne w sektorze edukacyjnym** są często organizowane w ramach programu „Erasmus+”, który polega na tym, że nauczyciele z Polski odwiedzają szkoły z innych krajów, aby zapoznać się z tamtejszym systemem edukacyjnym. Podczas odwiedzin uczestnicy mają okazję obserwować lekcje, rozmawiać z nauczycielami i uczniami oraz uczestniczyć w warsztatach dotyczących nowoczesnych metod nauczania. Dzięki temu polscy pedagodzy mogą zaadoptować w swoich szkołach zaobserwowane praktyki i tym samym podnieść jakość nauczania. Ponadto nauczyciele i pracownicy oświaty mogą odwiedzać krajowe szkoły i uczelnie, aby poznać innowacyjne metody nauczania czy zarządzania placówkami edukacyjnymi.
- **Wizyty studyjne dla JST** są doskonałą okazją do zdobycia wiedzy i wymiany doświadczeń w zakresie zarządzania i realizacji różnych przedsięwzięć czy projektów. Ten rodzaj spotkań dla organów samorządowych – skoncentrowanych na zagadnieniu cyfryzacji oświaty – stanowi doskonałą okazję do zapoznania się z nowoczesnymi technologiami i metodami zarządzania edukacją. To także wyjątkowy sposób na poznanie zaawansowanych rozwiązań cyfrowych w edukacji (np. e-dzienników, platform e-learningowych, zintegrowanych systemów zarządzania oświatą), integrowanie narzędzi cyfrowych w procesie nauczania (w tym rozwiązań STEAM), planowanie

i wdrażanie programów cyfryzacji (w tym wykorzystanie tabletów, smartfonów i tabletów czy laboratoriów w nauczaniu), a także rozwijanie kompetencji cyfrowych uczniów i nauczycieli.

Doskonalenie nauczycieli i formie procesowego wspomagania

Doskonalenie nauczycieli w formie procesowego wspomagania to podejście, które koncentruje się na długofalowym wsparciu i rozwoju szkoły oraz rozwijaniu kompetencji nauczycieli. Proces ten obejmuje kilka kluczowych etapów:

- **Diagnozę potrzeb.** Identyfikacja obszarów wymagających wsparcia w danej szkole lub przedszkolu.
- **Planowanie działań.** Opracowanie Planu Wspomagania, który zawiera konkretne działania szkoleniowe i rozwojowe.
- **Realizacja wsparcia.** Przeprowadzanie szkoleń, warsztatów, obserwacji lekcji, konsultacji oraz wymiany doświadczeń.
- **Oceny efektów** wdrożonych działań w procesie wraz z opracowanie wniosków i rekomendacji.

Takie podejście pozwala na systematyczne i efektywne rozwijanie kompetencji nauczycieli. Najważniejsze jest odejście od przypadkowych i jednorazowych form wsparcia na rzecz procesów rozwojowych. Co potem przekłada się na lepszą jakość edukacji w szkołach i przedszkolach.

5. Bibliografia.

Adamkiewicz J., (2016), „Nowe technologie informacyjne w edukacji. Niekoniecznie cyfrowa demencja”, Toruń: Wydawnictwo Adam Marszałek.

Centrum Mistrzostwa Informatycznego (CMI), zob <https://cmi.edu.pl/> [dostęp, online dn. 2.09.2025].

Centrum Projektów Polska Cyfrowa (CPPC), zob. <https://www.gov.pl/web/cppc> [dostęp, online dn. 2.09.2025].

Centrum Projektów Polska Cyfrowa (CPPC), „Cyberbezpieczny samorząd”, zob. <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad2> [dostęp, online dn. 2.09.2025].

Czapiński J., Panek T., (red.) (2015), „Diagnoza społeczna 2015: warunki i jakość życia Polaków. Raport”, Warszawa: Rada Monitoringu Społecznego.

Ferrari A., (2013), „DigComp. Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie”, Luksemburg: Urząd Publikacji Unii Europejskiej, zob. [lb-na-26035-en.pdf](https://ec.europa.eu/digital-storytelling/sites/default/files/2013/11/26035-en.pdf) [dostęp, online dn. 2.09.2025].

Fundacja Orange, Fundacja Stocznia, (2021), „Wykluczenie społeczno-cyfrowe w Polsce. Stan zjawiska, trendy, rekomendacje”, Warszawa: Fundacja Orange, zob. <https://fundacjaorange.pl/strefa-wiedzy/post/wykluczenie-spoecznie-cyfrowe-w-polsce-2021> [dostęp, online dn.2.09.2025].

Fundacja Orange, Fundacja Rozwoju Społeczeństwa, (2021), „Edukacja cyfrowa w szkołach. Raport z badań prowadzonych w ramach projektu «Lekcja: Enter»”, Warszawa: Fundacja Orange, zob. <https://lekcjaenter.pl/> [dostęp, online dn.2.09.2025].

Fundacja Orange, Fundacja Rozwoju Społeczeństwa Informacyjnego, No Input Signal sp. z o.o., (2025), „«Lekcja: AI». Projekt bezpłatnych szkoleń o sztucznej inteligencji”, Warszawa, zob. <https://lekciaai.pl/> [dostęp online, dn. 2.09. 2025].

Komisja Europejska, „Narzędzie do oceny umiejętności cyfrowych”, zob. Digital Skills Assessment Tool [dostęp, online dn. 2.09.2025].

Komisja Europejska, „SELFIE – narzędzie badania wspierające naukę w erze cyfrowej”, zob. <https://education.ec.europa.eu/pl/selfie> [dostęp, online dn. 2.09.2025].

Levitas A. (red.), (2012), *Strategie oświatowe*, Warszawa: Ośrodek Rozwoju Edukacji.

Ministerstwo Cyfryzacji, (2025), „Cyfryzacja”, Warszawa, zob. <https://www.gov.pl/web/cyfryzacja> [dostęp, online dn. 2.09.2025].

Ministerstwo Cyfryzacji, (2013), „Długookresowa Strategia Rozwoju Kraju «Polska 2030. Trzecia fala nowoczesności» (DSRK)”, Warszawa, zob. <https://mac.gov.pl/files/wp-content/uploads/2013/02/Strategia-DSRK-PL2030-RM.pdf> [dostęp, online dn. 2.09.2025].

Ministerstwo Cyfryzacji, (2023), „W drodze ku doskonałości cyfrowej. Raport końcowy z badania rynku na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych w jednostkach administracji centralnej”, Warszawa, zob. <https://cwd.info.pl/baza-wiedzy/w-drodze-ku-doskonosci-cyfrowej-raport-koncowy-z-badania-rynku-na-temat-gotowosci-wdrozenia-poziomu-wiedzy-i-wykorzystania-nowych-technologii-cyfrowych-w-jst/> [dostęp, online dn.2.09.2025].

Ministerstwo Edukacji Narodowej. Departament Innowacji i Rozwoju, (2020), „Zintegrowana Strategia Umiejętności 2030”, Warszawa, zob. <https://zsu2030.mein.gov.pl/#zsu> [dostęp, online dn. 2.09.2025].

Ministerstwo Funduszy i Polityki Realnej (2019), „Krajowa Strategia Rozwoju Regionalnego”, Warszawa, zob. Krajowa Strategia Rozwoju Regionalnego - Ministerstwo Funduszy i Polityki Regionalnej - Portal Gov.pl [dostęp, online dn. 2.09.2025].

Ministerstwo Funduszy i Polityki Realnej (2020), „Czym jest zarządzanie rozwojem”, Warszawa, zob. <https://www.gov.pl/web/fundusze-regiony/czym-jest-zarzadzanie-rozwojem> [dostęp, online dn. 2.09.2025].

Ministerstwo Rozwoju, Departament Strategii Rozwoju (2017), „Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 roku)”, Warszawa, zob. SOR (2).pdf [dostęp, online dn. 2.09.2025].

Ośrodek Rozwoju Edukacji, Związek Miast Polskich, (2023), „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu.pl/2023/10/cyfrowy-rozwoj-oswiaty-w-jednostkach-samorzadu-terytorialnego-zjst-o-projekcie> [dostęp, online dn. 2.09.2025].

Ośrodek Rozwoju Edukacji, (2023), „Cyfrowy rozwój oświaty w ramach samorządu terytorialnego”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://www.ore.edu.pl/category/projekty-fers/cyfrowy-rozwoj-oswiaty-w-jednostkach-samorzadu-terytorialnego-szkolenie-i-doradztwo-dla-kadr-jst/cyfrowy-rozwoj-oswiaty-w-jednostkach-samorzadu-terytorialnego-szkolenie-i-doradztwo-dla-kadr-jst-aktualnosci/> [dostęp online dn. 2.09.2025].

Ośrodek Rozwoju Edukacji, (2025), „Harmonogramy działań rozwojowych w zakresie cyfryzacji oświaty w JST”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu>.

pl/2025/07/harmonogramy-dzialan-rozwojowych-w-zakresie-cyfryzacji-oswiaty-w-jst/ [dostęp online dn. 2.09.2025].

Ministerstwo Funduszy i Polityki Realnej (2020), „Czym jest zarządzanie rozwojem”, Warszawa, zob. <https://www.gov.pl/web/fundusze-regiony/czym-jest-zarzadzanie-rozwojem> [dostęp, online dn. 2.09.2025].

Najwyższa Izba Kontroli. Departament Administracji Publicznej, (2022), „Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa”, Warszawa, zob. [kap~p_21_003_202106150859071623740347~01.pdf](#) [dostęp, online dn. 2.09.2025].

Ogólnopolska Sieć Edukacyjna, zob. <https://ose.gov.pl/> [dostęp online, dn. 28.09.2025].

Plebańska M., Tarkowski A., inni, (2016), „Cyfryzacja polskiej edukacji. Wizja i postulaty. Odpowiednio wprowadzane technologie cyfrowe poprawią edukację”, Warszawa: Fundacja Edukacja na NOWO i Centrum Cyfrowe, zob. https://centrumcyfrowe.pl/wp-content/uploads/2016/07/cyfryzacja-polskiej-edukacji_final.pdf [dostęp, online dn. 2.09.2025].

Polska Agencja Rozwoju Przedsiębiorczości (PARP), (2020), „Kompetencje cyfrowe i nauczanie zdalne w Unii Europejskiej. Raport tematyczny”, Warszawa, zob. <https://www.parp.gov.pl/publikacje/publication/kompetencje-cyfrowe-i-nauczanie-zdalne-w-unii-europejskiej> [dostęp, online dn. 2.09.2025].

Polska Agencja Rozwoju Przedsiębiorczości (PARP), (2023), „Rynek pracy, edukacja, kompetencje. Wykorzystanie sztucznej inteligencji w edukacji”, Dodatek specjalny do miesięcznika „Rynek pracy, edukacja, kompetencje. Aktualne trendy i wyniki badań”, Warszawa, zob. <https://www.parp.gov.pl/storeage/publications/pdf/Wykorzystanie-sztucznej-inteligencji-w-edukacji.pdf> [dostęp, online dn. 2.09.2025].

Rada Europejska, (2018), „Zalecenie Rady z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie”, „Dziennik Urzędowy Unii Europejskiej” nr 2018/C 189/01, zob. <https://op.europa.eu/pl/publication-detail/-/publication/6fda126a-67c9-11e8-ab9c-01aa75ed71a1> [dostęp, online dn. 2.09.2025].

Śledziwska K., Włoch R.,(2019), „Kompetencje przyszłości. Jak je kształtować w elastycznym ekosystemie edukacyjnym”, Warszawa: DELab Uniwersytet Warszawski, zob. <https://delab.uw.edu.pl/raporty/kompetencje-przyszlosci-jak-je-ksztaltowac-w-elastycznym-ekosystemie-edukacyjnym/> [dostęp, online dn. 2.09.2025].

Uchwała nr 8 Rady Ministrów z dnia 14 lutego 2017 roku w sprawie przyjęcia „Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 roku)”, zob. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20170000260> [dostęp, online dn. 2.09.2025].

Uchwała Nr 16 Rady Ministrów z dnia 5 lutego 2013 roku w sprawie przyjęcia „Długookresowej Strategii Rozwoju Kraju. Polska 2030. Trzecia Fala Nowoczesności”, zob. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wmp20130000121> [dostęp, online dn. 2.09.2025].

Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 roku w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych” (Dziennik Ustaw z dnia 30 marca 2023 roku pozycja 318), zob. <https://www.dziennikustaw.gov.pl/MP/2023/318https://eli.gov.pl/eli/MP/2023/318/ogl> [dostęp, online dn. 2.09.2025].

Uchwała nr 98 Rady Ministrów z dnia 12 września 2024 roku w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji”, Dziennik Ustaw z dnia 17 września 2024 roku, pozycja 812, zob. <https://dziennikustaw.gov.pl/M2024000081201.pdf> [dostęp, online dn. 2.09.2025].

Vuorikari R., Kluzer S., Punie Y., (2022), „DigComp 2.2. Ramy kompetencji cyfrowych dla obywateli – nowe przykłady wiedzy, umiejętności i postaw”, Luksemburg: Urząd Publikacji Unii Europejskiej, zob. <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415> [dostęp, online dn. 2.09.2025].

MATERIAŁ 4. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI I INFRASTRUKTURY IT



Michał Cupiał

Ważne!

Materiał 4. stanowi wsparcie przy realizacji przez JST zadań 6–10 w obszarze „Rola i zadania jednostek samorządu terytorialnego (dalej JST) w zakresie cyfryzacji oświaty”.

Wprowadzenie.

Cyfrowa transformacja stała się jednym z najważniejszych wyzwań współczesnej edukacji i administracji publicznej. Technologie informatyczne coraz mocniej przenikają do codziennego życia szkół, placówek oświatowych i jednostek samorządu terytorialnego, kształtując sposób zarządzania, komunikacji, gromadzenia danych oraz organizacji pracy. Dziś nie wystarcza już samo posiadanie nowoczesnego sprzętu czy dostępu do sieci – konieczne jest systemowe podejście do planowania rozwoju infrastruktury, zapewnienia cyberbezpieczeństwa i podnoszenia kompetencji osób odpowiedzialnych za zarządzanie tym obszarem.

Szczególną rolę w tym procesie odgrywają jednostki samorządu terytorialnego, które w większości przypadków pełnią funkcję organów prowadzących szkoły i przedszkola. To właśnie od ich decyzji strategicznych i zdolności do wypracowania spójnej polityki cyfryzacyjnej zależy, czy lokalna edukacja będzie miała dostęp do bezpiecznej, stabilnej i nowoczesnej infrastruktury. Samorządy muszą przy tym zmagać się z wieloma ograniczeniami – finansowymi, kadrowymi i organizacyjnymi – które sprawiają, że

wdrażanie cyfrowych rozwiązań wymaga nie tylko wiedzy, ale także umiejętności kompromisu i dostosowania modeli działania do lokalnych realiów.

Opracowanie to pozwoli JST na wybór optymalnego modelu zarządzania infrastrukturą informatyczną oraz na zapoznanie z doświadczeniami JST w formie dobrych praktyk, które mogą stanowić dla nich inspirację. Szczególną uwagę poświęcono problematyce cyberbezpieczeństwa, gdyż właśnie ten obszar wciąż stanowi największe wyzwanie dla szkół i samorządów – zarówno ze względu na deficyt wykwalifikowanej kadry, jak i rosnącą liczbę zagrożeń w sieci.

1. Obecna sytuacja w jednostkach samorządu terytorialnego.

Transformacja cyfrowa stała się nieodłącznym elementem współczesności, ale także współczesnej edukacji. Szybki rozwój technologii cyfrowych wpływa nie tylko na sam proces nauczania i wychowywania, ale także na zarządzanie oświatą w obrębie poszczególnych JST (np. gmin czy powiatów) i zapewnia bezpieczeństwo wykorzystywanym zasobom (tj. danym osobowym, infrastrukturze IT, informacjom o organizacji sieci cyfrowej, wszelkim informacjom organizacyjnym i zarządczym).

W procesie budowania skutecznego zarządzania oświatą i procesem kierowania edukacją w danej JST uczestniczą nie tylko placówki oświatowe, które wdrażają nowe technologie w codzienny proces edukacji i planują ich wykorzystanie, ale także organy samorządowe. W naszym kraju organy samorządowe – w przeważającej liczbie przypadków – są podmiotami prowadzącymi. Należy zwrócić uwagę, że ogromne znaczenie ma rola JST w zakresie kreowania gminnej lub powiatowej polityki podejścia do cyfryzacji oświaty, a także zapewnienia stosownych środków na realizację jej celów. To właśnie od spójnego podejścia organów prowadzących szkoły lub placówki oświatowe wobec zagadnień cyfryzacyjnych, jak i efektywnego wykorzystania swojego potencjału technologicznego przez jednostki edukacyjne zależy ich dostęp do stabilnej infrastruktury informatycznej, sprawnych systemów zarządzania danymi i ich zabezpieczania oraz kompetentnej kadry technicznej i administracyjnej.

Doświadczenia zebrane w trakcie realizacji zadań przez samorządy różnej wielkości (miejskie, wiejskie, powiatowe) pokazują, że z czasem – w odpowiedzi na lokalne potrzeby – dostępność zasobów, poziom kompetencji kadry zarządzającej, technicznej oraz organizacyjne możliwości JST, wykształciły się różne schematy zarządzania technologiami informatycznymi w placówkach oświatowych. Modele te nie powstały na podstawie jednego obowiązującego wzorca, lecz były naturalnym rezultatem lokalnych decyzji i kompromisów pomiędzy możliwościami finansowymi i organizacyjnymi. Niejednokrotnie na wybrane rozwiązania miały także wpływ uwarunkowania geograficzne i odległość pomiędzy poszczególnymi podmiotami.

Obecnie można wyróżnić dziś trzy główne podejścia wobec zarządzania zasobami cyfrowymi w oświacie:

- model zdecentralizowany;
- model scentralizowany;
- model hybrydowy.

Każde z tych rozwiązań niesie określone konsekwencje organizacyjne, finansowe i kompetencyjne. Zidentyfikowanie i uporządkowanie tych modeli stanowi fundament do dalszego opracowania praktycznych rekomendacji, które uwzględniają realne warunki funkcjonowania jednostek oświatowych w różnych strukturach samorządowych. Elementy wyróżniające te modele:

- **Model scentralizowany** charakteryzuje się tym, że wszystkie zadania związane z bezpieczeństwem informacji i zarządzaniem zasobami IT (np. konfiguracja systemów, aktualizacje, zakup sprzętu, tworzenie dokumentacji, reagowanie na incydenty) są realizowane są przez jedną, wyznaczoną jednostkę (zazwyczaj na poziomie urzędu gminy, miasta lub w centrum usług wspólnych). Takie działanie z jednej strony zapewnia to spójność działań, standaryzację procesów i lepszą kontrolę nad zasobami, ale z drugiej – może ograniczać elastyczność i szybkość reakcji w pojedynczych placówkach.
- **Model zdecentralizowany** oznacza, że każda jednostka (w tym szkoła, przedszkole lub inna placówka oświatowa) samodzielnie zarządza własną infrastrukturą i odpowiada za bezpieczeństwo informacji. Takie podejście pozostawia większą swobodę i stwarza możliwość natychmiastowego reagowania na potrzeby lokalne. Często jednak prowadzi do nierównomiernego poziomu zabezpieczeń,

braku standaryzacji i trudności w koordynacji działań na poziomie całej JST oraz utrudnia zapewnienie wykwalifikowanej kadry IT.

- **Model hybrydowy** zakłada podział kompetencji. Podstawowe wytyczne, dokumentacja, wybór narzędzi i nadzór są realizowane centralnie, natomiast wybrane zadania operacyjne wykonuje się lokalnie w placówkach. Taki model umożliwia pogodzenie jednolitego podejścia strategicznego z uwzględnieniem specyfiki i potrzeb konkretnych szkół.

2. Problematyka zarządzania zasobami IT i cyberbezpieczeństwem w jednostkach samorządu terytorialnego.

Niniejsze opracowanie ukazało się z inspiracji Ośrodka Badań Edukacyjnych (dalej ORE) w odpowiedzi na – zainicjowany przez ten podmiot program – „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST”. Celem tej inicjatywy jest wyposażenie samorządów w kompetencje umożliwiające skuteczne i odpowiedzialne zarządzanie cyfryzacją lokalnej edukacji. W projekcie uczestniczy 50 JST z całej Polski, a rezultaty pilotażu mają stanowić podstawę do wypracowania ogólnokrajowych standardów. Program ORE koncentruje się na kilku głównych obszarach:

- diagnozie stanu cyfryzacji w szkołach;
- budowie infrastruktury informatycznej;
- zarządzaniu cyberbezpieczeństwem;
- rozwojem kompetencji cyfrowych kadry JST;
- identyfikowaniu i przeciwdziałaniu wykluczeniu cyfrowemu.

To kompleksowe podejście ma nie tylko umożliwić efektywne planowanie zakupów elementów infrastruktury informatycznej i cyfrowych narzędzi edukacyjnych, ale przede wszystkim dąży do stworzenia długofalowej, lokalnej polityki cyfryzacyjnej, odpowiadającej na potrzeby społeczności edukacyjnej.

Należy też uwzględnić, że ogromną trudnością zarówno w zapewnieniu efektywnego rozwoju cyfryzacji w edukacji, jak i zarządzania tym procesem w sposób wspierający

osiąganie celów stawianych samorządom przepisami prawa oraz oczekiwaniami społecznymi jest aktualny rynek narzędzi IT. Ich nieustający rozwój powoduje, że to, co jeszcze rok lub dwa lata temu było nowoczesne, obecnie traktuje się jako przestarzałe technologicznie. W takiej sytuacji istotny element stanowi planowanie i zakup narzędzi wspierających realizację polityki samorządu w obszarze oświaty oraz osiągnięcie celów edukacyjnych w perspektywie kilku lat. Zmieniająca się rzeczywistość wymusza na szkołach, placówkach edukacyjnych i samorządowych konieczność doboru takich narzędzi cyfrowych, które będą mogły być wykorzystywane i rozwijane nie tylko przez rok lub dwa, ale co najmniej przez kilka lat. Równie ważny aspekt stanowi fakt, aby – w razie potrzeby – oprzyrządowanie to mogło być zastąpione nowymi narzędziami, ale bez konieczności wprowadzania rewolucyjnych zmian w infrastrukturze IT. Nie można także pomijać innego czynnika mówiącego o tym, aby nie ulegać pokusom zakupu najnowszych osiągnięć technologii, z których nie będzie można skorzystać. Taka postawa jest szczególnie popularna wówczas, gdy szkoły, placówki oświatowe i samorządowe mają do wykorzystania środki w ramach grantów lub projektów ze wsparciem publicznym.

W ramach prowadzonych w JST diagnozach, które ściśle wiążą się z projektem „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST”, zidentyfikowano także jeden z najbardziej powszechnych problemów wpływających na jakość zarządzania infrastrukturą teleinformatyczną w oświacie. Mowa o braku wykwalifikowanego personelu w jednostkach edukacyjnych. W wielu przypadkach obsługą techniczną sprzętu i sieci informatycznej zajmują się nauczyciele informatyki lub osoby bez formalnych kwalifikacji w zakresie IT, którym zadania te powierzono doraźnie. Trudności te są dodatkowo potęgowane przez ograniczone możliwości budżetowe szkół i placówek edukacyjnych. Podmioty te nie posiadają środków finansowych pozwalających na zatrudnienie określonych specjalistów lub przeprowadzanie regularnych szkoleń w tym zakresie. Taka sytuacja znacząco ogranicza możliwość zapewnienia bezpieczeństwa informacji, utrzymania ciągłości działania oraz planowania rozwoju infrastruktury w sposób profesjonalny i strategiczny.

Wszystkie te problemy składają się na obraz zagrożeń w zakresie cyberbezpieczeństwa, które choć najczęściej pojawiają się w sektorze publicznym, mają także miejsce w sektorze prywatnym. Zarówno na podstawie raportu Najwyższej Izby

Kontroli³⁸ (dalej NIK), jak i danych zawartych w sprawozdaniach o stanie cyberbezpieczeństwa w Polsce za 2024 rok, które zostały opracowane przez polski oddział niezależnej światowej organizacji skupiającej firmy świadczące usługi profesjonalne (dalej KPMG Poland)³⁹ i zespół reagowania na incydenty bezpieczeństwa komputerowego (działającego w strukturach Naukowej Akademickiej Sieci Komputerowej – NASK) (dalej CERT Polska)⁴⁰ – wywołania się niepokojący i powtarzalny obraz stanu bezpieczeństwa w sieci w szkołach, placówkach oświatowych i samorządowych. Najbardziej widocznymi konsekwencjami są: ciągły deficyt kompetencji, brak strategicznego planowania zarządzania zasobami IT oraz niewystarczający poziom organizacyjnego i finansowego wsparcia dla zarządzania systemami informacyjnymi i bezpieczeństwem informacji.

Sprawozdanie NIK wykazało, że zasoby kadrowe w jednostkach samorządowych, które poddano kontroli, nie były złe. Niestety jednak dokument ten nie uwzględniał szkół, przedszkoli i innych placówek edukacyjnych. Okazało się bowiem, że w tych jednostkach odpowiedzialność za sprawne działania infrastruktury IT oraz zapewnienie jej bezpieczeństwa powierzono nauczycielom informatyki lub były realizowane przez innych pracowników posiadających jakąkolwiek wiedzę w tym zakresie. Na taką sytuację wskazują wyniki diagnoz przeprowadzonych w ramach projektu NIK „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”.

Z raportu przywołanego powyżej wynika, że kontrolowane organy samorządowe – mimo tego że posiadały zasoby kadrowe – nie były w stanie skutecznie zapewnić odpowiedniego poziomu organizacji i nadzoru nad bezpieczeństwem informacji oraz ciągłością działania systemów informatycznych. W 92 proc. skontrolowanych urzędów stwierdzono poważne nieprawidłowości w tym obszarze, co oznacza, że samo przypisanie odpowiedzialności poszczególnym osobom nie przekładało się na realne działania systemowe. W ponad połowie placówek samorządowych

³⁸ Najwyższa Izba Kontroli (NIK), Jednostka kontrolująca: Delegatura NIK w Bydgoszczy, (2025), „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”, Warszawa: Najwyższa Izba Kontroli, zob. [kap~p_24_004_202405240817251716531445~01.pdf](#) [dostęp, online dn. 2.09.2025].

³⁹ KPMG Poland (2024), „Barometr cyberbezpieczeństwa. Na fali, czy w labiryncie regulacji?”, Warszawa, zob. <https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf> [dostęp, online dn. 22.08.2025].

⁴⁰ CERT Polska, (2025), „Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu”, Warszawa: Państwowy Instytut Badawczy NASK, zob. https://cert.pl/uploads/docs/Raport_CP_2024.pdf [dostęp, online dn. 22.08.2025].

brakowało wdrożonego lub aktualizowanego SZBI, a w wielu przypadkach przeglądy te były wykonane niezetelnie. Zaistniała sytuacja wskazuje na brak regularnego monitorowania stanu zabezpieczeń i skuteczności stosowanych procedur.

Warto podkreślić, że aż połowa urzędów nie przeprowadziła identyfikacji zbiorów danych podlegających ochronie, co stanowi podstawowy element zarządzania ryzykiem w obszarze przetwarzania informacji.

Pozytywnym aspektem jest to, że we wszystkich jednostkach samorządowych wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji. Niestety jednak brak zintegrowanego podejścia do planowania, dokumentowania i testowania mechanizmów ochronnych spowodował poważne luki organizacyjne. Szczególnie niepokojące są dane dotyczące ciągłości działania – w 71 proc. placówkach samorządowych nie opracowano polityk ciągłości działania, a w połowie nie istniały żadne plany odtworzeniowe lub plany zapewnienia dostępności usług w sytuacjach awaryjnych. W urzędach, w których takie mechanizmy ustanowiono, aż 58 proc. nie przeprowadzało testów ich skuteczności. Co w rezultacie oznacza brak przygotowania do realnego kryzysu lub zakłóceń pracy systemów. Problemy te nie ograniczały się jedynie do poziomu dokumentacyjnego. W 83% urzędów nieprawidłowości dotyczyły również wdrożonych środków technicznych i organizacyjnych:

- serwerownie nie były odpowiednio zabezpieczone;
- kopie zapasowe sporządzano nieregularnie lub niezgodnie z procedurami;
- umowy na usługi IT nie zawierały kluczowych zapisów dotyczących bezpieczeństwa informacji.

Stanowiło to naruszenie obowiązków wynikających z rozporządzenia w sprawie KRI. Co więcej, aż 75 proc. urzędów nie przestrzegało zasad dotyczących nadawania i weryfikacji dostępu do systemów informatycznych, a w 37 proc. nie zidentyfikowano kluczowych elementów infrastruktury IT. Warto też zauważyć, że w 83 proc. placówkach samorządowych nie prowadzono żadnego monitoringu urządzeń mobilnych (np. służbowych telefonów i tabletów), co znacząco zwiększało ryzyko utraty danych i braku kontroli nad przepływem informacji poza środowiskiem organizacji.

Opisany stan wskazuje na strukturalne braki w planowaniu, wdrażaniu i nadzorze nad działaniami z zakresu cyberbezpieczeństwa, które mają swoje źródło nie tylko

w ograniczeniach kadrowych czy finansowych, ale także w braku skutecznych mechanizmów zarządzania oraz odpowiedniego nadzoru strategicznego.

Należy zwrócić uwagę, że powyższe wyniki dotyczą jednostek posiadających informatyków z odpowiednimi kwalifikacjami. Niepokój wzbudza fakt na temat tego, jakie zatem mogłyby być wyniki podobnej kontroli przeprowadzonej w placówkach oświatowych, w których taka kadra najczęściej nie jest dostępna. Brak planowego i mierzalnego zarządzania zasobami IT oznacza również, co potwierdzono w ramach diagnoz prowadzonych w ramach projektu, że wiele jednostek nie prowadzi inwentaryzacji sprzętu, nie monitoruje stanu licencji, nie planuje cyklu życia urządzeń, ani nie analizuje skuteczności wdrażanych rozwiązań. W konsekwencji, nie są one w stanie ocenić, które elementy infrastruktury wymagają modernizacji, które systemy są przestarzałe, a które działania nie przynoszą oczekiwanych rezultatów. Zjawisko to prowadzi do nieefektywnego wykorzystania środków publicznych, braku optymalizacji kosztów oraz powstawania „martwych stref” w systemie bezpieczeństwa – czyli obszarów, które nie są objęte ochroną ani kontrolą.

Potwierdzeniem problemu systemowego są także wyniki – przywołanego wcześniej i opracowanego przez KPMG – raportu „Barometr Cyberbezpieczeństwa 2024”. Na podstawie ankiety przeprowadzonej wśród przedstawicieli polskich firm można stwierdzić, że aż 53 proc. badanych wskazało – jako główną przeszkodę w osiągnięciu właściwego poziomu bezpieczeństwa – trudności w rekrutacji i utrzymaniu wykwalifikowanych pracowników. W raporcie zaznaczono również, że chociaż w powszechnej świadomości coraz bardziej utrwała się konieczność podejmowania działań zabezpieczających zasoby cyfrowe, to jednak nadal brakuje strukturalnego podejścia do inwestowania w kompetencje. A przecież to właśnie zasoby osobowe są decydującym czynnikiem, który umożliwia skuteczne wdrożenie polityk, procedur i technicznych zabezpieczeń.

Równolegle CERT Polska w „Raporcie rocznym 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu” podkreśla, że wzrasta liczba incydentów wynikających z niewłaściwej konfiguracji systemów, braku aktualizacji oprogramowania oraz braku świadomości użytkowników końcowych. W sprawozdaniu wskazano również, że przeważająca liczba analizowanych zagrożeń dotyczyła organizacji, które nie posiadały podstawowych narzędzi monitorujących, nie wdrożyły mechanizmów wykrywania ataków ani procedur zgłaszania incydentów bezpieczeństwa.

Na podstawie wniosków z tych dwóch źródeł (KPMG Poland i CERT Polska) należy stwierdzić, że brak wykwalifikowanego personelu, niedobory finansowe oraz nieistniejące lub nieskuteczne mechanizmy planowania i monitorowania działań IT prowadzą do poważnych konsekwencji systemowych. JST i placówki oświatowe pozostają podatne na ataki, awarie, utratę danych oraz błędy ludzkie, co zagraża zarówno ciągłości działania instytucji, jak i zaufaniu obywateli do usług publicznych. W obliczu obowiązujących przepisów: Rozporządzenia Parlamentu Europejskiego i Rady (UE) roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich informacji oraz uchylenia dyrektywy 95/46/WE/(dalej RODO)⁴¹, rozporządzenie KRI⁴² czy ustawy o krajowym systemie cyberbezpieczeństwa⁴³, niezadbanie o te niedobory może skutkować nie tylko ryzykiem operacyjnym, ale również odpowiedzialnością prawną.

3. Znaczenie zarządzania bezpieczeństwem informacji.

Zarządzanie bezpieczeństwem informacji

Zarządzanie bezpieczeństwem informacji ma fundamentalne znaczenie dla funkcjonowania każdej jednostki samorządu terytorialnego i podległych jej placówek, ponieważ zapewnia ochronę zasobów cyfrowych niezbędnych do realizacji zadań publicznych, świadczenia usług obywatelom i uczniom, a także podejmowania decyzji administracyjnych. Informacje, zarówno w postaci danych osobowych, dokumentacji wewnętrznej, jak i danych systemowych, jest jednym z najcenniejszych zasobów organizacji publicznych, a jej utrata, nieuprawniony dostęp czy zafałszowanie

⁴¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich informacji oraz uchylenia dyrektywy 95/46/WE/(RODO), Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016_679 z dnia 27 kwietnia (1).pdf [online, dostęp dn. 2.09.2025].

⁴² Rozporządzenie Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dziennik Ustaw z 2024 roku pozycja 773), zob. D20140773.pdf [dostęp, online dn. 2.09.2025].

⁴³ Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dziennik Ustaw z 2018 roku pozycja 1560; opracowano na podstawie Dziennika Ustaw z 2024 roku pozycja 1077, 1222; z 2025 roku pozycja 1017, 1069), zob. D20181560.pdf [dostęp, online dn. 2.09.2025].

mogą prowadzić do poważnych zakłóceń w działaniu, strat wizerunkowych oraz odpowiedzialności prawnej.

Bezpieczeństwo informacji to nie tylko ochrona przed cyberatakami, ale również zapewnienie dostępności danych wtedy, kiedy są potrzebne, ich integralności oraz poufności. Sprawnie funkcjonujący system zarządzania bezpieczeństwem informacji pozwala w sposób uporządkowany identyfikować zagrożenia, zarządzać ryzykiem, wdrażać adekwatne środki ochrony i monitorować ich skuteczność. Wprowadzenie jednolitych zasad, procedur i standardów w tym zakresie zwiększa odporność instytucji na awarie, błędy ludzkie, celowe działania osób trzecich oraz inne sytuacje kryzysowe.

Znaczenie zarządzania bezpieczeństwem informacji wyraża się również w jego funkcji wspierającej zaufanie zarówno wewnętrzne (wśród pracowników i współpracowników), jak i zewnętrzne, w relacji z mieszkańcami, interesariuszami czy instytucjami kontrolnymi. Odpowiednie procedury i narzędzia chronią nie tylko dane, ale też reputację jednostki oświatowej lub jej wiarygodność jako administratora informacji publicznych. W coraz bardziej cyfrowym środowisku prawnym i społecznym brak systemowego podejścia do ochrony informacji przestaje być kwestią techniczną, a staje się istotnym ryzykiem organizacyjnym i strategicznym, wpływającym bezpośrednio na jakość i ciągłość realizacji zadań publicznych.

Warto sobie uzmysłowić, że nie ma większego znaczenia, na jakim poziomie organizacyjnym realizowane jest zarządzanie bezpieczeństwem informacji, czy funkcjonuje ono w modelu scentralizowanym, zdecentralizowanym, czy hybrydowym. Każdy z tych modeli może być skuteczny pod warunkiem, że przyjęte rozwiązania są odpowiednio zaplanowane, przypisane do konkretnych ról i odpowiedzialności, a ich funkcjonowanie jest stale monitorowane i dostosowywane do zmieniających się warunków prawnych, technologicznych i organizacyjnych. Tak naprawdę istotne jest, aby zarządzanie bezpieczeństwem nie było działaniem okazjonalnym ani doraźnym, ale stanowiło integralny element procesów zarządczych w jednostce. Tylko w takim ujęciu możliwe jest zachowanie ciągłości działania, adekwatna reakcja na incydenty oraz budowa kultury bezpieczeństwa wewnątrz organizacji.

Znaczenie kierownictwa w systemie zarządzania bezpieczeństwem informacji

Skuteczne zarządzanie zasobami informatycznymi oraz zapewnienie bezpieczeństwa informacji w jednostkach samorządu terytorialnego i placówkach oświatowych

wymaga nie tylko odpowiedniej infrastruktury i kompetencji operacyjnych, ale przede wszystkim zaangażowania najwyższego kierownictwa. To właśnie kadra kierownicza, zarówno na poziomie JST, jak i w szkołach, przedszkolach czy innych placówkach oświatowych, kształtuje strategiczne podejście do wykorzystania technologii w edukacji i administracji. Kadra zarządzająca w tych jednostkach odpowiada za nadanie kierunku działań, ustalenie celów i polityk w zakresie zarządzania informacjami oraz za zapewnienie odpowiednich zasobów do ich realizacji.

Zaangażowanie kierownictwa przekłada się bezpośrednio na budowę kultury bezpieczeństwa informacji. To od niego zależy, czy bezpieczeństwo IT będzie traktowane jako integralna część zarządzania organizacją, czy też jako techniczna i odseparowana funkcja. Właściwa rola kadry kierowniczej polega na nadzorowaniu wdrożenia systemów zarządzania bezpieczeństwem informacji, zatwierdzaniu polityk, przypisywaniu odpowiedzialności, egzekwowaniu zgodności z przyjętymi standardami oraz podejmowaniu decyzji strategicznych w obliczu incydentów lub zmian w środowisku technologicznym. Istotne jest, że skuteczność tych działań nie zależy od przyjętego modelu organizacyjnego. Niezależnie od tego, czy JST i jednostki edukacyjne funkcjonują w modelu scentralizowanym, zdecentralizowanym czy hybrydowym, rola kierownictwa zawsze pozostaje kluczowa. Niezależnie od lokalnego podziału zadań, konieczne jest, aby działania związane z bezpieczeństwem informacji i zarządzaniem zasobami IT były zaplanowane, monitorowane i aktualizowane w kontekście zmieniających się warunków prawnych, technologicznych i społecznych. To właśnie kadra kierownicza odpowiada za zapewnienie cyklicznego przeglądu stosowanych środków ochrony, identyfikację potrzeb szkoleniowych personelu, alokację budżetu oraz ocenę ryzyk i szans związanych z cyfryzacją.

W ten sposób najwyższe kierownictwo pełni funkcję nie tylko nadzorczą, ale i inspirującą, ustanawiając standardy postępowania, promując odpowiedzialne podejście do danych, a także wzmacniając odporność organizacyjną JST oraz podmiotów oświatowych wobec współczesnych zagrożeń cyfrowych.

Zadania przypisywane najwyższemu kierownictwu w zakresie zarządzania zasobami IT i bezpieczeństwa informacji nie wynikają wyłącznie z dobrych praktyk czy standardów zarządczych, ale mają również umocowanie prawne. Obowiązki te są jasno określone w aktach normatywnych (np. RODO czy KRI). Wymagania te obejmują m.in.:

- konieczność zapewnienia ciągłości działania, zarządzania ryzykiem;

- wdrożenie odpowiednich środków technicznych i organizacyjnych;
- nadzór nad realizacją polityk bezpieczeństwa;
- prowadzenie dokumentacji i monitorowania skuteczności zastosowanych rozwiązań.

Brak zaangażowania kadry kierowniczej w te obszary stanowi nie tylko ryzyko operacyjne badane na poziomie kontroli zarządczej, ale również potencjalne naruszenie przepisów prawa. W takiej sytuacji JST i placówki edukacyjne oraz kierujące nimi osoby mogą ponosić odpowiedzialność administracyjną i finansową.

Znaczenie szkoleń i budowania świadomości

Innym elementem niezbędnym do zapewnienia chęci poprawy stanu organizacji i zarządzania zasobami IT oraz zapewnienia przetwarzanym informacjom jest odpowiedni poziom bezpieczeństwa. Dotychczasowe przepisy prawa, za wyjątkiem rozporządzenia KRI, nie nakładały w tym zakresie znacznych obowiązków, jednakże sytuacja ta się zmienia. Niezależnie od tego utrzymanie odpowiedniego poziomu wiedzy wśród kadry zaangażowanej w realizację zadań JST oraz placówek edukacyjnych ma kluczowe znaczenie dla efektywnego zarządzania zasobami informatycznymi i zapewnienia bezpieczeństwa przetwarzanych informacji.

W szczególności dotyczy to zarówno kadry administracyjnej urzędów, jak i pracowników placówek oświatowych, którzy w codziennej pracy korzystają z wielu systemów i narzędzi wspierających prowadzenie dokumentacji, rozliczeń finansowych, ewidencji uczniów, realizację zadań dydaktycznych oraz sprawozdawczości wymaganej przez przepisy prawa. Systemy te (obejmujące m.in. programy dziedzinowe, sprawozdawcze, księgowe i kadrowe) są nośnikami informacji o wysokim znaczeniu, a ich nieprawidłowe użytkowanie, wynikające z braku wiedzy lub niewłaściwych nawyków, może prowadzić do poważnych konsekwencji, w tym zagrożeń dla integralności, dostępności oraz poufności przetwarzanych informacji i danych.

Nieustannie zmieniające się środowisko cyfrowe oraz rosnąca liczba zagrożeń związanych z cyberprzestępczością powodują, że poziom wiedzy personelu nie może być traktowany jako stan osiągnięty jednorazowo. Konieczne jest systematyczne podnoszenie kwalifikacji pracowników jednostek oświatowych oraz samorządowych i dostosowywanie ich do aktualnych wyzwań oraz zmian

w wykorzystywanych technologiach. Bez odpowiedniego przygotowania merytorycznego użytkownicy końcowi mogą nie być świadomi istnienia wielu zagrożeń, nie będą w stanie rozpoznać ich symptomów lub nie będą umieli właściwie zareagować w sytuacjach potencjalnego naruszenia bezpieczeństwa informacji. Może to prowadzić do nieautoryzowanego dostępu do danych, ich nieuprawnionego ujawnienia, usunięcia, zmiany lub utraty, co w konsekwencji zarówno narusza obowiązujące przepisy, jak i godzi w wizerunek instytucji i zaufanie społeczne.

W tym kontekście istotne jest także budowanie świadomości w zakresie konsekwencji prawnych wynikających z naruszenia zasad ochrony informacji. Pracownicy muszą znać nie tylko obowiązujące procedury i polityki, ale również rozumieć, jakie skutki – zarówno dla organizacji, jak i indywidualnie dla nich samych – może nieść niewłaściwe postępowanie z informacjami. Uświadomienie odpowiedzialności prawnej, zarówno cywilnej, jak i karnej, ma działanie prewencyjne i motywujące do większej staranności w realizacji obowiązków.

Znaczenie szkoleń i podnoszenia kompetencji w tym zakresie znajduje swoje najmocniejsze umocowanie w przepisach prawa (np. w KRI obowiązujących od 2012 roku). Jednostki są zobowiązane – zgodnie z paragrafem 19 (dalej par.) ustęp 6 (dalej ust.) rozporządzenia KRI – do zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, pamiętając szczególnie o następujących zagadnieniach:

- zagrożenia bezpieczeństwa informacji;
- skutki naruszenia zasad bezpieczeństwa informacji (w tym odpowiedzialność prawna);
- stosowanie środków zapewniających bezpieczeństwo informacji (w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich).

Oznacza to, że JST i placówki oświatowe mają obowiązek organizować działania edukacyjne i informacyjne, które nie tylko dostarczają wiedzy, ale również w codziennej pracy kształtują pożądane postawy i zachowania.

Należy podkreślić, że szkolenia te nie powinny być traktowane wyłącznie jako formalność lub jednorazowe działanie. W rzeczywistości powinny stanowić element systematycznego, zaplanowanego procesu budowania kultury bezpieczeństwa informacji w całej organizacji. Tylko takie podejście pozwala na rzeczywiste ograniczenie ryzyka błędów wynikających z niewiedzy lub rutyny. Podczas wdrażania programów szkoleniowych, należy również uwzględnić specyfikę zadań realizowanych przez

poszczególne grupy pracowników. Trzeba to zrobić w taki sposób, aby przekazywane treści były adekwatne i praktyczne. Inne bowiem potrzeby mają osoby pracujące w administracji centralnej JST, a zupełnie odmienne pracownicy Centrum Usług Wspólnych (dalej CUW) czy nauczyciele zatrudnieni w różnych typach szkół.

Utrzymanie odpowiedniego poziomu wiedzy i świadomości wśród kadry (w tym kadry zarządzającej) jest także ważne punktu widzenia ciągłości działania oraz możliwości reagowania na incydenty bezpieczeństwa. Personel, który rozumie zasady identyfikacji podejrzanych sytuacji, wie, do kogo zgłaszać potencjalne problemy, a także w jaki sposób dokumentować zdarzenia, staje się pierwszą linią obrony w systemie bezpieczeństwa informacji. Brak takich kompetencji skutkuje z kolei opóźnioną reakcją, niewłaściwym postępowaniem w sytuacjach kryzysowych i zwiększonym ryzykiem eskalacji problemu.

Zagrożenia, które wynikają z braku szkoleń lub niskiej świadomości użytkowników, są złożone i często trudne do jednoznacznego zidentyfikowania przed wystąpieniem incydentu. Mogą mieć charakter zarówno techniczny, jak i organizacyjny. Wśród przykładowych zachowań mogących prowadzić do naruszeń można wskazać:

- niewłaściwe użytkowanie systemów;
- ignorowanie ostrzeżeń;
- posługiwanie się słabymi hasłami;
- niedozwolone udostępnianie danych.

Warto sobie uzmysłowić, że takie sytuacje mogą się pojawiać nawet przy wdrożeniu nowoczesnych rozwiązań technologicznych, jeżeli towarzyszy im deficyt kompetencji i brak bieżącego wsparcia szkoleniowego.

Dlatego w strategii rozwoju i utrzymania systemów zarządzania bezpieczeństwem informacji kluczowe miejsce powinny zajmować programy edukacyjne i szkoleniowe, które będą trwałym elementem zarządzania organizacją. Inwestycja w wiedzę pracowników nie tylko podnosi poziom bezpieczeństwa, ale również przyczynia się do efektywniejszego i bardziej świadomego wykorzystania zasobów technologicznych w realizacji celów edukacyjnych i administracyjnych jednostek samorządowych.

Cel opracowania

Celem niniejszego opracowania jest zaprezentowanie dobrych praktyk oraz uogólnionych modeli rozwiązań, które mogą być wdrażane przez JST w różnym

kontekście organizacyjnym i budżetowym. Zamierzeniem autorów jest stworzenie praktycznego poradnika, który stanowiłby wsparcie dla wspierającej kadry zarządzającej jednostek samorządowych oraz edukacyjnych w podejmowaniu trafnych decyzji technologicznych i organizacyjnych. Zawarte w niniejszym materiale rekomendacje mają charakter elastyczny, gdyż ich celem jest wskazanie kierunków i możliwości, a nie sztywnych wzorców. Jest to istotne, ponieważ każda JST działa w unikalnych warunkach lokalnych⁴⁴.

4. Wymagania prawne dla systemu zarządzania bezpieczeństwem informacji.

W niniejszym fragmencie publikacji zostaną scharakteryzowane aktualne wymagania prawne wobec podmiotów samorządowych i oświatowych, które realizują zadania publiczne polegające na wdrażaniu systemu zarządzania bezpieczeństwem informacji i ochrony danych osobowych.

Należy zaznaczyć, że wymagania dotyczące ustawy o krajowym systemie cyberbezpieczeństwa zostaną zaprezentowane – na stronie internetowej Rządowego Centrum Legislacji – na podstawie aktualnie obowiązującego (pochodzącego z 2024 roku) projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw⁴⁵.

Rozporządzenie określające Krajowe Ramy Interoperacyjności

Wskazany powyżej akt prawny stanowi kluczowy element polskiego systemu regulacji dotyczących zarządzania bezpieczeństwem informacji. Ich celem jest m.in. zapewnienie interoperacyjności systemów teleinformatycznych oraz wdrożenie, monitorowanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji przetwarzanych przez podmioty realizujące zadania publiczne.

⁴⁴ Ośrodek Rozwoju Edukacji (2023), „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego (ZJST) – o projekcie”, op. cit.

⁴⁵ Rządowe Centrum Legislacji, „Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw”, Warszawa, zob. <https://legislacja.rcl.gov.pl/projekt/12384504> [dostęp, online dn. 2.09.2024].

Pierwsze rozporządzenie w sprawie KRI zostało wydane 12 kwietnia 2012 roku na podstawie ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne⁴⁶. Przywołany akt prawny określa minimalne wymagania dla rejestrów publicznych, wymiany informacji w postaci elektronicznej oraz systemów teleinformatycznych. Poza tym rozporządzenie KRI wprowadziło obowiązki w trzech podstawowych obszarach: organizacyjnym, semantycznym i technicznym. Do głównych wymogów należało m.in. zarządzanie bezpieczeństwem informacji, stosowanie określonych formatów plików oraz zapewnienie dostępności cyfrowej zgodnie z wymaganiami zamieszczonymi w Wytycznych Dostępności Treści Internetowych (dalej WCAG).

W związku z rozwojem technologii oraz zmianami legislacyjnymi (związanymi z wejściem w życie ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych⁴⁷) konieczne stało się zaktualizowanie przepisów dotyczących KRI. Nowe rozporządzenie zostało wydane 21 maja 2024 roku. Akt ten uwzględniał m.in. usunięcie przepisów dotyczących dostępności cyfrowej, które zostały uregulowane w odrębnej ustawie, a także dostosowanie wymagań do aktualnych standardów technicznych.

Obecnie obowiązujące przepisy rozporządzenia KRI nadal nakładają na podmioty publiczne obowiązki w zakresie zapewnienia interoperacyjności systemów, bezpieczeństwa informacji. Wszelkie wymagania dotyczące wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji zawarte zostały w szczególności w art. 19 przywołanego aktu prawnego. Zgodnie z jego treścią do obowiązków podmiotów realizujących zadania publiczne należą działania:

- opracowywanie i ustanawianie;
- wdrażanie i eksploatacja;
- monitorowanie i przeglądanie;
- utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji, zapewniając poufność, dostępność i integralność informacji (z uwzględnieniem następujących czynników: autentyczność, rozliczalność, niezaprzeczalność i niezawodność).

⁴⁶ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dziennik Ustaw z 2012 roku pozycja 526), zob. D20120526.pdf [dostęp, online dn. 02.09.2025].

⁴⁷ Ustawa z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dziennik Ustaw z 2019 roku pozycja 848), zob. D20190848.pdf [dostęp, online dn. 2.09.2025].

Zawarte w rozporządzeniu wymagania obejmują szereg wiele skonkretyzowanych zadań. Postulaty te powinny być rozumiane nie tylko jako obowiązek formalny, lecz jako praktyczne wytyczne wspierające instytucje publiczne w przeciwdziałaniu zagrożeniom cyfrowym oraz w budowaniu kultury bezpieczeństwa informacji. Podstawowym założeniem KRI jest aktywna rola kierownictwa jednostki w tworzeniu i egzekwowaniu polityki bezpieczeństwa informacji. Kadra zarządzająca placówką oświatową lub samorządową jest zobowiązane do zapewnienia warunków umożliwiających realizację wielu działań wspierających bezpieczeństwo. W pierwszej kolejności dotyczy to dbałości o to, aby – zgodnie ze zmieniającym się otoczeniem prawnym, technologicznym oraz organizacyjnym – wszelkie regulacje wewnętrzne były systematycznie aktualizowane. Brak aktualnych procedur i polityk może prowadzić do niezgodności z prawem oraz do nieskuteczności wdrażanych mechanizmów ochronnych.

Kolejnym wymogiem jest dokonywanie na bieżąco inwentaryzacji sprzętu i oprogramowania wykorzystywanego w procesie przetwarzania informacji. Przegląd ten powinien obejmować zarówno sprawdzenie rodzaju dostępnego sprzętu, jak i konfigurację urządzeń i systemów. A to z kolei pozwala nie tylko na bieżące monitorowanie stanu zasobów, ale też na efektywne zarządzanie ryzykiem, planowanie inwestycji oraz reagowanie w sytuacjach kryzysowych. KRI zobowiązuje również do regularnego przeprowadzania analiz ryzyka w odniesieniu do utraty integralności, poufności lub dostępności informacji. Analiza taka powinna być nie tylko dokumentowana, ale też stanowić podstawę do podejmowania działań zaradczych i profilaktycznych. System zarządzania w sytuacjach kryzysowych musi być ciągły, a nie incydentalny. Co z kolei oznacza konieczność jego weryfikacji w odpowiedzi na zmiany technologiczne, organizacyjne lub pojawienie się nowych zagrożeń.

Ważnym elementem SZBI jest także zarządzanie uprawnieniami zarówno w zakresie ich przyznawania, jak i niezwłocznej modyfikacji w razie zmiany zadań pracownika. Osoby przetwarzające informacje muszą mieć uprawnienia adekwatne do swoich obowiązków, a dostęp do informacji powinien być ograniczany wyłącznie do niezbędnego minimum. Wymóg ten ma istotne znaczenie dla zapewnienia egzekwowania i ograniczania ryzyka nadużyć. Wśród obowiązków kierownictwa wskazano także konieczność organizowania szkoleń dla pracowników zaangażowanych w przetwarzanie informacji o czym napisano wyżej.

W kontekście ochrony przed nieautoryzowanym dostępem, KRI zobowiązuje do stosowania rozwiązań technicznych oraz procedur organizacyjnych umożliwiających monitorowanie dostępu do informacji, wykrywanie działań nieautoryzowanych oraz zapobieganie im na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Systemy te – nie tylko poprzez odpowiednie zabezpieczenia sprzętowe i programowe, ale też dzięki ustaleniu jasnych zasad postępowania – powinny również zapewniać bezpieczeństwo w przypadku pracy mobilnej oraz pracy zdalnej. Informacje przetwarzane w systemach muszą być chronione przed ich przypadkowym lub celowym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. Wymaga to stosowania różnorodnych zabezpieczeń (np. szyfrowania danych, stosowania mechanizmów kontroli dostępu oraz odpowiednie rozwiązanie kopii zapasowych (obejmujących automatyzację, regularność, szyfrowanie i testowanie odzyskiwania danych).

W przypadku współpracy z podmiotami zewnętrznymi (np. firmami serwisowymi lub dostawcami oprogramowania) przepisy KRI nakładają obowiązek zawierania odpowiednich klauzul w umowach, które zagwarantują utrzymanie odpowiedniego poziomu bezpieczeństwa informacji. W raporcie NIK, który przywołano na początku tego opracowania, konieczność obowiązkowego uwzględniania dodatkowych zabezpieczeń w dokumentach została negatywnie oceniona.

Przedmiotem szczególnej uwagi powinny być także urządzenia mobilne, które – z uwagi na swoją przenośność – są bardziej podatne na kradzież, zgubienie czy nieautoryzowany dostęp. KRI wymaga opracowania zasad postępowania z informacjami oraz z nośnikami i urządzeniami służącymi do ich przetwarzania, w sposób ograniczający ryzyko takich zdarzeń.

Systemy teleinformatyczne, w których informacje są przechowywane i przetwarzane, powinny być zarządzane w sposób zapewniający ich bezpieczeństwo na wielu płaszczyznach. W szczególności konieczne jest dbanie o regularną aktualizację oprogramowania, mechanizmy ochrony przed awariami i utratą danych, wdrażanie rozwiązań chroniących przed nieuprawnioną modyfikacją danych oraz stosowanie mechanizmów kryptograficznych w sposób adekwatny do skali zagrożeń. Istotne jest także reagowanie na publikacje nowych podatności oraz podejmowanie działań prewencyjnych w celu zminimalizowania potencjalnych luk bezpieczeństwa.

Wszystkie te inicjatywy muszą być zgodne z przyjętymi politykami bezpieczeństwa oraz standardami określonymi w normach branżowych.

KRI w sposób określony z góry nakłada również obowiązek zgłaszania incydentów bezpieczeństwa. Oznacza to, że organizacja powinna posiadać zdefiniowaną i udokumentowaną procedurę reagowania na incydenty. Dzięki temu możliwe jest szybkie podjęcie działań korygujących oraz ograniczenie skutków potencjalnego naruszenia.

Nieodłącznym elementem SZBI jest także obowiązek przeprowadzania – nie rzadziej niż raz do roku – okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji. Kontrola ta powinna weryfikować zgodność wdrożonych środków z wymaganiami prawa, przyjętymi politykami, a także sprawdzać skuteczność stosowanych mechanizmów ochronnych. KRI – w sytuacjach uzasadnionych wynikami analizy ryzyka – przewiduje również obowiązek wprowadzenia dodatkowych zabezpieczeń. Co w konsekwencji oznacza, że podejście do bezpieczeństwa nie może być jednolite dla wszystkich jednostek, ale musi być dostosowane do konkretnego kontekstu działania i rodzaju zagrożeń.

Na koniec należy wskazać jeszcze jeden istotny element, którym jest rozliczalność działań w systemach teleinformatycznych. KRI nakazuje, aby wszystkie działania użytkowników (szczególnie te związane z dostępem do systemu z uprawnieniami administracyjnymi, konfiguracją zabezpieczeń oraz przetwarzaniem danych objętych ochroną prawną) były rejestrowane w dziennikach systemowych (logach sieciowych). Powinny być one przechowywane przez wymagany okres i zabezpieczone w sposób chroniący ich integralność. Poza tym jednostka edukacyjna lub samorządowa ma prawo – w zależności od analizy ryzyka – rejestrować również inne zdarzenia systemowe (w tym działania użytkowników bez uprawnień administracyjnych oraz zdarzenia środowiskowe).

Podsumowanie

Wymagania KRI wobec systemów zarządzania bezpieczeństwem informacji nie są jedynie zbiorem obowiązków technicznych. Stanowią one kompleksowe ramy, które mają na celu budowę odporności organizacji publicznych na zagrożenia cyfrowe, zapewnienie zgodności z prawem oraz zwiększenie efektywności i odpowiedzialności w zarządzaniu informacją. Ich wdrożenie – oparte na standardach międzynarodowych

i wspierane przez kulturę bezpieczeństwa – jest niezbędne dla każdej jednostki aspirującej do nowoczesnego i bezpiecznego funkcjonowania w erze cyfrowej.

Projekt ustawy o krajowym systemie cyberbezpieczeństwa

Ministerstwo Cyfryzacji – w odpowiedzi na dynamicznie ewoluujące zagrożenia w cyberprzestrzeni oraz konieczność wdrożenia przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii⁴⁸ – przedstawiło projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Propozycja dokumentu została opublikowana na stronie Rządowego Centrum Legislacji (dalej RCL) i opatrzono ją w wykazie numerem UC32⁴⁹. Celem proponowanych zmian jest wzmocnienie krajowych mechanizmów ochrony przed incydentami cybernetycznymi oraz dostosowanie krajowych regulacji do unijnych standardów.

Wyjaśnienie

Według aktualnej treści projektu ustawy o krajowym systemie cyberbezpieczeństwa obowiązki zapisane w tej ustawie obejmą m.in. samorządowe jednostki budżetowe (np. placówki oświatowe prowadzone przez JST) i urzędy gmin zatrudniające do 50 pracowników jako tzw. podmioty publiczne ważne (art. 5 ust. 2 pkt.7), a także urzędy gmin zatrudniające powyżej 50 pracowników jako tak zwane (dalej tzw.) podmioty publiczne kluczowe (załącznik 1 do projektu). Podmioty te, zgodnie z art. 2a, zobowiązane są, na ten moment do stosowania obowiązków projektowanej ustawy w zakresie do świadczonych przez siebie usług rozumianych jako realizowane zadanie publiczne. W takim rozumieniu placówki oświatowe także są zobowiązane do stosowania tych przepisów. Jednakże projekt ustawy zawiera wielostopniową redakcję przepisów i często niespójne zapisy. Wskazać tu można przepis art. 16c projektu ustawy, który określa, że podmioty publiczne realizują obowiązki wymienione we wskazanych przepisach ustawy, w tym w bardzo istotnym art. 8, tylko jeżeli prowadzą system informacyjny w celu realizacji zadania publicznego. Tym samym ustawa nie będzie dotyczyła podmiotów publicznych, które nie prowadzą takiego systemu.

⁴⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), (Dziennik Urzędowy Unii Europejskiej L 333 z dnia 27 grudnia 2022 roku, strona 80), zob. <http://data.europa.eu/eli/dir/2022/2555/oj> [dostęp, online 2.09.2025].

⁴⁹ Rządowe Centrum Legislacji, op. cit. (numer z wykazu UC32), zob. <https://legislacja.rcl.gov.pl/projekt/12384504> [dostęp, online dn. 2.09.2024].

Zdecydowano o uwzględnieniu przepisów projektu ustawy ze względu, że obowiązki w niej wskazane są w części zgodne z wymaganiami rozporządzenia KRI, a także mogą stanowić właściwy kierunkowskaz do projektowania systemu zarządzania bezpieczeństwem informacji.

Projektowana ustawa przewiduje rozszerzenie katalogu podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa, w tym o jednostki samorządu terytorialnego oraz placówki edukacyjne. Podmioty te zostaną zobligowane do wdrożenia systemów zarządzania bezpieczeństwem informacji zgodnych z określonymi normami. Ponadto projekt zakłada wprowadzenie bardziej rygorystycznych wymogów dotyczących zarządzania ryzykiem, raportowania incydentów oraz odpowiedzialności kadry kierowniczej za zapewnienie odpowiedniego poziomu. Zgodnie z projektem ustawy podmioty ważne (placówki oświatowe i urzędy zatrudniające do 50. pracowników) będą zobowiązane w zakresie zapewnienia odpowiedniego poziomu cyberbezpieczeństwa do stosowania zasad określonych w Załączniku 4 do projektu ustawy. Natomiast jednostki samorządowe zatrudniające powyżej 50. pracowników, które zgodnie z Załącznikiem 1 do projektu ustawy pełnią rolę kluczową, będą musiały stosować bardziej rygorystyczne wymogi opisane w art. 8 projektu ustawy.

W kontekście wymagań dotyczących systemu zarządzania bezpieczeństwem informacji warto porównać przepisy obowiązującego rozporządzenia KRI (w szczególności art. 19 i art. 20) z projektowanymi przepisami ustawy o krajowym systemie cyberbezpieczeństwa (w szczególności z Załącznikiem nr 4 określającym wymogi dla podmiotów ważnych będących jednostkami publicznymi). Zarówno rozporządzenie KRI, jak i projekt ustawy o KSC kładą nacisk na systemowe podejście do bezpieczeństwa informacji, opierając się na założeniu, że ochrona informacji wymaga nie tylko zastosowania narzędzi technicznych, ale również wdrożenia świadomego, planowego i odpowiedzialnego zarządzania ryzykiem. W obu dokumentach widoczny jest wspólny rdzeń wymagań, do którego należą: obowiązek prowadzenia inwentaryzacji zasobów IT, zarządzanie uprawnieniami dostępu, zapewnienie bezpiecznej pracy zdalnej i mobilnej, regularne szkolenia kadry, mechanizmy raportowania incydentów oraz cykliczna weryfikacja skuteczności wdrożonych rozwiązań.

W obu aktach prawnych znajdziemy także zbliżone oczekiwania w zakresie przypisywania i aktualizacji uprawnień do systemów, egzekwowania zasady minimalnego dostępu, prowadzenia audytów bezpieczeństwa informacji nie rzadziej

niż raz w roku oraz systematycznego monitorowania dostępu i działań użytkowników. Wspólne są również wymagania dotyczące konieczności prowadzenia szkoleń, których zakres ma obejmować zagrożenia bezpieczeństwa, skutki prawne naruszeń oraz stosowanie dostępnych narzędzi i procedur ochronnych.

Jednocześnie projekt ustawy o KSC rozwija i konkretyzuje te zagadnienia w znacznie szerszym zakresie. Wprowadza m.in. pojęcia i obowiązki dostosowane do aktualnych technologii:

- konieczność kontroli wersji produktów i usług ICT;
- testowania kopii zapasowych;
- stosowania oprogramowania antywirusowego;
- monitorowania cyklu życia wykorzystywanych narzędzi;
- kontrolowania dostępu do usług chmurowych i dużych modeli sztucznej inteligencji.

Ponadto propozycja tego aktu prawnego rozszerza również zakres obowiązków kierownictwa jednostki, nakładając odpowiedzialność za realizację zasad tzw cyberhigieny (czyli codziennych praktyk ograniczających ryzyko powstania incydentów bezpieczeństwa). Projekt zakłada także możliwość korzystania z polecanych rozwiązań w zakresie monitorowania i zarządzania incydentami (np. Dostawca Zarządzanych Usług Bezpieczeństwa – dalej MSSP), co odzwierciedla bardziej zaawansowane podejście operacyjne.

W projekcie ustawy pojawiają się też nowe mechanizmy reagowania (np. obowiązek bezzwłocznego przeglądu systemu zarządzania bezpieczeństwem informacji) w przypadku otrzymania polecenia od Pełnomocnika Rządu do spraw Cyberbezpieczeństwa lub wystąpienia zdarzenia mogącego istotnie zwiększyć ryzyko incydentu. Takiego zapisu nie zawiera KRI, ponieważ zakłada główne podejście oparte na corocznym audycie.

Rozporządzenie KRI kładzie nacisk na ogólne zasady i ramy zarządzania bezpieczeństwem, w tym obowiązek prowadzenia dzienników systemowych (logów), które zawierają informacje o działaniach administracyjnych, konfiguracjach systemowych oraz operacjach na danych objętych ochroną prawną. Jest to jeden z bardziej precyzyjnych elementów tego aktu prawnego. Z kolei projekt KSC podchodzi do zagadnienia dokumentowania w sposób bardziej systemowy i elastyczny,

koncentrując się na obowiązku udokumentowania działań w SZBI oraz możliwości wykorzystania nowoczesnych narzędzi monitorujących.

Warto również zaznaczyć, że KRI – jako rozporządzenie obowiązujące wszystkie podmioty publiczne – ma charakter uniwersalny. Natomiast projekt ustawy o KSC – zgodnie z zapisami Załącznika nr 4 – odnosi się tylko do wybranych podmiotów wskazanych w przepisach ustawy. Choć są one dość skomplikowane w zakresie adresowania obowiązków.

Znacznie więcej powinności będą miały natomiast urzędy gminy, miasta, powiatu (poza placówkami edukacyjnymi), które zatrudniają więcej niż 50. pracowników. Jak już wcześniej wspomniano jednostki te będą musiały realizować o wiele bardziej wymagające zobowiązania wynikające z art. 8 projektu ustawy o KSC. Artykuł ten akcentuje nie tylko konieczność wdrożenia SZBI, ale także jego ścisłe osadzenie w realiach operacyjnych i ryzykach wpływających na ciągłość działania. A nie było to w tak wyraźny sposób ujęte w przepisach KRI.

Ustawodawca rozszerza również podejście do zarządzania w sytuacjach kryzysowych w przeciwieństwie do KRI, które koncentruje się na przeprowadzaniu okresowych analiz ryzyka i podejmowaniu działań na ich podstawie. Zapis wynikający z art. 8 ust. 1 pkt 1 nakazuje **systematyczne** oszacowanie zagrożenia, a także zarządzania nim jako ciągłego procesu. Ponadto element ten uwzględnia konieczność wdrażania środków bezpieczeństwa proporcjonalnych do poziomu ryzyka, a jednocześnie uwzględnienie kontekstu ekonomicznego, organizacyjnego i społecznego (w tym wielkości podmiotu oraz kosztów wdrożenia). Tak szeroka ocena ryzyka nie znajduje swojego odpowiednika w przepisach KRI ani w Załączniku nr 4.

Jednostki samorządowe, które określa się mianem większych, a jednocześnie traktuje je jako podmioty kluczowe, mają dodatkowy obowiązek. Jest nim konieczność zapewnienia bezpieczeństwa **w cyklu życia systemu informacyjnego**, który obejmujący zarówno procesy jego nabywania, rozwoju, testowania, eksploatacji, jak i utrzymania. Projektowane przepisy przewidują także obowiązek planowania ciągłości działania i odtwarzania po awarii – z uwzględnieniem konieczności wdrażania, testowania i utrzymywania planów awaryjnych oraz planów odtworzeniowych, co istotnie wykracza poza dotychczasowe zapisy KRI.

Art. 8 wprowadza także wymóg **ciągłego monitorowania** systemu informacyjnego, a nie jedynie incydentalnej kontroli działań użytkowników. Elementem nowym – w

w porównaniu z dotychczasowym stanem prawnym – jest obowiązek prowadzenia polityk i procedur oceny skuteczności stosowanych środków bezpieczeństwa. Takie działanie ma zapewnić nie tylko ich wdrożenie, ale również cykliczne doskonalenie.

Wyraźnie rozwinięte zostały również wymagania wobec bezpieczeństwa łańcucha dostaw. Artykuł 8 w ust. 1 pkt. 2 podpunkt w postaci litery e) (dalej ppkt.) nakłada obowiązek zarządzania ryzykiem wynikającym z zależności od zewnętrznych dostawców produktów i usług ICT. Uzupełnieniem tego podejścia jest ust. 2, który wymaga uwzględnienia w ocenie bezpieczeństwa m.in. podatności związanych z dostawcą, jakość produktów oraz wyniki skoordynowanej oceny bezpieczeństwa prowadzonej na poziomie UE. Tego rodzaju wymogi nie są wprost przewidziane ani w przepisach KRI, ani w załączniku nr 4. Stanowią realizację mechanizmów wynikających bezpośrednio z dyrektywy NIS2.

Omawiany przepis wskazuje również na potrzebę prowadzenia działań prewencyjnych i ograniczających skutki incydentów w sposób bardziej rozbudowany niż dotychczas. Przede wszystkim ma to zapewnić integralność, poufność i autentyczności danych, regularne aktualizowanie oprogramowania (z oceną krytyczności poprawek), ochronę przed nieautoryzowaną modyfikacją oraz możliwość czasowego ograniczenia ruchu sieciowego w celu minimalizacji skutków incydu. Te elementy łączą bezpieczeństwo z odpornością operacyjną i są osadzone w logice kryzysowego zarządzania ryzykiem.

Warto też wskazać, że choć zgodnie z art. 8 ust. 3 podmioty ważne (jednocześnie będące jednostkami publicznymi) są wyłączone z bezpośredniego stosowania ust. 1 (ich obowiązki wynikają z Załącznika nr 4), to ustawa zobowiązuje je do uwzględniania w swoim systemie informacji dostarczanych przez inne podmioty publiczne (np. w ramach wspólnych rejestrów lub systemów dziedzicznych). To oznacza, że jednostki te są zobowiązane do synchronizacji polityk bezpieczeństwa z innymi instytucjami, co nie zostało ujęte ani w par. 19, ani w par. 20 rozporządzenia KRI.

Projekt ustawy KSC w art. 10 – niezależnie od różnic przedstawionych powyżej – nakłada na główne publiczne podmioty i podmioty ważne obowiązek opracowania, stosowania i aktualizacji kompletnej dokumentacji dotyczącej bezpieczeństwa systemów informacyjnych, które wykorzystuje się w procesie świadczenia usługi publicznej. Dokumentacja ta dzieli się na normatywną (opisującą zasady, oceny ryzyka i zabezpieczenia) oraz operacyjną (potwierdzającą wykonanie działań). Ustawa zobowiązuje także odpowiednie jednostki do nadzoru nad dokumentacją, ochrony

jej integralności oraz zapewnienia kontroli wersji. Dokumenty mogą być prowadzone elektronicznie lub papierowo i muszą być przechowywane przez minimum dwa lata po zakończeniu ich obowiązywania.

Rozporządzenie ogólne o ochronie danych osobowych (RODO)

W kontekście systemu zarządzania bezpieczeństwem informacji warto też wspomnieć o wymaganiach RODO. Celem poniższego opisu jest jedynie wskazanie najistotniejszych wyzwań z punktu widzenia systemu zarządzania bezpieczeństwem informacji, a nie przedstawienie wymagań tego aktu prawnego.

Kluczowym elementem wskazanym w RODO jest obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewniają zgodność działań z zasadami ochrony danych na każdym etapie przetwarzania (zarówno podczas projektowania procesów, jak i w trakcie ich bieżącej realizacji). Planowane regulacje wewnętrzne powinny zawierać mechanizmy umożliwiające identyfikację zagrożeń, ocenę ryzyka i dostosowanie zabezpieczeń do poziomu tego zagrożenia. Ochrona danych powinna być integralną częścią projektowania nowych usług, aplikacji i procesów. System musi także zapewniać, że dostęp do danych mają wyłącznie osoby upoważnione, a zakres tego dostępu jest ograniczony do minimum niezbędnego do realizacji obowiązków służbowych. Należy uwzględnić również procedury umożliwiające niezwłoczne wykrywanie naruszeń ochrony danych osobowych, ich ocenę pod kątem potencjalnych skutków dla osób, których dane dotyczą, a także zgłaszanie ich odpowiednim organom nadzorczym i – gdy to wymagane – samym osobom. Niezwykle ważne jest także prowadzenie rejestrów naruszeń i analiza incydentów pod kątem wdrożenia działań zapobiegawczych. Elementem systemu musi być także zapewnienie ciągłości działania oraz zdolność do szybkiego przywrócenia dostępu do danych w przypadku awarii lub incydentu.

Nieodzowne jest także uwzględnienie wymogu wyznaczenia osoby odpowiedzialnej za nadzór nad przestrzeganiem zasad ochrony danych. Będzie ona zaangażowana w ocenę i projektowanie procesów związanych z przetwarzaniem danych oraz będzie współpracować z organem nadzorczym, czyli inspektorem ROD.

5. Zarządzanie infrastrukturą informatyczną w trzech wariantach organizacyjnych

Poniższe opracowanie przedstawia szczegółową analizę trzech różnych modeli zarządzania infrastrukturą informatyczną w organizacjach z wieloma oddziałami. Każdy z wariantów (w pełni zdecentralizowany, hybrydowy oraz scentralizowany) charakteryzuje się odmiennym podejściem do zarządzania zasobami IT, podziału odpowiedzialności oraz alokacji budżetu. Badanie obejmuje szczegółowe porównanie zalet i wad każdego rozwiązania wraz ze wskazaniem dotyczącymi optymalizacji procesów zarządzania infrastrukturą informatyczną.

Wariant 1: Model w pełni zdecentralizowany

W tym wariantcie każda z jednostek funkcjonuje jako autonomiczny podmiot z własnym budżetem i pełną odpowiedzialnością za swoją infrastrukturę informatyczną. Podmioty samodzielnie zarządzają procesami zakupowymi, administracją sieci, bezpieczeństwem oraz obsługą techniczną.

Zalety i wady modelu zdecentralizowanego

Zalety modelu zdecentralizowanego:

- Elastyczność i szybkość reakcji – każdy podmiot może podejmować niezależnie decyzje i szybko reagować na pojawiające się potrzeby bez konieczności konsultacji z jednostką centralną.
- Większa autonomia decyzyjna – zespoły lokalne mają swobodę w wyborze rozwiązań najlepiej dopasowanych do specyficznych potrzeb swojej jednostki.
- Przypisywana wiedza ekspercka – zespoły IT posiadają dogłębną znajomość specyficznych wymagań danej jednostki i mogą lepiej dostosować rozwiązania do lokalnych potrzeb.
- Efektywniejsze cykle produkcyjne i przeglądowe – dzięki lokalnemu podejmowaniu decyzji procesy mogą przebiegać sprawniej na poziomie jednostki.
- Dopasowanie do indywidualnych wymagań – każda jednostka może wybierać rozwiązania idealnie dopasowane do swoich unikalnych potrzeb operacyjnych, co trudno osiągnąć w modelu scentralizowanym.

Wady modelu zdecentralizowanego:

- Brak spójności – różne jednostki mogą stosować odmienne standardy, co utrudnia współpracę między oddziałami i wymianę danych.
- Duplikacja wysiłków i kosztów – każda jednostka niezależnie rozwiązuje podobne problemy techniczne i organizacyjne, co prowadzi do nieefektywnego wykorzystania zasobów.
- Trudności w zapewnieniu jednolitego poziomu bezpieczeństwa – różnice w podejściu do cyberbezpieczeństwa mogą tworzyć luki w ochronie całej organizacji.
- Wyższe koszty całkowite – brak efektu skali przy zakupach sprzętu i licencji oraz konieczność zatrudniania pełnych zespołów IT w każdej jednostce zwiększa całkowity koszt utrzymania infrastruktury.
- Nierównomierne kompetencje – jednostki mogą dysponować kadrą IT o różnym poziomie wiedzy i doświadczenia, co przekłada się na nierówny poziom usług cyfrowych.

Planowanie zakupów w modelu zdecentralizowanym

Zalety planowania zakupów w modelu zdecentralizowanym:

- Precyzyjne dopasowanie do potrzeb – każda jednostka może dokładnie zaplanować zakupy pod kątem własnych, specyficznych wymagań.
- Szybkość procesów decyzyjnych – brak konieczności uzgadniania decyzji zakupowych z innymi jednostkami przyspiesza cały proces.
- Elastyczność budżetowa – możliwość dynamicznego dostosowania planów zakupowych do zmieniających się potrzeb jednostki.

Wady i problemy planowania zakupów w modelu zdecentralizowanym:

- Brak korzyści skali – mniejsze wolumeny zakupowe skutkują wyższymi cenami jednostkowymi i gorszymi warunkami handlowymi.
- Nierównomierna jakość planowania – różnice w kompetencjach zespołów IT prowadzą do zróżnicowanej jakości planów zakupowych w poszczególnych jednostkach.
- Trudności w standaryzacji – różne jednostki mogą kupować niekompatybilne systemy, co utrudnia późniejszą integrację i wymianę danych.
- Ograniczona siła negocjacyjna – mniejsze zamówienia osłabiają pozycję negocjacyjną wobec dostawców.

- Zwiększone ryzyko nietrafionych inwestycji – brak szerszej perspektywy i koordynacji może prowadzić do zakupu rozwiązań nieodpowiednich z punktu widzenia całej organizacji.

Analiza wdrożenia rozwiązań chmurowych w modelu zdecentralizowanym

Zalety wdrożenia rozwiązań chmurowych:

- Zmniejszenie obciążenia lokalnych zespołów IT – przeniesienie odpowiedzialności za utrzymanie infrastruktury na dostawcę usług chmurowych.
- Elastyczne skalowanie zasobów – możliwość dostosowania wykorzystywanych zasobów do aktualnych potrzeb jednostki bez konieczności inwestycji w fizyczną infrastrukturę.
- Dostęp do zaawansowanych technologii – nawet mniejsze jednostki mogą korzystać z nowoczesnych rozwiązań bez dużych inwestycji początkowych.
- Odciążenie z konieczności zarządzania infrastrukturą fizyczną – dostawca usług chmurowych przejmuje odpowiedzialność za utrzymanie, aktualizacje i bezpieczeństwo fizycznej infrastruktury.

Zalety utrzymania własnej infrastruktury:

- Pełna kontrola nad danymi – dane pozostają w obrębie organizacji, co może być istotne z punktu widzenia bezpieczeństwa i zgodności z regulacjami.
- Niezależność od zewnętrznych dostawców – brak ryzyka związanego z ciągłością działania usług zewnętrznych.
- Brak kosztów transferu danych – eliminacja opłat za przesyłanie danych, które mogą być znaczące w przypadku dużych wolumenów.
- Możliwość precyzyjnego dostosowania – infrastruktura może być dokładnie dopasowana do specyficznych wymagań jednostki.

W modelu zdecentralizowanym każda jednostka samodzielnie podejmuje decyzję o wdrożeniu rozwiązań chmurowych, co może prowadzić do niejednolitego środowiska informatycznego w całej organizacji. Wariant ten utrudnia też wprowadzenie spójnej strategii chmurowej i może prowadzić do problemów z integracją systemów między jednostkami.

Ważne!

Należy przeprowadzić analizę, odwołując się do aktualnej sytuacji prawnej, a także zwracając uwagę na to, czy i jakie dane mogą być przechowywane w systemach

chmurowych, zarówno prywatnych jak i państwowych (jednostki nadrzędne aż do szczebla krajowego).

Realizacja szkoleń informatycznych w modelu zdecentralizowanym

W pełni zdecentralizowany model umożliwia realizację szkoleń informatycznych poprzez:

- Szkolenia e-learningowe – każda jednostka może indywidualnie wykupić dostęp do platform szkoleniowych online dopasowanych do swoich potrzeb.
- Warsztaty i szkolenia stacjonarne – jednostki mogą organizować dedykowane szkolenia stacjonarne uwzględniające specyficzne potrzeby ich pracowników.
- Szkolenia przy stanowisku pracy (on-the-job) – pracownicy uczą się poprzez wykonywanie zadań pod nadzorem bardziej doświadczonych kolegów.
- Coaching indywidualny – personalizowane podejście do rozwoju kompetencji pracowników IT.
- Cross-training – wzajemne szkolenie pracowników w różnych obszarach IT dla zwiększenia elastyczności zespołu.

Głównym wyzwaniem jest zapewnienie jednolitego poziomu kompetencji we wszystkich jednostkach oraz efektywne wykorzystanie budżetów szkoleniowych, które w modelu rozproszonym są zwykle mniejsze.

Narzędzia wspomagające zarządzanie infrastrukturą w modelu zdecentralizowanym

W zdecentralizowanym modelu zarządzania IT można wykorzystać następujące rozwiązania:

- Systemy monitorowania infrastruktury – narzędzia analizujące dane z różnych źródeł w celu wykrywania anomalii i potencjalnych problemów, aby nie dopuścić do ich kontaktu z użytkownikami.
- Automatyzacja rutynowych zadań administracyjnych – rozwiązania mogą przejąć powtarzalne czynności administracyjne, pozwalając zespołom IT skupić się na bardziej strategicznych zadaniach.
- Systemy help desk – automatyczna kategoryzacja i priorytetyzacja zgłoszeń oraz sugerowanie rozwiązań na podstawie historycznych danych.
- Narzędzia do inteligentnej inwentaryzacji – automatyczne wykrywanie i katalogowanie sprzętu oraz oprogramowania w sieci lokalnej.

- Systemy predykcyjnego zarządzania infrastrukturą – przewidywanie awarii sprzętu na podstawie analizy wzorców wykorzystania i parametrów pracy urządzeń.

Analiza wdrożenia rozwiązań bezpieczeństwa w modelu zdecentralizowanym

W pełni zdecentralizowanym modelu zaleca się następujące wdrożenia:

- Wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia UTM – każda jednostka powinna posiadać własne rozwiązanie UTM na styku z internetem, zapewniające podstawową ochronę przed zagrożeniami sieciowymi.
- Technologia cyberbezpieczeństwa Endpoint Detection and Response (dalej EDR) – konieczne wdrożenie na wszystkich stacjach roboczych i serwerach w każdej jednostce, z lokalnym zarządzaniem i monitorowaniem.
- Ochrona przed utratą danych Data Loss Prevention (dalej DLP) – wdrożenie może być problematyczne ze względu na autonomię jednostek, niemniej sugeruje się wybór przynajmniej podstawowych rozwiązań, które zapobiegą wyciekowi danych wrażliwych.
- Antywirus – każdy podmiot potrzebuje kompleksowego rozwiązania antywirusowego z centralnym zarządzaniem na poziomie danej jednostki.

Głównym wyzwaniem jest zapewnienie spójnego poziomu bezpieczeństwa we wszystkich jednostkach oraz koordynacja działań w przypadku wykrycia zagrożeń obejmujących wiele lokalizacji.

Propozycje usprawnień dla wariantu zdecentralizowanego

- Utworzenie forum wymiany doświadczeń – regularne spotkania przedstawicieli IT z poszczególnych jednostek w celu wymiany wiedzy i umiejętności.
- Standaryzacja minimalnych wymagań bezpieczeństwa – opracowanie wspólnych standardów ochrony obowiązujących wszystkie jednostki.
- Wspólna platforma do raportowania incydentów – wprowadzenie rozwiązania umożliwiającego szybkie informowanie innych jednostek o wykrytych zagrożeniach.
- Grupowe zakupy – dobrowolne łączenie zamówień kilku jednostek w celu uzyskania lepszych warunków cenowych.
- Wspólne szkolenia – organizacja wybranych szkoleń dla pracowników z różnych jednostek sposobem obniżenia kosztów i szansą na wymianę doświadczeń.

Wariant 2: Model hybrydowy z jednostką nadrzędną

W tym wariantcie CUW pełni funkcję nadzorczą i koordynacyjną, ale podmioty podrzędne zachowują znaczną autonomię, szczególnie w zakresie budżetowania i realizacji zadań informatycznych.

Zalety i wady modelu hybrydowego

Zalety modelu hybrydowego:

- Równowaga między centralizacją a elastycznością – model łączy korzyści płynące ze standaryzacji i koordynacji z możliwością dopasowania do lokalnych potrzeb.
- Standaryzacja kluczowych procesów – CUW może określać standardy i najlepsze praktyki, jednocześnie pozostawiając pewną swobodę w ich implementacji.
- Optymalizacja kosztów – możliwość realizacji wspólnych zakupów przy jednoczesnym uwzględnieniu specyficznych potrzeb jednostek.
- Wsparcie eksperckie – jednostka nadrzędna może zapewnić specjalistyczne wsparcie i wiedzę, które mogą nie być dostępne w mniejszych jednostkach.
- Lepsza koordynacja działań – CUW umożliwia koordynację działań informatycznych w skali całej organizacji przy zachowaniu lokalnej elastyczności operacyjnej.
- Dzielenie się wiedzą i doświadczeniami – przepływ wiedzy między jednostkami za pośrednictwem CUW.

Wady modelu hybrydowego:

- Potencjalne konflikty kompetencyjne – niejasny podział odpowiedzialności między CUW a jednostkami podrzędnymi może rodzić różnego rodzaju problemy.
- Ryzyko nadmiernej biurokracji – dodatkowy poziom zarządzania może wydłużać procesy decyzyjne i wprowadzać dodatkową formalizację.
- Złożoność modelu zarządzania – wymaga precyzyjnego określenia ról, odpowiedzialności i procesów współpracy.
- Wyzwania komunikacyjne – efektywna komunikacja między CUW a jednostkami podrzędnymi może być trudna do utrzymania.
- Różnice w priorytetach – CUW może mieć inne priorytety niż jednostki podrzędne, co może prowadzić do napięć.
- Potrzeba dodatkowych zasobów administracyjnych – model hybrydowy często wymaga większych zasobów administracyjnych do zarządzania współpracą między jednostkami.

Planowanie zakupów w modelu hybrydowym

Zalety planowania zakupów w modelu hybrydowym:

- Korzyści skali przy zachowaniu elastyczności – możliwość realizacji wspólnych zakupów dla wielu jednostek przy jednoczesnym uwzględnieniu specyficznych potrzeb.
- Centralne specyfikacje zakupowe – CUW może opracowywać standardowe specyfikacje sprzętu i oprogramowania, zapewniając kompatybilność i interoperacyjność.
- Wsparcie eksperckie przy planowaniu – jednostki podrzędne mogą korzystać z wiedzy specjalistów CUW przy planowaniu zakupów.
- Lepsza koordynacja długoterminowych planów – CUW może koordynować długoterminowe strategie zakupowe, tym samym zapewniając spójność z celami strategicznymi organizacji.

Wady planowania zakupów w modelu hybrydowym:

- Konieczność uzgadniania specyfikacji – proces uzgadniania specyfikacji między CUW a jednostkami podrzędnymi może być czasochłonny.
- Ryzyko opóźnień – potrzeba koordynacji i zatwierdzania planów zakupowych przez CUW może wydłużać proces decyzyjny.
- Potencjalne konflikty interesów – różnice w priorytetach między CUW a jednostkami podrzędnymi mogą prowadzić do konfliktów przy ustalaniu priorytetów zakupowych.
- Wyzwania w synchronizacji budżetów – konieczność koordynacji planów zakupowych wielu jednostek z różnymi cyklami budżetowymi może być trudna.

Analiza wdrożenia rozwiązań chmurowych w modelu hybrydowym

Model hybrydowy zarządzania IT szczególnie dobrze komponuje się z hybrydowymi strategiami chmurowymi, które łączą pozytywne aspekty różnych podejść.

Zalety wdrożenia rozwiązań hybrydowych:

- Koordynacja strategii chmurowej – CUW może opracować spójną strategię wykorzystania chmury dla całej organizacji.
- Korzystniejsze warunki handlowe – centralne negocjacje z dostawcami usług chmurowych mogą zapewnić lepsze warunki dla wszystkich jednostek.

- Standaryzacja kluczowych rozwiązań – CUW może określić standardowe rozwiązania chmurowe dla podstawowych systemów, zapewniając interoperacyjność.
- Elastyczność w wyborze rozwiązań – jednostki podrzędne mogą mieć pewną swobodę w wyborze dodatkowych usług chmurowych odpowiadających ich specyficznym potrzebom.

Ważne!

Należy przeprowadzić analizę na podstawie aktualnej sytuacji prawnej i określić, czy możliwe jest przechowywanie określonych danych w systemach chmurowych zarówno prywatnych, jak i państwowych (jednostki nadrzędne aż do szczebla krajowego).

Realizacja szkoleń informatycznych w modelu hybrydowym

W modelu hybrydowym szkolenia informatyczne mogą być realizowane poprzez połączenie centralnego planowania i lokalnej implementacji:

- Centralne programy szkoleniowe – CUW może opracowywać standardowe programy szkoleniowe dla całej organizacji.
- Wspólne szkolenia dla pracowników różnych jednostek – organizacja szkoleń grupowych dla pracowników z różnych jednostek, co sprzyja wymianie doświadczeń.
- Centralna platforma e-learningowa – wdrożenie wspólnej platformy e-learningowej z możliwością dostosowania ścieżek szkoleniowych do potrzeb poszczególnych jednostek.
- Lokalne warsztaty praktyczne – organizacja warsztatów praktycznych na poziomie jednostek podrzędnych, dostosowanych do ich specyficznych potrzeb.
- Mentoring i coaching – program mentoringowy koordynowany przez CUW, ale realizowany lokalnie.

Narzędzia wspomagające zarządzanie infrastrukturą w modelu hybrydowym

W modelu hybrydowym można efektywnie zastosować następujące rozwiązania:

- Centralne systemy monitorowania – CUW może wdrożyć zaawansowane systemy monitorowania infrastruktury do wykrywania anomalii i potencjalnych problemów.
- Systemy zarządzania aktywami informatycznymi – rozwiązania do inwentaryzacji i zarządzania cyklem życia sprzętu i oprogramowania.

- Zintegrowane systemy help desk – centralna platforma help desk do kategoryzacji i priorytetyzacji zgłoszeń z możliwością lokalnej obsługi pierwszej linii wsparcia.
- Narzędzia do predykcyjnej analizy awarii – systemy do przewidywania potencjalnych awarii infrastruktury na podstawie analizy historycznych danych.
- Rozwiązania do automatyzacji rutynowych zadań – narzędzia automatyzujące powtarzalne zadania administracyjne, pozwalające zespołom IT skupić się na bardziej strategicznych zadaniach.

Analiza wdrożenia rozwiązań bezpieczeństwa w modelu hybrydowym

W modelu hybrydowym zaleca się następujące podejście do wdrożenia rozwiązań bezpieczeństwa:

- Wielofunkcyjna zaporą sieciową UTM (centralne zarządzanie polityką bezpieczeństwa przez CUW, a także możliwość wprowadzenia centralnego systemu UTM na styku z internetem – szczególnie w sytuacji, gdy cały ruch sieciowy jest realizowany przez podmioty zajmujące się usługami dla urzędów oraz jednostek publicznych).
- Technologia cyberbezpieczeństwa Endpoint Detection and Response (dalej EDR) – centralne zarządzanie polityką EDR przez CUW przy lokalnym wdrożeniu agentów na stacjach roboczych i serwerach w jednostkach podrzędnych.
- Ochrona przed utratą danych DLP – koordynacja przez CUW spójnego wdrożenia systemów DLP we wszystkich jednostkach, uwzględniając możliwość dostosowania polityk do specyficznych potrzeb.
- Platforma Extended Detection and Response (dalej XDR) – wdrożenie centralnej platformy XDR do obsługi zdarzeń związanych z rozszerzonym wykrywaniem zagrożeń i reagowaniem, a także integrującej dane z różnych źródeł (np. sieci, punktów końcowych, chmury) w celu kompleksowej analizy ryzyk.
- Antywirus – jednolite rozwiązania antywirusowe z centralnym zarządzaniem politykami przez CUW, ale z lokalną administracją w jednostkach podrzędnych.

Propozycje usprawnień dla wariantu hybrydowego

- Jasne określenie podziału kompetencji – precyzyjne zdefiniowanie ról i odpowiedzialności CUW oraz jednostek podrzędnych w celu uniknięcia konfliktów kompetencyjnych.

- Zastosowanie systemu zarządzania usługami informatycznymi, czyli IT Service Management (dalej ITSM) – wdrożenie platformy do zarządzania usługami informatycznymi, a jednocześnie ułatwiającej komunikację i koordynację między CUW a jednostkami podrzędnymi.
- Utworzenie forum informatycznego – regularne spotkania przedstawicieli IT z CUW i wszystkich jednostek podrzędnych w celu wymiany doświadczeń i koordynacji działań.
- Opracowanie katalogu usług – precyzyjne zdefiniowanie usług oferowanych przez CUW wraz z poziomami świadczenia usługi SLA (Service Level Agreement).
- Mechanizmy szybkiego reagowania – wprowadzenie procesów umożliwiających szybkie reagowanie na potrzeby jednostek podrzędnych.
- Wdrożenie hybrydowego modelu chmurowego – strategiczne wykorzystanie chmury publicznej, prywatnej i infrastruktury lokalnej w zależności od charakteru danych i wymagań biznesowych.

Wariant 3: Model w pełni scentralizowany

W tym modelu jednostka nadrzędna (CUW) posiada pełną kontrolę nad budżetem, zakupami i realizacją zadań informatycznych dla wszystkich podległych jednostek. Wszelkie działania informatyczne są wykonywane przez pracowników CUW.

Zalety i wady modelu scentralizowanego

Zalety modelu scentralizowanego:

- Pełna standaryzacja infrastruktury i procesów – jednolite standardy, procedury i rozwiązania techniczne w całej organizacji.
- Maksymalne korzyści skali – możliwość realizacji zakupów dla wszystkich jednostek łącznie gwarantem znacznych oszczędności.
- Jednolity poziom bezpieczeństwa – spójne polityki i rozwiązania bezpieczeństwa dla całej organizacji.
- Efektywne wykorzystanie zasobów cyfrowych – eliminacja niepotrzebnego powtarzania zadań lub tworzenia zbędnych zasobów informatycznych, a także optymalne wykorzystanie specjalistów IT.
- Uprozczone zarządzanie i raportowanie – jedno centralne miejsce zarządzania wszystkimi aspektami IT.

- Łatwiejsza kontrola jakości – możliwość zagwarantowania jednolitych standardów jakości usług IT dla wszystkich jednostek.
- Spójność informacji – jednolity system zarządzania informacją zapewniający większą spójność danych w całej organizacji.

Wady modelu scentralizowanego:

- Ograniczona elastyczność – trudności w dopasowaniu rozwiązań do specyficznych potrzeb poszczególnych jednostek.
- Dłuższe czasy reakcji – centralizacja możliwym powodem do wydłużenia czasu odpowiedzi na lokalne potrzeby.
- Ryzyko niedopasowania rozwiązań – rozbieżności między proponowanym standardowym podejściem a specyficznymi wymaganiami niektórych jednostek.
- Całkowite uzależnienie od CUW – wpływ awarii lub innego problemu w jednostce centralnej na działanie wszystkich jednostek podrzędnych.
- Ryzyko biurokracji – związek dodatkowych poziomów zatwierdzania i kontroli a nadmierną biurokracją i spowolnieniem procesów.
- Ograniczona wiedza o lokalnych potrzebach – rozbieżność między sposobem kierowania przez zespołu centralny a specyficznymi wymaganiami jednostek lokalnych.

Planowanie zakupów w modelu scentralizowanym

Zalety planowania zakupów w modelu scentralizowanym:

- Maksymalizacja efektu skali – największe możliwe oszczędności dzięki zakupom dla wszystkich jednostek łącznie.
- Jednolite standardy – pełna standaryzacja sprzętu i oprogramowania w całej jednostce.
- Uproszczony proces zakupowy – jeden mechanizm zakupowy zamiast wielu równoległych procesów w poszczególnych jednostkach.
- Bardzo dobra pozycja negocjacyjna – pozytywny związek między większymi wolumenami zamówień a poprawą strategii negocjacyjnej.
- Strategiczne planowanie rozwoju – możliwość całościowego opracowania rozwoju infrastruktury IT w perspektywie długoterminowej.
- Redukcja kosztów administracyjnych – zmniejszenie wydatków związanych z obsługą procesu zakupowego.

Wady planowania zakupów w modelu scentralizowanym:

- Ryzyko niedopasowania do potrzeb lokalnych – ewentualna rozbieżność między standardowymi zakupami a specyficznymi potrzebami niektórych jednostek.
- Mniejsza elastyczność – ograniczona zdolność do szybkiego reagowania na nagłe, lokalne potrzeby.
- Wydłużony proces decyzyjny – konieczność uwzględnienia potrzeb wszystkich jednostek powodem wydłużenia procesu planowania zakupów.
- Ryzyko priorytetyzacji potrzeb większych jednostek – trudności z uzyskaniem nadrzędnego traktowania swoich potrzeb przez mniejsze podmioty.
- Kompromisy jakościowe – konieczność wyboru rozwiązań uniwersalnych przez niektóre jednostki powodem kompromisów jakościowych dla niektórych z nich.

Analiza wdrożenia rozwiązań chmurowych w modelu scentralizowanym

Model scentralizowany pozwala na wdrożenie spójnej strategii chmurowej dla całej organizacji.

Zalety wdrożenia rozwiązań chmurowych:

- Jednolita strategia chmurowa – CUW może opracować i wdrożyć spójną strategię chmurową dla całej organizacji.
- Bardzo korzystne warunki handlowe – możliwość negocjacji najlepszych warunków z dostawcami dzięki wielkości kontraktu.
- Spójna migracja – skoordynowane przenoszenie systemów do chmury zgodnie z ustalonym harmonogramem i priorytetami.
- Centralne zarządzanie bezpieczeństwem – jednolite polityki bezpieczeństwa dla wszystkich zasobów chmurowych.
- Optymalizacja kosztów – możliwość dokładnego monitorowania i optymalizacji wykorzystania zasobów chmurowych w skali całej organizacji.

Ważne!

Należy przeprowadzić analizę na podstawie aktualnej sytuacji prawnej, zwracając uwagę na to, czy i jakie dane mogą być przechowywane w systemach chmurowych, zarówno prywatnych jak i państwowych (jednostki nadrzędne aż do szczebla krajowego).

Realizacja szkoleń informatycznych w modelu scentralizowanym

W pełni scentralizowany model umożliwia kompleksowe podejście do szkoleń IT:

- Jednolity program szkoleń – opracowanie i wdrożenie spójnego programu szkoleń dla wszystkich pracowników (niezależnie od jednostki).
- Centralna platforma e-learningowa – wdrożenie wspólnej platformy szkoleniowej online z ustandaryzowanymi ścieżkami edukacyjnymi.
- Efektywne szkolenia grupowe – pozytywny związek między planowaniem jednoczesnej organizacji szkoleń dla pracowników z różnych jednostek a optymalizacją kosztów i wymianą doświadczeń.
- Blended learning – łączenie różnych metod szkoleniowych (e-learning, szkolenia stacjonarne, warsztaty praktyczne) dla osiągnięcia najlepszych efektów.
- Centralny system zarządzania wiedzą – gromadzenie i udostępnianie wiedzy i doświadczeń z całej organizacji.

Narzędzia wspomagające zarządzanie infrastrukturą w modelu scentralizowanym

Model scentralizowany stwarza najlepsze warunki do wdrożenia zaawansowanych rozwiązań:

- Kompleksowe systemy monitorowania infrastruktury – centralne narzędzia do monitorowania całej infrastruktury do wykrywania anomalii i potencjalnych problemów.
- Analizy wzorców ruchu sieciowego – identyfikacja nietypowych zachowań w sieci mogących wskazywać na zagrożenia bezpieczeństwa.
- Predykcyjna analiza awarii – systemy do przewidywania potencjalnych uszkodzeń sprzętu na podstawie analizy historycznych danych i bieżących parametrów pracy.
- Zautomatyzowane zarządzanie zasobami – narzędzia do optymalizacji wykorzystania zasobów IT i planowania rozbudowy infrastruktury.
- Centralna platforma help desk – wykorzystanie narzędzi do automatycznej kategoryzacji, priorytetyzacji i rozwiązywania zgłoszeń użytkowników.

Analiza wdrożenia rozwiązań bezpieczeństwa w modelu scentralizowanym

Model w pełni scentralizowany umożliwia kompleksowe i spójne podejście do bezpieczeństwa:

- Centralna zapora sieciowa UTM / firewall dla całej organizacji – zarządzane przez zespół CUW – zapewniająca jednolity poziom ochrony dla wszystkich jednostek.

- XDR – wdrożenie kompleksowej platformy XDR integrującej dane z różnych źródeł (np. sieci, punktów końcowych, chmury) dla całej organizacji.
- EDR – jednolite wdrożenie i centralne zarządzanie rozwiązaniami EDR na wszystkich stacjach roboczych i serwerach.
- DLP – kompleksowe zastosowanie systemów DLP z centralnymi politykami i zarządzaniem.
- Security Operations Center (SOC) – utworzenie centralnego zespołu monitorującego bezpieczeństwo i reagującego na incydenty w całej organizacji.

Na podstawie poszczególnych etapów opisanych przedstawionych w przytoczonych materiałach trzeba stwierdzić, że wdrożenie EDR powinno obejmować: ocenę bieżącej pozycji bezpieczeństwa, inwentaryzację punktów końcowych, wybór odpowiedniego rozwiązania, strategiczne planowanie wdrożenia i testowanie pilotażowe przed pełnym wdrożeniem.

Propozycje usprawnień dla wariantu scentralizowanego

Formy usprawnienia wariantu scentralizowanego:

- Rozwój systemu zbierania informacji o potrzebach lokalnych – wdrożenie formalnego procesu zbierania informacji o specyficznych potrzebach jednostek podrzędnych.
- Lokalni koordynatorzy IT – wyznaczenie w każdej jednostce podrzędnej osoby zarządzającej jako łącznika z CUW.
- Regularne spotkania konsultacyjne – organizowanie cyklicznych zebrań z przedstawicielami jednostek podrzędnych w celu omówienia planów i priorytetów IT.
- Service Level Agreements (dalej SLA) – zdefiniowanie i monitorowanie poziomu usług świadczonych przez CUW dla jednostek podrzędnych.
- Procedury przyspieszonych zakupów – opracowanie procedur umożliwiających szybką realizację pilnych potrzeb jednostek podrzędnych.
- Decentralizacja pierwszej linii wsparcia – utworzenie lokalnych punktów wsparcia pierwszej linii przy zachowaniu centralnego zarządzania.
- Elastyczne pakiety usług – opracowanie różnych pakietów usług informatycznych dostosowanych do potrzeb różnych typów jednostek.

6. Porównanie wariantów i sugestie

Zestawienie kosztowe

Wariant scentralizowany oferuje największe potencjalne oszczędności kosztowe dzięki efektowi skali, eliminacji duplikacji wysiłków i zasobów, a także optymalnemu wykorzystaniu specjalistów IT.

Porównanie pod kątem elastyczności

Wariant zdecentralizowany zapewnia największą elastyczność i szybkość reakcji na poziomie lokalnym, ale kosztem efektywności globalnej. Wariant hybrydowy proponuje rozsądny kompromis między elastycznością a standaryzacją. Powyższe zalety mogą być niemożliwe do uzyskania w przypadku braku wykwalifikowanej kadry IT w każdej z lokalnych jednostek.

Porównanie pod kątem bezpieczeństwa

Wariant scentralizowany umożliwia wprowadzenie najbardziej spójnego i kompleksowego systemu bezpieczeństwa (szczególnie w przypadku braku wykwalifikowanej kadry IT w każdej z lokalnych jednostek). W modelach zdecentralizowanym i hybrydowym istnieje ryzyko nierównomiernego poziomu zabezpieczeń.

Podsumowanie

- Podmiotom z bardzo zróżnicowanymi jednostkami poleca się wariant hybrydowy zapewniający równowagę między standaryzacją a elastycznością.
- Dla placówek szkolnych i samorządowych dążących do maksymalnej efektywności kosztowej najbardziej odpowiedni będzie wariant scentralizowany.
- Podmiotom, w których jednostki mają bardzo specyficzne i różnorodne wymagania, wariant zdecentralizowany może być najlepszym wyborem. Trzeba jednak pamiętać, że ten model wymaga wdrożenia mechanizmów koordynacji i wymiany informacji.
- Niezależnie od wybranego wariantu, warto rozważyć:
 - » wdrożenie hybrydowej strategii chmurowej;
 - » wykorzystanie rozwiązań AI do monitorowania i zarządzania infrastrukturą;

- » wprowadzenie centralnie zarządzanych rozwiązań bezpieczeństwa;
- » ustanowienie formalnych procesów komunikacji i koordynacji między jednostkami;
- » regularne przeglądy i aktualizacje przyjętej strategii zarządzania IT.

Wybór optymalnego wariantu zarządzania infrastrukturą informatyczną powinien być podyktowany specyficznymi potrzebami, kulturą organizacyjną, strukturą oraz długoterminowymi celami strategicznymi określonego podmiotu.

7. Zarządzanie infrastrukturą informatyczną z uwzględnieniem modeli zatrudnienia kadry IT.

Poniższe opracowanie stanowi rozszerzenie analizy trzech wariantów zarządzania infrastrukturą IT, stosując analizę pod kątem wpływu modelu zatrudnienia na efektywność, bezpieczeństwo i koszty.

Porównanie zatrudnienia w różnych modelach zarządzania zasobami technologii informacyjnej

Model scentralizowany

Ten wariant opiera się na założeniu, że wszystkie działania związane z utrzymaniem, rozwojem i bezpieczeństwem infrastruktury informatycznej są realizowane przez jedną jednostkę (najczęściej JST lub CUW). Centralizacja pozwala na uzyskanie znaczących korzyści kosztowych dzięki efektowi skali, jednolitym zakupom sprzętu i oprogramowania, a także skoncentrowanemu zarządzaniu licencjami. Zespół specjalistów IT, który obsługuje wiele jednostek, może być bardziej kompetentny i lepiej przeszkolony. Taka sytuacja pozytywnie wpływa na poziom bezpieczeństwa całego systemu. Standardy ochrony danych są spójne, a systemy monitoringu i reagowania na incydenty łatwiejsze do wdrożenia i utrzymania.

Model ten cechuje się jednak ograniczoną elastycznością. Lokalne potrzeby placówek mogą nie być właściwie identyfikowane, a czas reakcji na incydenty i awarie bywa dłuższy. Dzieje się tak szczególnie w sytuacji, gdy obsługa jednostek

wymaga fizycznej obecności technika. Pojawiają się także problemy w komunikacji między CUW a szkołami, przedszkolami czy innymi placówkami edukacyjnymi (np. z powodu różnic w priorytetach czy braku zrozumienia kontekstu lokalnego). Zespół centralny, choć zazwyczaj dobrze wykwalifikowany, może nie znać specyfiki działania każdej placówki. W sytuacji rotacji pracowników w CUW, wiedza o indywidualnych konfiguracjach i potrzebach jednostek oświatowych może być trudna do utrzymania, co powoduje konieczność prowadzenia szczegółowej dokumentacji i procedur. Choć scentralizowany model jest szczególnie korzystny z perspektywy kosztów i bezpieczeństwa, wymaga silnego systemu komunikacji i skutecznego mechanizmu rozpoznawania lokalnych potrzeb.

Model zdecentralizowany

W tym wariantcie każda jednostka (np. szkoła, przedszkole, poradnia) samodzielnie zarządza własną infrastrukturą informatyczną. Oznacza to niezależne planowanie budżetu, zakupy, konfigurację systemów, wdrażanie zabezpieczeń i bieżące utrzymanie sprzętu. Taki model pozwala na dużą elastyczność. Placówki bowiem mogą szybko dostosowywać się do swoich potrzeb, testować różne rozwiązania i reagować bezpośrednio na lokalne problemy techniczne. W wielu przypadkach ułatwia to wdrażanie nowoczesnych narzędzi edukacyjnych i dopasowywanie ich do bieżącej sytuacji.

Jednak decentralizacja niesie też poważne zagrożenia. Są nimi wyższe koszty, ponieważ brakuje możliwości wspólnych zakupów. Ponadto brak standaryzacji powoduje, że każda szkoła, przedszkole czy inna jednostka edukacyjna może płacić więcej za te same rozwiązania. Poziom bezpieczeństwa jest nierównomierny – niektóre placówki wdrażają zabezpieczenia zgodne z najlepszymi praktykami, inne ograniczają się do minimum. Problemy pojawiają się również w zakresie komunikacji między poszczególnymi jednostkami, ponieważ nie tylko brakuje jednolitego punktu kontaktowego między nimi, ale także nie dochodzi do wymiany informacji o incydentach czy zagrożeniach. Sytuację dodatkowo komplikuje fakt częstej rotacji pracowników w szkołach, przedszkolach i innych podmiotach oświatowych. Dlatego też niejednokrotnie rolę opiekuna systemów informatycznych pełni nauczyciel bez formalnych kwalifikacji, który po rezygnacji z pracy w tym miejscu pozostawia placówkę bez wiedzy o wcześniejszych wdrożeniach. Nierzadko także pojawiają się luki w dokumentacji, a potrzebne procedury są tworzone na szybko, bez głębszej

analizy. Taki model może sprawdzić się w warunkach wysokiej kompetencji lokalnej kadry i przy silnym wsparciu organizacyjnym ze strony JST, ale w praktyce często prowadzi do nieefektywności i podatności na błędy.

Model hybrydowy

Model hybrydowy łączy elementy centralizacji i decentralizacji. Kluczowe decyzje strategiczne, planowanie zakupów, wyznaczanie standardów bezpieczeństwa czy nadzór nad systemami są realizowane centralnie (zwykle przez CUW lub zespół informatyczny w JST). Natomiast codzienne operacje (np. drobne naprawy, obsługa użytkowników końcowych czy bieżące reagowanie na problemy) odbywa się lokalnie, w placówkach. Taki podział umożliwia połączenie efektywności i bezpieczeństwa modelu centralnego z elastycznością lokalnego działania.

Koszty w modelu hybrydowym mogą być lepiej dopracowane. Bowiem wspólne zakupy pozwalają na uzyskanie rabatów, a ujednolicenie ułatwia zarządzanie licencjami i aktualizacjami. Jednocześnie placówki zachowują możliwość samodzielnego zgłaszania potrzeb i uczestniczenia w procesie decyzyjnym, co zwiększa ich zaangażowanie i poczucie odpowiedzialności. Dzięki centralnie opracowanym podejściom poziom bezpieczeństwa wariantu hybrydowego jest wyższy niż w modelu zdecentralizowanym. Należy jednak pamiętać, że skuteczność podejścia hybrydowego zależy od jakości współpracy między jednostkami.

Największe wyzwanie dla rozwiązania łączącego model scentralizowany z decentralizowanym stanowi komunikacja. Dlatego tak istotne jest precyzyjne określenie ról i zakresów odpowiedzialności między CUW a placówkami, a także stworzenie skutecznych kanałów informowania o incydentach, awariach czy potrzebach szkoleniowych. W sytuacji rotacji personelu (zarówno lokalnego, jak i centralnego) model hybrydowy okazuje się bardziej odporny, ponieważ wiedza i zadania są rozdzielone, co zmniejsza ryzyko utraty ciągłości działania. Wariant ten wymaga jednak wysokiego poziomu koordynacji, przejrzystych procedur oraz systematycznego podejścia do dokumentowania działań i rozwoju kompetencji. W wielu JST model hybrydowy uznawany jest za najbardziej racjonalny kompromis między bezpieczeństwem, kosztami i elastycznością działania.

Podsumowanie

Dobór modelu organizacyjnego w zakresie zarządzania infrastrukturą informatyczną i bezpieczeństwem informacji powinien uwzględniać nie tylko wielkość i strukturę JST, ale także poziom dostępnych kompetencji kadrowych, potrzeby w zakresie elastyczności operacyjnej, wymagania związane z bezpieczeństwem oraz możliwości finansowe.

Organom samorządowym, które posiadają wykwalifikowaną kadrę informatyczną w placówkach edukacyjnych, a także mają wysokie wymagania w zakresie dostępności i kontroli nad danymi, poleca się model zdecentralizowany. Warunkiem satysfakcji z wybranego modelu zarządzania jest konieczność wprowadzenia obowiązkowych mechanizmów nadzorczych (np. cyklicznych audytów koordynowanych przez JST lub CUW). Takie podejście pozwoli na zachowanie elastyczności operacyjnej przy jednoczesnym zapewnieniu standardów bezpieczeństwa i zgodności z przepisami.

W przypadku podmiotów dążących do optymalizacji kosztów, które dysponują ograniczonymi zasobami kadrowymi, racjonalnym rozwiązaniem będzie model hybrydowy. W tym podejściu do zarządzania podstawowe działania są realizowane lokalnie, natomiast wsparcie specjalistyczne, standardy, zakupy i polityki są koordynowane centralnie, wykorzystując do tego celu umowy ramowe i zewnętrznych usługodawców (outsourcing). Takie rozwiązanie umożliwia łączenie efektywności kosztowej z kontrolą nad kluczowymi aspektami zarządzania infrastrukturą.

Dla większych JST oraz instytucji publicznych o rozbudowanej strukturze organizacyjnej i dużej liczbie podmiotów podległych najlepszym rozwiązaniem będzie model scentralizowany. W tym wariantcie kierowanie infrastrukturą IT i bezpieczeństwem informacji jest w całości prowadzone przez CUW lub wyodrębnioną jednostkę centralną. Podejście scentralizowane wyróżnia zastosowanie strategii chmury hybrydowej (hybrid cloud) rozszerzającej rozwiązania chmurowe. Hybrid Cloud stanowi przestrzeń łączącą dwa lub więcej odmienne środowiska (najczęściej infrastruktury lokalnej) z jedną lub większą liczbą chmur publicznych. Takie połączenie skoordynowanych – choć różnych – środowisk chmurowych pozwala im jednocześnie funkcjonować w ramach jednego zadania. Ponadto to doskonały sposób na integrację i przesyłanie danych wrażliwych, a także na wykorzystanie rozwiązań chmurowych dla celów operacyjnych i edukacyjnych. Model hybrydowy umożliwia pełną standaryzację, lepszą kontrolę

nad kosztami, łatwiejsze raportowanie oraz spójną politykę bezpieczeństwa w całej strukturze JST.

Najważniejsze jest, aby – niezależnie od wybranego wariantu – decyzje w zakresie kierowaniem IT były poprzedzone analizą realnych potrzeb oraz zdolności do zarządzania ryzykiem i odpowiedzialnością formalnoprawną. Przyjęty model powinien być elastyczny w dostosowywaniu się do zmieniających się warunków technologicznych, organizacyjnych i prawnych, a także przewidywać mechanizmy ciągłego doskonalenia i przeglądu efektywności zastosowanych rozwiązań.

8. Wdrożenie od podstaw infrastruktury informatycznej w jednostce organizacyjnej.

Kompleksowe tworzenie bazy informatycznej w jednostce organizacyjnej wymaga systematycznego podejścia, które obejmujące pięć głównych etapów:

- zabezpieczenie dostępu do sieci publicznej poprzez odpowiednie urządzenia brzegowe;
- segmentację sieci wewnętrznej z wykorzystaniem technologii VLAN;
- konfigurację urządzeń sieciowych;
- przygotowanie stacji końcowych;
- implementację systemów zarządzania aktualizacjami.

Każdy z nich odgrywa istotną rolę w budowaniu bezpiecznej, wydajnej i skalowalnej infrastruktury IT, która będzie wspierać działalność operacyjną organizacji przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa i możliwości efektywnego zarządzania.

Etap 1: Zabezpieczenie dostępu do sieci publicznej

Analiza porównawcza rozwiązań UTM i NGFW

Wybór odpowiedniego urządzenia brzegowego stanowi fundamentalny element bezpieczeństwa infrastruktury IT. Zarówno UTM, jak i zaporę sieciową nowej generacji,

czyli Next Generation Firewall (dalej NGFW) reprezentują dwa różne podejścia do zabezpieczania sieci. Każde z tych rozwiązań posiada zalety i ograniczenia.

Zintegrowane urządzenie do ochrony sieci w różnych jednostkach (UTM) łączy podstawowe zastosowanie firewall z szerszymi funkcjami bezpieczeństwa (np. ochrona antywirusowa i możliwości Virtual Private Network (dalej VPN)), integrując wiele możliwości ochrony na jednym sprzęcie. Z kolei NGFW rozszerza możliwości tradycyjnej zatory sieciowej (firewall), wzbogacając ją o nową funkcjonalność analizy na poziomie aplikacji. To umożliwia kontrolowanie ruchu sieciowego do siódmej warstwy koncepcyjnego wzorca przetwarzania danych i przesyłania ich sieci, jakim jest model Open Systems Interconnection (dalej OSI).

Różnica w zakresie funkcjonalności przekłada się na odmienne zastosowania w rozmaitych środowiskach organizacyjnych. UTM oferuje rozwiązanie typu „wszystko w jednym”, które jest szczególnie atrakcyjne dla małych organizacji o ograniczonych zespołach cyberbezpieczeństwa. Sprzęty UTM zapewniają podstawową ochronę poprzez umieszczenie w jednym urządzeniu różnorodnych funkcji firewall, antywirusowych, filtrowania treści i VPN. A to znacznie upraszcza wdrażanie i zarządzanie. Podejście to jest szczególnie wartościowe dla organizacji, które potrzebują natychmiastowej ochrony bez konieczności posiadania specjalistycznej wiedzy z zakresu bezpieczeństwa informatycznego. UTM charakteryzuje się również niższymi kosztami podczas wstępnego wprowadzania oraz nieskomplikowaną konfiguracją. Wszystkie te elementy czynią z tego urządzenia atrakcyjnym wybór dla środowisk o ograniczonych zasobach technicznych i finansowych.

Natomiast NGFW zapewnia nie tylko skonfigurowaną ochronę, która jest szczególnie przydatna dla średnich i dużych firm, ale także poleca im specjalistów do spraw bezpieczeństwa. Urządzenia NGFW mogą analizować ruch na poziomie aplikacji, umożliwiając blokowanie pakietów z nieautoryzowanych aplikacji, a jednocześnie zezwalać na inspekcję zaszyfrowanego ruchu VPN. Ta zaawansowana funkcjonalność sprzyja tworzeniu bardzo szczegółowych polityk bezpieczeństwa dostosowanych do specyficznych potrzeb organizacji. NGFW oferuje również lepszą wydajność w środowiskach o wysokim natężeniu ruchu. Umożliwia obsługę dziesiątek jednostek informacji, czyli gigabitów (dalej GB) na sekundę. A jednocześnie NGFW może

dokonywać kontroli ruchu sieciowego Deep Packet Inspection (dalej DPI) oraz systemów zapobiegania włamaniom Intrusion Prevention System (dalej IPS).

Różnice w wydajności i zastosowaniu

Zasadnicza różnica między UTM a NGFW dotyczy ich wydajności i możliwości skalowania. Powszechnie uważa się, że UTM jest najlepiej dostosowany do środowisk o niższym natężeniu ruchu ze względu na ograniczenia wynikające z konsolidacji wielu funkcji bezpieczeństwa w jednym urządzeniu. Wysokie obciążenie liczbą wizyt na stronie lub skomplikowane wymagania przetwarzania bardzo negatywnie wpływają na wydajność całej sieci przy wyborze rozwiązań UTM. Trzeba również pamiętać o tym, że specjalistyczne urządzenia NGFW, które posiadają zoptymalizowane oprogramowanie do wspierania środowisk o wysokiej przepustowości, mogą obsługiwać większe wolumeny ruchu sieciowego niż UTM.

Organizacje rozwijające się i reagujące na zwiększające się wymagania bezpieczeństwa często napotykają ograniczenia pojedynczych platform UTM. W takich sytuacjach NGFW oferuje większą elastyczność i możliwości dostosowania do zmieniających się potrzeb biznesowych. NGFW umożliwia również bardziej szczegółową kontrolę ruchu sieciowego, pozwalając administratorom sieci na tworzenie i utrzymywanie jej ochrony poprzez bardzo szczegółowe polityki. Ta zdolność do precyzyjnego zarządzania ruchem jest szczególnie wartościowa w środowiskach, w których różne typy ruchu wymagają rozmaitych poziomów bezpieczeństwa i priorytetyzacji.

Rozwiązania programowe i wirtualne

Alternatywą dla rozwiązań sprzętowych są platformy programowe oferujące znaczną elastyczność i oszczędności kosztów. Darmowe oprogramowanie typu open source, jakim jest pfSense, bazuje na dystrybucji **Free Berkley Software Distribution** (dalej FreeBSD, czyli systemu operacyjnego typu Unix).

System operacyjny pfSense oferuje:

- routing statyczny;
- routing domyślny;
- routing dynamiczny,;

- stateful firewall;
- Network Address Translation (dalej NAT);
- VPN;
- Dynamic Host Configuration Protocol (dalej DHCP);
- Domain Name System (dalej DNS);
- load balancing (technikę równoważenia obciążenia sieci).

Oprogramowanie pfSense charakteryzuje się rozbudowaną funkcjonalnością z możliwością instalacji rozmaitych dodatkowych elementów. Przykładowo mogą nimi być:

- Snort – system wykrywania i zapobiegania włamaniom;
- FreeSWITCH – bezpłatna platforma telefoniczna typu open source dla telefonii internetowej, czyli Voice over Internet Protocol (dalej VoIP);
- Squid jako oprogramowanie proxy (serwer pośredniczący między użytkownikiem a stronami internetowymi);
- Darkstat narzędzie do monitorowania ruchu sieciowego.

Platforma pfSense jest szczególnie atrakcyjna dla organizacji z doświadczonymi administratorami, którzy mogą w pełni wykorzystać jej możliwości konfiguracyjne.

Innym interesującym rozwiązaniem jest bezpłatne oprogramowanie OPNsense, które jest rozgałęzieniem (forkiem) systemu pfSense i ma swe korzenie na platformie FreeBSD. OPNsense został utworzony w 2014 roku, ale jego pierwsza oficjalna wersja została upubliczniona w styczniu 2015 roku. Ten fork oferuje bardziej nowoczesny i intuicyjny interfejs, kładąc nacisk na bezpieczeństwo i innowacyjność. OPNsense charakteryzuje się wielojęzycznym wsparciem, wbudowaną pomocą i szybką nawigacją z polem wyszukiwania, co czyni go bardziej dostępnym dla początkujących administratorów. Platforma ta zapewnia częstsze aktualizacje bezpieczeństwa i funkcji w porównaniu z pfSense (stosującym bardziej konserwatywny harmonogram wydań i będącym ukierunkowanym na stabilność). OPNsense jest szczególnie polecany dla użytkowników i firm priorytetowo traktujących łatwość użycia, nowoczesne praktyki bezpieczeństwa i częste aktualizacje.

Etap 2: Segmentacja sieci wewnętrznej z wykorzystaniem technologii Virtual Local Area Network (dalej VLAN)

Projektowanie architektury VLAN

Właściwy podział sieci wewnętrznej za pomocą technologii VLAN stanowi główny element bezpieczeństwa i wydajności infrastruktury IT. Ta metoda podziału sieci na oddzielne obszary umożliwia tworzenie mniejszych grup podsieci, które są wirtualnie połączone w tej samej domenie rozgłoszeniowej. Przy czym użytkownicy w tym samym VLAN mogą komunikować się między sobą bezpośrednio. Każda podsieć posługuje się swoim odrębnym adresem, czyli Internet Protocol Address (dalej IP). Ciekawe jest to, że te podsieci (zgrupowane w obrębie VLAN) będą komunikować się tylko ze sobą, a nie z żadnymi innymi urządzeniami podłączonymi do tej samej sieci fizycznej. Wymiana informacji pomiędzy różnymi VLAN wymaga routingu przez urządzenie warstwy 3, którym zwykle jest router lub przełącznik. Taka architektura zapewnia naturalną segmentację ruchu i ułatwia implementację polityk bezpieczeństwa.

Dla projektowanej infrastruktury proponuje się następującą numerację VLAN bazującą na najlepszych praktykach branżowych.

- VLAN 10 to doskonałe rozwiązanie dla sieci administracyjnej, która obejmuje stacje robocze administratorów IT i urządzenia zarządzające infrastrukturą.
- VLAN 20 zostanie przeznaczony dla urządzeń drukujących, zapewniając centralne zarządzanie drukarkami i kontrolę dostępu do funkcji drukowania.
- VLAN 30 będzie obsługiwać systemy monitoringu CCTV i kontroli dostępu, izolując ruch związany z bezpieczeństwem fizycznym od pozostałej infrastruktury IT.
- VLAN 40 jest skonfigurowaną siecią dla gości, umożliwiając bezpieczny dostęp do internetu dla klientów poprzez punkty dostępowe Wi-Fi bez narażania sieci wewnętrznej.
- VLAN 50 będzie przeznaczony dla sal komputerowych używanych do prowadzenia szkoleń, zapewniając izolowane środowisko edukacyjne z możliwością łatwego resetowania konfiguracji po każdym szkoleniu.
- VLAN 60 zostanie wykorzystany w komunikacji między serwerami usług a systemami przechowywania danych (np. macierze dyskowe HDD lub SSD zapewniające wysoką przepustowość i niskie opóźnienia dla krytycznych operacji na danych).
- VLAN 70 stanowi alternatywę dla przyszłej ekspansji lub specjalnych projektów.

- VLAN 80 może służyć jako sieć zarządzania dla urządzeń sieciowych, umożliwiając bezpieczny dostęp do interfejsów administracyjnych przełączników i routerów.

Polecane urządzenia sieciowe

Wybór odpowiednich przełączników sieciowych ma duże znaczenie dla wydajności i niezawodności infrastruktury VLAN. Przy przeglądania asortymentu przełączników należy zwrócić uwagę na liczbę portów, wsparcie dla standardów VLAN (IEEE 802.1Q), możliwości Power over Ethernet (dalej PoE) dla punktów dostępowych sieci internetowej, a także funkcje mechanizmu sieciowego Quality of Service (dalej QoS) dla priorytetyzacji ruchu. Podczas wybierania urządzenia sieciowego w środowiskach krytycznych są preferowane modele posiadające zasilacze nadmiarowe. Kolejnym ważnym kryterium decydującym o zakupie konkretnego przełącznika jest możliwość skorzystania przez klienta z wsparcia producenta (przy uwzględnieniu charakteru tej pomocy i czasu jej trwania). Taka ewentualność wynika nie tylko z lokalnych przepisów prawa, ale także jak i z możliwość przedłużenia przez sprzedawcę.

Kontrola dostępu i bezpieczeństwo VLAN

Kontrolowanie dostępu użytkowników do VLAN jest niezbędnym elementem bezpiecznej segmentacji sieci. W wielu podmiotach dopuszczenie chętnych osób do korzystania z internetu wymaga określonej przynależności portów lub adresów MAC do VLAN. Następnie przełączniki pozwalają tylko na wysyłanie i odbieranie danych do odpowiednich portów, umożliwiając administratorom sieci egzekwowanie dostępu do VLAN w całej jednostce edukacyjnej lub samorządowej. Alternatywną metodą są połączenia pojedynczego VLAN, które można również osiągnąć za pomocą tagowania VLAN.

Konfiguracja VLAN wiąże się z podziałem sieci na mniejsze obszary (podsieci). Takie rozwiązanie wpływa na poprawę bezpieczeństwa oraz wydajność internetu. Sieć VLAN tworzy się poprzez przypisanie portów przełącznika do konkretnych portów dostępowych, a także budowanie połączeń międzysieciowych w celu komunikacji między nimi. Ramka Ethernet jest podstawową jednostką danych w sieciach lokalnych. W celu uruchomienia VLAN do standardowej ramki Ethernet dodaje się specjalny nagłówek (zgodny ze standardem IEEE 802.1Q) zawierający identyfikator VLAN (dalej VLAN ID).

Tagowanie VLAN wpływa korzystnie na usprawnienie organizacji ruchu sieciowego, pomaga bowiem przełącznikom i routerom przypisać dany pakiet do określonej sieci VLAN. Tagi wirtualnej sieci VLAN działają na warstwie 2 (niezależnie od adresu IP). Urządzenia mogą być podłączone do tej samej struktury VLAN, nawet wtedy, gdy znajdują się w różnych zakresach adresów numerycznych identyfikatorów przypisywanych urządzeniom w sieci. Segmentacja VLAN wymaga własnych rozważań bezpieczeństwa, gdyż izolując ruch sieciowy, nie chroni sama siebie. Odpowiednia opieka i ochrona muszą być zastosowane do operacji między podsieciami. Wdrożenie może obejmować również zaawansowane funkcje (np. Dynamic VLAN Assignment bazuje na autentykacji 802.1X, co zapewnia automatyczne przypisywanie użytkowników do odpowiednich VLAN na podstawie ich tożsamości).

Etap 3: Konfiguracja urządzeń sieciowych

Konfiguracja przełączników sieciowych

Konfiguracja przełączników sieciowych wymaga systematycznego podejścia, który obejmuje podstawowe ustawienia bezpieczeństwa, konfigurację VLAN oraz implementację polityk Quality of Service (dalej QoS). Pierwszy etap stanowi zabezpieczenie urządzenia poprzez zmianę domyślnych haseł administracyjnych, konfigurację szyfrowanych połączeń zarządzania (Secure Shell – dalej SSH – zamiast Telnet) oraz wyłączenie nieużywanych usług i portów. Konfiguracja VLAN powinna następować zgodnie z wcześniej zaprojektowaną architekturą, z przypisaniem odpowiednich portów do poszczególnych VLAN, a także skonfigurowaniem portów trunk dla komunikacji między przełącznikami. Szczególną uwagę należy zwrócić na konfigurację natywnego VLAN i tagowanie ruchu, aby zapewnić właściwą segmentację i bezpieczeństwo.

Implementacja protokołów Spanning Tree Protocol (dalej STP) lub jego nowszych wariantów: Rapid Spanning Tree Protocol (dalej RSTP), Multiple Spanning Tree Protocol (dalej MSTP) jest kluczowa dla zapobiegania pętlom w sieci i zapewnienia redundancji. Proces ustawiania i dostosowywania parametrów i ustawień sieciowych musi uwzględniać planowane mapowanie VLAN do instancji, co wpływa na rozwój systemu numeracji.

Konfiguracja funkcji bezpieczeństwa portów powinna obejmować ograniczenie liczby adresów MAC na port, dynamiczne uczenie się adresów oraz działania podejmowane

przy wykryciu naruszenia. Power over Ethernet (dalej PoE) musi być skonfigurowany na portach obsługujących urządzenia (np. punkty dostępowe sieci, telefony IP czy kamery IP). Należy skonfigurować QoS w celu priorytetyzacji krytycznego ruchu, jakim są: ruch VoIP czy dane z systemów bezpieczeństwa. Simple Network Management Protocol (SNMP) winno się ustawić dla monitorowania i zarządzania, przy czym – ze względów bezpieczeństwa – wymagane jest zastosowanie Simple Network Management Protocol version 3 (dalej SNMPv3).

Konfiguracja urządzeń brzegowych

Ustawienie urządzeń brzegowych – (bez względu na to, czy są to rozwiązania UTM czy NGFW) – wymaga precyzyjnego podejścia do polityk bezpieczeństwa i routingu. Podstawowa konfiguracja powinna rozpocząć się od aktualizacji firmware'u do najnowszej wersji, ustawienia podstawowych parametrów sieciowych, a także stworzenia bezpiecznych kont administracyjnych z uwierzytelnianiem wieloczynnikowym. Formowanie interfejsów sieciowych musi uwzględniać podłączenie do łącza internetowego dostawcy oraz połączenie z siecią wewnętrzną. Trzeba pamiętać, że może być konieczne skonfigurowanie wielu interfejsów dla różnych stref bezpieczeństwa.

Polityki firewall muszą bazować na zasadzie najmniejszych uprawnień, z domyślnym blokowaniem całego ruchu i selektywnym otwieraniem tylko niezbędnych portów i protokołów. Konfiguracja Network Address Translation (dalej NAT) umożliwi dostęp urządzeń wewnętrznych do internetu przy zachowaniu prywatności adresów IP sieci wewnętrznej. Systemy wykrywania i zapobiegania włamaniom (IDS / IPS) powinny być skonfigurowane z aktualnymi sygnaturami zagrożeń oraz dostosowanymi progami alertów, aby zminimalizować liczbę fałszywych alarmów przy jednoczesnym zachowaniu wysokiej skuteczności detekcji.

W rozwiązaniach NGFW szczególnie istotne są filtrowanie treści i kontrola aplikacji. Działania te pozwalają na szczegółową kontrolę dostępu do zasobów internetowych i aplikacji. Ustawienie wirtualnej sieci prywatnej VPN dla dostępu zdalnego musi uwzględniać silne algorytmy szyfrowania, uwierzytelnianie certyfikatami oraz segmentację ruchu VPN od sieci wewnętrznej. Logging i monitorowanie powinny być skonfigurowane dla rejestrowania wszystkich istotnych zdarzeń bezpieczeństwa z możliwością integracji z centralnymi systemami SIEM. Regularne kopie zapasowe

konfiguracji oraz testowanie procedur odzyskiwania są niezbędne dla zapewnienia ciągłości działania.

Etap 4: Konfiguracja urządzeń końcowych

Przygotowanie systemu operacyjnego i oprogramowania biurowego

Konfiguracja urządzeń końcowych z systemem Microsoft Windows 10 lub 11 wymaga systematycznego podejścia zapewniającego bezpieczeństwo, wydajność i zgodność z politykami organizacji. Do wykonania instalacji systemu operacyjnego powinno się użyć aktualnych obrazów systemowych zawierających najnowsze aktualizacje bezpieczeństwa. Formatowanie musi obejmować tworzenie standardowych profili użytkowników, konfigurację polityk grupowych (Group Policy), a także wdrożenie zasad bezpieczeństwa lokalnego. Pomimo że przyłączenie komputerów do domeny Windows Server Active Directory (dalej AD) znacząco zwiększa koszty wdrożenia, to jednak pozwala na centralne zarządzanie kontami użytkowników, politykami bezpieczeństwa oraz dystrybucją oprogramowania.

Należy dbać o to, aby instalację oprogramowania biurowego (Microsoft Office czy LibreOffice) wykonano z wykorzystaniem licencji zbiorczych i narzędzi automatyzacji wdrażania. Microsoft Office oferuje pełną integrację z usługami Microsoft 365, zaawansowane funkcje współpracy oraz regularne aktualizacje bezpieczeństwa i funkcjonalności. LibreOffice stanowi – przy znacznie niższych kosztach licencjonowania – alternatywę open source oferującą kompatybilność z formatami Microsoft Office. Wybór między tymi rozwiązaniami powinien uwzględniać specyficzne potrzeby organizacji, wymogi interoperacyjności z zewnętrznymi partnerami oraz dostępny budżet na licencje oprogramowania.

W ramach formatowania systemu trzeba także uwzględnić: wyłączenie niepotrzebnych usług systemowych, konfigurację zapory Windows Defender, włączenie szyfrowania dysku BitLocker oraz konfigurację automatycznych aktualizacji systemu. Wdrożenie polityk kontroli kont użytkowników User Account Control (dalej UAC) oraz formatowanie Windows Defender Advanced Threat Protection (dalej ATP) mogą znacząco podnieść poziom bezpieczeństwa stacji roboczych. Standaryzacja konfiguracji z wykorzystaniem Microsoft System Center Configuration Manager (dalej SCCM) lub Windows Deployment Services (dalej WDS) zapewni spójność środowiska i ułatwi zarządzanie flotą urządzeń.

Wdrożenie zabezpieczeń końcowych z ESET Protect Entry

Zastosowanie pakietu bezpieczeństwa dla firm Protect Entry (dalej ESET) stanowi kompleksowe rozwiązanie ochronne dla stacji końcowych. Oferuje nowoczesną, wielowarstwową ochronę z wykorzystaniem uczenia maszynowego i przyjaznej konsoli zarządzania. System zapewnia ochronę komputerów, urządzeń mobilnych i serwerów plików poprzez zastosowanie zaawansowanych algorytmów, które działające w czasie rzeczywistym, wykrywają oraz neutralizują zagrożenia. Wielowarstwowa architektura bezpieczeństwa ESET jest zdolna do wykrywania złośliwego oprogramowania malware zarówno przed, podczas, jak i po jego wykonaniu. Do tego celu wykorzystuje następujące czynniki: uczenie maszynowe, zaawansowaną analizę behawioralną, big data i ludzką ekspertyzę do równoważenia wydajności, detekcji i fałszywych alarmów.

Konsola bezpieczeństwa ESET PROTECT jest wielofunkcyjnym narzędziem zdalnym, które jest oparte na chmurze i służy do zarządzania ochroną sieci produktów korporacyjnych rozwiązań bezpieczeństwa systemach operacyjnych. Rozwiązanie to umożliwia centralne wdrażanie bezpieczeństwa i zapewnia widoczność sieci bez konieczności dodatkowego sprzętu. Konsola ESET PROTECT oferuje zdalne zarządzanie z widocznością zagrożeń, użytkowników i obiektów w kwarantannie.

Główne funkcje ESET Protect Entry obejmują pełne szyfrowanie dysku zabezpieczające wrażliwe dane solidnymi algorytmami szyfrowania, które chronią cały dysk. Zaawansowane zabezpieczenie przed zagrożeniami wykorzystuje rozbudowane mechanizmy (np. analiza behawioralna, uczenie maszynowe do identyfikacji i eliminacji zaawansowanych zagrożeń). Ochrona poczty elektronicznej zabezpiecza serwery pocztowe i komunikację wieloma warstwami bezpieczeństwa, w tym filtrami spam i skanami malware. Zarządzanie podatnościami sprawia, że systemy są wciąż aktualizowane i chronione. Jest to możliwe dzięki automatycznym ocenom podatności i zarządzaniu aktualizacjami.

Alternatywne rozwiązania zabezpieczeń końcowych

Rynek oferuje wiele alternatywnych rozwiązań zabezpieczeń końcowych z centralnym zarządzaniem. Microsoft Defender for Business stanowi natywne rozwiązanie dla środowisk Windows, oferując głęboką integrację z systemem operacyjnym i usługami Microsoft 365. Kaspersky Endpoint Security oferuje zaawansowaną ochronę przed zagrożeniami z możliwościami uczenia maszynowego

i analizę zachowań. Bitdefender GravityZone Business Security gwarantuje kompleksowe zabezpieczenie systemu, minimalnie wpływając na jego wydajność, a także na zaawansowane funkcje detekcji zagrożeń.

Symantec Endpoint Protection, obecnie część Broadcom, dostarcza wielowarstwową ochronę z zaawansowanymi możliwościami analizy zagrożeń. Trend Micro Apex One zapewnia automatyzowane detekcję i wsparcie w sytuacjach związanych z wykorzystaniem AI i uczenia maszynowego. Każde z tych podejść powinno być oceniane pod kątem specyficznych potrzeb organizacji, kompatybilności z istniejącą infrastrukturą, kosztów licencjonowania oraz dostępnego wsparcia technicznego.

Monitoring i zarządzanie stacjami roboczymi z Axence Navision

Axence nVision stanowi kompleksowe narzędzie zarządzania i monitorowania siecią oraz jej użytkownikami. Tym samym umożliwia inwentaryzację sprzętu i oprogramowania, zapewnia zdalne wsparcie oraz chroni dane firmowe przed wyciekami. System został zaprojektowany z myślą o łatwości wdrażania, prostocie zarządzania i przyjemności użytkowania. Osoby korzystające z oprogramowania nVision potwierdzają, że wpływa ono korzystnie na pracę działów IT, oszczędzając do 40 proc. ich czasu. Wszystko jest możliwe dzięki alertom, licznym automatyzacjom i posiadaniu wszystkich kluczowych funkcji w jednym miejscu. Kompleksowe narzędzie zarządzania infrastrukturą IT, jakim jest Navision, pozwala na spełnienie wielu kluczowych przepisów RODO, standardów International Organization for Standardization (dalej ISO), a także dyrektywy NIS2 i ustawy o ochronie sygnalistów. System umożliwia przewidywanie awarii, zanim one wystąpią, a także zapewnia minimalizację ryzyka kar za wycieki danych lub nielegalne oprogramowanie. Najnowsza wersja oferuje liczne ulepszenia helpdesku, potężny nowy silnik raportowania oraz maskowanie ekranu podczas sesji zdalnych. Funkcjonalności obejmują monitorowanie sieci i użytkowników, inwentaryzację sprzętu i oprogramowania, zdalne wsparcie, ochronę przed wyciekami danych oraz kompleksowe raportowanie zgodności.

Alternatywne rozwiązania monitorowania i zarządzania w środowiskach Windows proponują bardzo ciekawe narzędzie, jakim jest Microsoft System Center Configuration Manager (dalej SCCM). Produkt ten oferuje zaawansowane możliwości dystrybucji oprogramowania i zarządzania konfiguracją. Istnieją także systemy Statlook, eAuditor posiadające funkcję monitoringu. Z kolei ManageEngine Desktop Central jest doskonałą

alternatywą dla całościowego zarządzania komputerami stacjonarnymi, laptopami i serwerami. Z kolei Lansweeper posiada w swej funkcjonalności automatyczną inwentaryzację IT i raportowanie aktywów. Platforma społecznościowa Spiceworks zapewnia bezpłatne narzędzia monitorowania sieci i helpdesk dla małych firm. TeamViewer Business oferuje zaawansowane możliwości zdalnego dostępu i wsparcia technicznego. Wybór odpowiedniego rozwiązania powinien uwzględniać wielkość organizacji, złożoność infrastruktury IT oraz specyficzne wymagania compliance i bezpieczeństwa.

Etap 5: Zarządzanie aktualizacjami oprogramowania

Windows Server Update Services

Windows Server Update Services (dalej WSUS) pełni rolę serwera w systemie Windows Server, umożliwiając administratorom IT w całej sieci zarządzanie i dystrybucję krytycznych poprawek bezpieczeństwa oraz aktualizacji produktów Microsoft. Można powiedzieć, że WSUS działa jak centrum kontroli zdrowia i ochrony urządzeń Windows, eliminując potrzebę indywidualnych aktualizacji sprzętów poprzez zatwierdzanie ich centralnie, ustawianie harmonogramów wdrażania i ich dystrybucję w całej sieci z jednej głównej lokalizacji. Taka funkcjonalność stanowi znaczącą oszczędność czasu dla administratorów IT, którzy tym samym mogą skupić się na bardziej strategicznych zadaniach.

WSUS znacząco poprawia postawę bezpieczeństwa organizacji, umożliwiając przejęcie kontroli nad procesem aktualizacji. Administratorzy mogą priorytetyzować krytyczne poprawki bezpieczeństwa, zapewniając ich szybkie wdrożenie w całej sieci. Dodatkowo WSUS pozwala opóźnić niekrytyczne aktualizacje w celach testowych, minimalizując ryzyko nieoczekiwanych zakłóceń. System działa również jako lokalne źródło aktualizacji dla urządzeń, gdzie zatwierdzone aktualizacje są jednorazowo pobierane na serwer WSUS, co znacząco redukuje ogólne zużycie przepustowości. Ten aspekt jest szczególnie istotny dla organizacji z licznymi urządzeniami.

WSUS oferuje funkcjonalność testowania, zapewniając ochronę w zakresie sprawdzania aktualizacji przed wdrożeniem ich w całej sieci na małej grupie urządzeń. Ten fakt pomaga identyfikować i rozwiązywać potencjalne problemy kompatybilności lub błędy, zanim mogą wpłynąć na całą bazę użytkowników. System oferuje różnorodne opcje wdrażania dostosowane do różnych potrzeb organizacyjnych (w tym

automatyczne rozwiązania dla krytycznych aktualizacji bezpieczeństwa, zaplanowane przystosowania dla rutynowych aktualizacji, a także opcje testowania dla aktualizacji wymagających walidacji).

Alternatywne rozwiązania zarządzania patchami

Rynek oferuje wiele alternatywnych rozwiązań zarządzania aktualizacjami, które mogą być bardziej odpowiednie dla określonych środowisk. SecOps Solution stanowi zaawansowane narzędzie zarządzania podatnościami i poprawkami, które działa bez agentów, a także umożliwiając organizacjom szybką identyfikację, priorytetyzację i naprawę podatności w całej infrastrukturze i aplikacjach. Z kolei Automox jest natywną platformą zarządzania poprawkami w chmurze, zaprojektowaną do automatyzacji i uproszczenia patchingu w różnych systemach operacyjnych. Dla większych jednostek ta funkcjonalność jest atrakcyjna także dlatego, że posiada scentralizowany pulpit, a proces instalowania patchy odbywa się w czasie rzeczywistym.

Narzędziem służącym do automatyzacji i upraszczania procesu aktualizacji oprogramowania w sieci określonego podmiotu jest **SolarWinds Patch Manager**. Zapewnia on kompleksowe rozwiązanie zarządzania poprawkami, które integruje się z istniejącą infrastrukturą (np. WSUS i SCCM), oferując wgląd w czasie rzeczywistym, a poza tym także i automatyzację w celu utrzymania bezpieczeństwa i zgodności systemów. Innym podejściem jest GFI LanGuard, łącząc zarządzanie poprawkami ze skanowaniem podatności, zapewniając organizacjom solidne rozwiązanie do zabezpieczania systemów Windows, macOS i Linux. Z kolei **NinjaOne** tworzy nowoczesne oprogramowanie do zintegrowanego zarządzania IT poprzez kompleksowe zdalne monitorowanie i zarządzanie (w tym zarządzanie poprawkami i wdrażanie oprogramowania). A **Ivanti Patch for Windows** dostarcza automatyczne patchowanie zarówno systemów Windows i Linux, jak oferuje szerokie wsparcie dla aplikacji stron trzecich i dobrą integrację z SCCM.

Narzędzia dystrybucji oprogramowania

Ninite stanowi bezpłatne narzędzie, które w tym samym czasie upraszcza instalację wielu popularnych aplikacji. Wygląda w ten sposób, że użytkownicy wybierają pożądane programy z wyselekcjonowanej listy, a Ninite pobiera je i instaluje w usprawnionym, zautomatyzowanym procesie. Popularność Ninite wynika z łatwości użycia i unikania oprogramowania dołączonego lub bloatware, które są

często umieszczone w indywidualnych instalatorach. Użytkownicy doceniają korzyści płynące z Ninite, które obejmują bezproblemową instalację, a tym samym znacząco redukującą czas i wysiłek wymagany do wprowadzenia wielu aplikacji. Czyste instalacje zazwyczaj unikają dołączonego oprogramowania i bloatware znajdującego w wielu indywidualnych instalatorach. Łatwa deinstalacja upraszcza proces usuwania aplikacji, oferując usprawniany odpowiednik instalacji.

Alternatywne rozwiązania dystrybucji oprogramowania i inwentaryzacji zasobów:

- Chocolatey – menager pakietów dla Windows;
- PDQ Deploy & Inventory – narzędzie wdrożeniowe dla Windows;
- NinjaOne – platforma zarządzania punktami końcowymi;
- Action1 – chmurowa platforma zarządzania poprawkami;
- Atera – platforma IT All-in-One;
- Datto Remote Monitoring and Management (dalej RMM) – ujednolicona platforma centralnego zdalnego zarządzania urządzeniami końcowymi oraz całą infrastrukturą informatyczną danego podmiotu;
- Patch My Personal Computer (dalej PC) – specjalistyczne zarządzanie poprawkami;
- ManageEngine Patch Manager Plus – kompleksowe zarządzanie poprawkami.

Podsumowanie

Implementacja kompleksowej infrastruktury IT wymaga zintegrowanego podejścia uwzględniającego wszystkie przedstawione etapy. Wybór między rozwiązaniami UTM a NGFW powinien być podyktowany wielkością organizacji, dostępnymi zasobami technicznymi oraz specyficznymi wymaganiami bezpieczeństwa. Segmentacja VLAN musi być zaprojektowana z uwzględnieniem przyszłego rozwoju danego podmiotu oraz wymogów zgodności. Konfiguracja urządzeń sieciowych powinna następować zgodnie z najlepszymi praktykami bezpieczeństwa i być regularnie aktualizowana. Zabezpieczenia końcowe wymagają wielowarstwowego podejścia obejmującego ochronę antywirusową, monitoring behawioralny oraz centralne zarządzanie. System zarządzania aktualizacjami jest niezbędny dla utrzymania bezpieczeństwa całej infrastruktury i powinien być zintegrowany z pozostałymi systemami zarządzania IT.

Sukces wdrożenia zależy od właściwego planowania, testowania w środowisku pilotażowym oraz systematycznego podejścia do każdego etapu. Regularne audyty bezpieczeństwa, aktualizacja dokumentacji oraz szkolenia personelu IT są niezbędne dla

długoterminowego sukcesu infrastruktury. Monitoring wydajności i bezpieczeństwa powinien być ciągły, z możliwością szybkiego reagowania na incydenty i anomalie. Planowanie ciągłości działania oraz procedury odzyskiwania po awarii muszą być integralną częścią całej architektury IT, zapewniając określonej jednostce możliwość utrzymania operacyjności nawet w przypadku nieprzewidzianych zdarzeń.

9. Rola i kompetencje kadry zarządzającej.

Poniżej przedstawiono najważniejsze zadania kierowników jednostek i najwyższego kierownictwa w kontekście budowania sprawnego systemu zarządzania bezpieczeństwem informacji.

Na poziomie zarządczym

Skuteczne zarządzanie bezpieczeństwem informacji i infrastrukturą informatyczną w JST, a także w podległych im placówkach oświatowych wymaga pełnego zaangażowania kierownictwa, zarówno w aspekcie strategicznym, jak i operacyjnym. Na poziomie zarządczym najważniejszym elementem jest zrozumienie formalnoprawnej odpowiedzialności ponoszonej przez JST oraz ich przedstawicieli w zakresie zgodności z przepisami prawa (w szczególności z RODO, ustawą o krajowym systemie cyberbezpieczeństwa oraz rozporządzeniem w sprawie KRI).

Świadomość odpowiedzialności formalnoprawnej

Kierownictwo JST musi być świadome, że to na nim spoczywa odpowiedzialność za wdrożenie i nadzorowanie zgodności organizacji z przepisami dotyczącymi ochrony danych i cyberbezpieczeństwa. Obejmuje to nie tylko zapewnienie, że jednostki przetwarzające dane osobowe wdrożyły odpowiednie środki techniczne i organizacyjne, ale również że są one dokumentowane, utrzymywane i okresowo weryfikowane. Brak należytej staranności w tym zakresie może skutkować konsekwencjami administracyjnymi, finansowymi, a nawet odpowiedzialnością osobistą decydentów. Rola kierownictwa nie ogranicza się więc do zatwierdzania dokumentów, lecz obejmuje aktywne podejmowanie decyzji i nadzór nad realizacją obowiązków wynikających z prawa.

Komunikacja z innymi interesariuszami

Jednym z istotnych zadań zarządczych jest zapewnienie sprawnej i efektywnej komunikacji pomiędzy wszystkimi podmiotami zaangażowanymi w system zarządzania IT i bezpieczeństwem informacji. Dotyczy to zarówno komunikacji wewnętrznej (z dyrektorami szkół i jednostkami organizacyjnymi), jak i zewnętrznej (z dostawcami usług informatycznych, instytucjami nadzorczymi, audytorami czy innymi organami samorządowymi). Kierownictwo musi rozumieć, że skuteczność systemu bezpieczeństwa opiera się nie tylko na technologii, ale przede wszystkim na współpracy i wymianie informacji. Regularne spotkania, konsultacje, przekazywanie decyzji i zbieranie informacji zwrotnych są nieodzowne dla budowania spójnego i odpornego środowiska informacyjnego.

Wsparcie i nadzór nad procesem rekrutacji i rozwoju kadry informatycznej

Niedobór wykwalifikowanych pracowników IT w sektorze publicznym jest problemem ogólnokrajowym. W związku z tym kierownictwo JST powinno odgrywać aktywną rolę w procesie planowania zatrudnienia, definiowania kompetencji wymaganych od kandydatów oraz wspierania rozwoju już zatrudnionych pracowników. Odpowiednie wsparcie oznacza nie tylko zabezpieczenie środków finansowych, ale również wprowadzenie systemowych działań (np. programów szkoleniowych, mentoringu czy ścieżek awansu). Kierownictwo musi również podejmować decyzje w sytuacjach rotacji personelu, zapewniając płynność operacyjną i zachowanie ciągłości wiedzy w organizacji.

Na poziomie przywódczym

Poza obowiązkami wynikającymi z przepisów prawa i zarządzania personelem, kierownictwo pełni także funkcję przywódczą, która ma bezpośredni wpływ na kulturę organizacyjną, podejście do innowacji technologicznych oraz sposób postrzegania bezpieczeństwa informacji przez pracowników. To właśnie liderzy nadają kierunek rozwojowi cyfryzacji i odpowiadają za tworzenie środowiska pracy sprzyjającego skutecznej i bezpiecznej realizacji zadań publicznych.

Kształtowanie kultury organizacyjnej uwzględniającej bezpieczeństwo informacji

Tworzenie kultury organizacyjnej opartej na świadomości zagrożeń i odpowiedzialności za dane to jedno z najważniejszych zadań przywódczych. Oznacza to, że kierownictwo

powinno nie tylko promować zasady ochrony informacji, ale również egzekwować ich przestrzeganie i dawać przykład właściwego postępowania. Kultura bezpieczeństwa powinna być widoczna w codziennych działaniach, poczynając od sposobu logowania się do systemów, przez zasady korzystania z nośników danych, aż po reagowanie na incydenty. Taka postawa wzmacnia zaufanie wewnętrzne i zewnętrzne, a ponadto minimalizuje ryzyko błędów wynikających z ludzkiej nieuwagi lub nieświadomości.

Tworzenie polityki budżetowej, planowanie inwestycji i ustalanie priorytetów w zakresie IT

Rozwój infrastruktury IT i systemów bezpieczeństwa wymaga odpowiedniego finansowania, co z kolei wiąże się z koniecznością planowania strategicznego. Kierownictwo odpowiada za określenie celów inwestycyjnych, nadanie priorytetów oraz zapewnienie równowagi pomiędzy kosztami a ryzykiem. Należy brać pod uwagę zarówno inwestycje w sprzęt i oprogramowanie, jak i koszty operacyjne, szkoleniowe oraz audytowe. Długofalowe planowanie (np. cyklu życia urządzeń, wymiany systemów czy wdrażania nowych rozwiązań chmurowych) musi być elementem budżetów wieloletnich i dostosowane do możliwości finansowych jednostki.

Promowanie systematycznych szkoleń i podnoszenia kwalifikacji personelu

Bezpieczne zarządzanie informacją nie jest możliwe bez odpowiednich kompetencji wśród pracowników. Zadaniem kierownictwa jest inicjowanie i wspieranie działań szkoleniowych, nie tylko dla pracowników technicznych, ale również dla użytkowników końcowych. Należy zapewnić regularne szkolenia w zakresie cyberbezpieczeństwa, ochrony danych osobowych, obsługi systemów informatycznych oraz reagowania na incydenty. Równocześnie warto promować kulturę ciągłego uczenia się, zachęcając do korzystania z kursów online, udziału w konferencjach czy certyfikacji branżowych. Dobrze zaplanowana strategia rozwoju kompetencji przekłada się bezpośrednio na odporność organizacyjną i stabilność procesów informacyjnych w JST i placówkach oświatowych.

10. Rola i kompetencje kadry informatycznej.

Współczesna kadra informatyczna w JST oraz w podległych placówkach edukacyjnych odgrywa coraz ważniejszą rolę w zapewnieniu ciągłości działania, bezpieczeństwa informacji oraz sprawnego zarządzania zasobami IT. Obecnie – w dobie rosnących zagrożeń cyfrowych, dynamicznego rozwoju technologii, a także coraz bardziej rygorystycznych wymagań prawnych – od informatyków oczekuje się nie tylko znajomości technologii, ale również kompetencji doradczych, analitycznych i organizacyjnych. Zadania specjalistów IT obejmują nie tylko bieżące utrzymanie systemów, ale również długofalowe planowanie, zarządzanie ryzykiem i aktywne wspieranie procesów decyzyjnych.

Nowe wyzwania dla informatyków

Odejście od postrzegania pracownika IT jako „osoby od wymiany tonera i myszki” na rzecz traktowania go jako specjalisty odpowiedzialnego za sieci, bezpieczeństwo i zarządzanie infrastrukturą

Tradycyjne pojmowanie roli informatyka jako osoby zajmującej się sprzętem biurowym, instalacją drukarek czy naprawą komputerów, jest dziś całkowicie nieadekwatne do rzeczywistych wymagań funkcjonowania nowoczesnej infrastruktury IT w jednostkach publicznych. Kadra informatyczna musi obecnie pełnić funkcję specjalistów z zakresu bezpieczeństwa informacji, architektów sieci, administratorów systemów. Niejednokrotnie informatycy pełnią rolę również doradców w zakresie zakupów sprzętu i oprogramowania. Oczekuje się od nich biegłości w zarządzaniu serwerami, sieciami lokalnymi i rozległymi, systemami backupu oraz rozwiązań chmurowych.

Dodatkowo informatyk musi rozumieć kontekst prawny swojej pracy, wykazując się znajomością podstawowych wymagań wynikających z przepisów RODO, KRI oraz ustawy o krajowym systemie cyberbezpieczeństwa. Brak tej wiedzy przekłada się bezpośrednio na ryzyko formalne dla placówki i całego JST. W wielu przypadkach informatyk staje się więc kluczowym doradcą kierownictwa w zakresie implementacji zabezpieczeń i organizacji systemu zarządzania informacją.

Kompleksowe wsparcie placówek w zakresie konfiguracji urządzeń, planowania zakupów, aktualizacji oprogramowania czy monitorowania ruchu w sieci

Wyzwania, z jakimi mierzy się dziś kadra informatyczna, obejmują nie tylko obsługę bieżących potrzeb technicznych, ale także zapewnienie kompleksowego wsparcia dla placówek w zakresie doboru odpowiednich rozwiązań sprzętowych i programowych. Informatyk powinien brać udział w procesie planowania zakupów, wspierać wybór dostawców, weryfikować kompatybilność z istniejącą infrastrukturą i przewidywać potrzeby eksploatacyjne w dłuższej perspektywie. Wymaga to zarówno umiejętności technicznych, jak i kompetencji komunikacyjnych oraz analizy potrzeb użytkowników końcowych.

Konfiguracja urządzeń sieciowych, wdrażanie polityk bezpieczeństwa, prowadzenie aktualizacji, testowanie poprawności działania systemów wymaga od kadry IT wiedzy eksperckiej i stałego doskonalenia zawodowego. Coraz większego znaczenia nabiera także umiejętność monitorowania ruchu w sieci, identyfikowania nietypowych zdarzeń oraz wykorzystania narzędzi klasy Endpoint Detection and Response (dalej EDR), Extended Detection and Response (dalej XDR) czy Security Information and Event Management (dalej SIEM), jeśli takie zostały wdrożone. Informatyk musi być również w stanie opracować raporty stanowiące podstawę do audytów lub przeglądów SZBI, oraz rekomendować działania naprawcze lub zapobiegawcze.

Znajomość potrzeb jednostki

Dostosowanie sprzętu i oprogramowania do konkretnych celów szkoły lub urzędu

Rola informatyka nie ogranicza się do zapewnienia „działającej infrastruktury”, lecz obejmuje aktywne dopasowywanie rozwiązań IT do zadań realizowanych przez jednostkę. Oznacza to konieczność znajomości celów funkcjonowania szkoły, przedszkola, jednostki oświatowej lub samorządowej (zarówno administracyjnych, jak i edukacyjnych). W przypadku placówek edukacyjnych specjalista IT powinien rozumieć potrzeby związane z prowadzeniem lekcji informatyki, korzystaniem z narzędzi edukacyjnych, obsługą dzienników elektronicznych, platform e-learningowych czy systemów egzaminacyjnych.

W JST rola informatyka obejmuje nieco inne zadania (np. wsparcie systemów finansowo-księgowych, obiegu dokumentów czy obsługi rejestrów). Kadra informatyczna – niezależnie od typu placówki – musi umieć przewidzieć wymagania

sprzętowe i programowe, rekomendować rozwiązania zgodne z przepisami oraz przewidywać ich wpływ na użytkowników i procesy. Często to właśnie informatyk jest osobą oceniającą, czy proponowane zakupy są uzasadnione i czy możliwe jest ich efektywne wykorzystanie w istniejącym środowisku.

Utrzymanie wysokiego poziomu bezpieczeństwa (tworzenie kopii zapasowych, reagowanie na incydenty, kontrola dostępu, wykrywanie zagrożeń)

Bezpieczeństwo informacji to jeden z głównych obszarów odpowiedzialności kadry IT. Informatyk musi zapewnić, że dane przechowywane i przetwarzane w systemach są odpowiednio chronione (zarówno przed awariami technicznymi, jak i przed nieautoryzowanym dostępem). Do obowiązków tego specjalisty należy m.in. wdrożenie i cykliczne testowanie mechanizmów kopii zapasowych, weryfikacja ich poprawności oraz planowanie polityk odtworzeniowych. Informatyk jest także odpowiedzialny za zapewnienie odpowiedniego poziomu kontroli dostępu poprzez wdrożenie systemu haseł, logowania dwuskładnikowego, segmentacji sieci i uprawnień użytkowników.

W zakresie wykrywania zagrożeń specjalista IT powinien musi wykazać się nie tylko znajomością oprogramowania antywirusowego, ale także bardziej zaawansowanych narzędzi do analizy zachowań systemowych i anomalii sieciowych. Wiedza o aktualnych wektorach ataków, lukach bezpieczeństwa i dobrych praktykach hardeningu systemów powinna być stale aktualizowana. Informatyk pełni zatem funkcję pierwszej linii obrony, a jego skuteczność decyduje o poziomie odporności całej placówki lub urzędu na cyberzagrożenia.

Zarządzanie ryzykiem i incydentami

Rozpoznawanie symptomów wycieku danych czy zaszyfrowania plików i podejmowanie szybkich działań

Jednym z najważniejszych zadań kadry informatycznej jest zdolność szybkiego rozpoznania incydentu zagrażającego bezpieczeństwu systemu informacyjnego. Może to być podejrzany ruch sieciowy, nieautoryzowany dostęp do zasobów, nietypowe działanie stacji roboczych lub szyfrowanie plików będące wynikiem ataku ransomware. Informatyk powinien być przeszkolony w zakresie identyfikacji symptomów ataku i posiadać procedury pozwalające na szybkie odizolowanie zagrożenia, zablokowanie punktu wejścia i zabezpieczenie danych przed dalszą utratą.

Czas reakcji na incydent ma ogromne znaczenie, ponieważ opóźnienie w tym zakresie (nawet o kilkanaście minut) może skutkować nieodwracalnymi stratami. Dlatego pracownik IT powinien mieć nie tylko wiedzę, ale również dostęp do odpowiednich narzędzi oraz uprawnień umożliwiających natychmiastowe działanie. Regularne szkolenia i udział w ćwiczeniach symulacyjnych pozwalają utrzymać gotowość operacyjną i poprawiają jakość reakcji w sytuacjach kryzysowych.

Informowanie decydentów o koniecznych krokach prawnych i organizacyjnych (zgłaszanie incydentów, wdrażanie procedur awaryjnych)

W sytuacji wykrycia incydentu informatyk musi również pełnić rolę łącznika między technicznym poziomem zagrożenia a pionem decyzyjnym. Oznacza to nie tylko dokumentowanie zdarzenia, ale także jego właściwą klasyfikację i ocenę skutków. To specjalista IT powinien poinformować o zaistniałej sytuacji dyrekcję szkoły, przedszkola lub innej placówki edukacyjnej lub samorządowej albo inspektora RODO. Ponadto obowiązkiem informatyka jest także wskazanie możliwych scenariuszy działań, poczynwszy od uruchomienia procedur awaryjnych, aż po zgłoszenie incydentu do organów nadzorczych.

Tak różnorodny zakres zadań wymaga od pracownika IT posiadania umiejętności formułowania wniosków, oceny ryzyka oraz wskazania niezbędnych kroków formalnych (np. przygotowania materiałów do zgłoszenia naruszenia RODO, ochrony danych osobowych zgodnie z wymaganiami RODO). Dobrze funkcjonująca kadra informatyczna powinna wyróżniać się nie tylko wiedzę techniczną, ale także umiejętnością współpracy z administracją, prawnikiem czy koordynatorem SZBI.

Podsumowanie

W czasach współczesnych dynamiczny rozwój technologii cyfrowych, rosnące wymagania prawne oraz potrzeba efektywnego zarządzania informacją sprawiają, że jednostki samorządu terytorialnego oraz podległe im placówki oświatowe stają przed koniecznością systemowego podejścia do zarządzania infrastrukturą IT i bezpieczeństwem informacji. W niniejszym opracowaniu przedstawiono kluczowe modele organizacyjne, wyzwania, role oraz rekomendacje, które mają na celu wsparcie JST w budowaniu skutecznych i odpornych struktur zarządzania technologią informacyjną.

Punktem wyjścia była analiza trzech modeli zarządzania infrastrukturą informatyczną (zdecentralizowanego, scentralizowanego i hybrydowego) z uwzględnieniem aspektów organizacyjnych, finansowych i bezpieczeństwa. Każdy z wariantów niesie ze sobą określone korzyści, ale również ryzyka i ograniczenia, których świadomość jest niezbędna przy podejmowaniu decyzji strategicznych. Model zdecentralizowany zapewnia elastyczność i szybkość działania na poziomie placówki, ale wiąże się z wysokimi kosztami i trudnościami w utrzymaniu jednolitego poziomu bezpieczeństwa. Z kolei model scentralizowany oferuje spójność i efektywność kosztową, lecz wymaga dobrej komunikacji z jednostkami podległymi i może ograniczać reagowanie na lokalne potrzeby. Wariant hybrydowy stanowi kompromis między elastycznością a standaryzacją, a przy odpowiedniej koordynacji i wsparciu może być najbardziej efektywnym rozwiązaniem dla wielu JST.

Istotnym elementem dokumentu było także wskazanie roli najwyższego kierownictwa, zarówno na poziomie zarządczym, jak i przywódczym. Podkreślono, że skuteczna polityka bezpieczeństwa informacji wymaga zaangażowania liderów, którzy rozumieją swoją odpowiedzialność prawną, wspierają budowę kultury bezpieczeństwa, a także aktywnie uczestniczą w procesach decyzyjnych i planowaniu inwestycji. Kierownictwo musi nie tylko nadzorować, ale i promować działania wzmacniające odporność cyfrową organizacji, w tym wspierać rozwój kompetencji kadry oraz monitorować efektywność wdrażanych rozwiązań.

Szczególną uwagę poświęcono również roli kadry informatycznej. Współczesny informatyk w JST lub placówce edukacyjnej posiada różnorodne obowiązki. Okazuje się bowiem, że specjalista IT pełni już nie tylko rolę technika od problemów sprzętowych, ale jest także ekspertem odpowiedzialnym za bezpieczeństwo danych, planowanie zakupów, monitorowanie sieci, a także wsparcie użytkowników i doradztwo dla kierownictwa. Kompetencje te muszą być nieustannie rozwijane, a ich znaczenie doceniane zarówno na poziomie organizacyjnym, jak i strategicznym. Zdolność kadry IT do zarządzania ryzykiem, reagowania na incydenty oraz komunikowania się z decydentami ma bezpośredni wpływ na odporność całego systemu edukacyjnego.

Niniejsze opracowanie podkreśla również znaczenie szkoleń i systematycznego podnoszenia świadomości w zakresie bezpieczeństwa informacji. Zarówno kadra kierownicza, jak i użytkownicy systemów powinni być objęci procesem edukacyjnym, który umożliwi im nie tylko lepsze wykorzystanie dostępnych narzędzi, ale również

zrozumienie ich wpływu na ochronę danych i ciągłość działania. Tylko instytucje świadome zagrożeń i wyposażone w wiedzę będą w stanie skutecznie im przeciwdziałać.

Warto też podkreślić, że opracowany materiał kładzie nacisk na potrzebę elastycznego, ale przemyślanego podejścia do zarządzania technologią w oświacie. Każda JST działa w specyficznych warunkach lokalnych i organizacyjnych, dlatego wdrażane rozwiązania muszą uwzględniać realne możliwości, uwarunkowania kadrowe i infrastrukturalne. Wszelkie wskazania zawarte w niniejszym opracowaniu mają służyć jedynie jako punkt odniesienia, nie sztywny schemat. Celem zaprezentowanych rekomendacji jest wspieranie jednostek w budowaniu zintegrowanych, bezpiecznych i nowoczesnych systemów zarządzania informacją, które będą korzystne dla placówek edukacyjnych, samorządowych i społeczności lokalnych.

MATERIAŁ 5. ROZWIĄZANIA WSPIERAJĄCE JAKOŚCIOWY ROZWÓJ CYFRYZACJI W EDUKACJI

Dorota Pintał

Ważne!

Materiał 5. stanowi inspirację do zaplanowanych warsztatów i wykładów w programie szkoleniowo-doradczym. To zbiór praktycznych rozwiązań funkcjonujących w szkołach.

Wprowadzenie.

Współczesna edukacja stoi przed wieloma wyzwaniami i możliwościami, które wynikają z dynamicznego rozwoju technologii cyfrowych. ORE, wychodząc naprzeciw potrzebom rozwojowym, a także odpowiadając na aktualne potrzeby środowiska samorządowego (uwidocznione podczas kryzysu wywołanego pandemią COVID-19) realizuje projekt „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego”.

Niniejszy materiał ma na celu przedstawienie najważniejszych aspektów związanych z cyfryzacją edukacji, a także wskazanie dobrych praktyk, które mogą wspierać procesy edukacyjne, a także zarządzanie placówkami oświatowymi i samorządowymi. W tym opracowaniu zawarto też treści, które odnoszą się do zagadnień związanych z rozwijaniem kompetencji cyfrowych uczniów.

W materiale omówiono kompetencje podstawowe i przekrojowe, które stanowią fundament dla planowania i wdrażania zmian w edukacji. W rozdziale „Cyberedukacja w centrum uwagi” skupiono się na roli nauczania cyfrowego w nowoczesnym systemie edukacyjnym.

Kolejne rozdziały poświęcone są dobrym praktykom w zakresie cyfryzacji, zarówno w zarządzaniu szkołą, jak i w organizowaniu procesów edukacyjnych. W niniejszej pracy zaprezentowano możliwości i wyzwania związane z wykorzystaniem AI w edukacji, które z jednej otwierają nowe perspektywy, ale z drugiej wymagają również odpowiedzialnego podejścia.

W materiale znajdują się różnorodne inspiracje do organizacji procesu edukacyjnego z wykorzystaniem ZPE. Ponadto w niniejszym opracowaniu wskazano zagrożenia związane z cyberbezpieczeństwem w edukacji.

Przedstawione treści będą cennym źródłem wiedzy i inspiracji dla wszystkich zaangażowanych w rozwój cyfryzacji w szkołach, przedszkolach i placówkach oświatowych.

1. Kompetencje przekrojowe i podstawowe jako punkt wyjścia do planowania oraz wdrażania zmian w edukacji.

Współczesne systemy edukacyjne stoją przed wyzwaniem dostosowania się do dynamicznie zmieniającego się świata. Najważniejszym elementem tego procesu jest rozwijanie kompetencji przekrojowych i podstawowych, które stanowią fundament dla efektywnego uczenia się i adaptacji do nowych warunków. Znaczenie tego faktu podkreśla ZSU 2030⁵⁰ na mocy uchwały nr 195/2020 z 28 grudnia 2020 roku. Dokument ten stanowi ramy strategiczne dla polityki edukacyjnej, która zmierza do wzmocnienia kapitału społecznego, włączenie społeczne oraz wzrost gospodarczy.

⁵⁰ Ministerstwo Edukacji Narodowej. Departament Innowacji i Rozwoju, (2020), „Zintegrowana Strategia Umiejętności 2030”, Warszawa, zob. <https://zsu2030.mein.gov.pl/#zsu> [dostęp, online dn. 2.09.2025].

Kompetencje podstawowe obejmują umiejętności, które są niezbędne do funkcjonowania w społeczeństwie i na rynku pracy. Należą do nich⁵¹:

rozumienie i tworzenie informacji – zdolność identyfikowania, rozumienia, wyrażania, tworzenia i interpretowania pojęć, uczuć, faktów i opinii w mowie i piśmie, przy wykorzystaniu obrazów, dźwięków i materiałów cyfrowych we wszystkich dziedzinach i kontekstach; zdolność skutecznego komunikowania się i porozumiewania się z innymi osobami, we właściwy i kreatywny sposób;

- wielojęzyczność – zdolność do prawidłowego i skutecznego korzystania z różnych języków w celu porozumiewania się; zdolność rozumienia, wyrażania i interpretowania pojęć, myśli, uczuć, faktów i opinii w mowie i piśmie w odpowiednim zakresie kontekstów społecznych i kulturowych, w zależności od potrzeb lub pragnień danej osoby;
- umiejętności matematyczne – zdolność rozwijania i wykorzystywania myślenia matematycznego w celu rozwiązywania problemów wynikających z codziennych sytuacji; zdolność i chęć wykorzystywania matematycznych sposobów myślenia (myślenie logiczne i przestrzenne) oraz prezentacji (wzory, modele, konstrukty, wykresy, tabele);
- umiejętności w zakresie nauk przyrodniczych, technologii i inżynierii – zdolność i chęć wykorzystywania istniejącego zasobu wiedzy i metodologii do wyjaśniania świata przyrody, w celu formułowania pytań i wyciągania wniosków opartych na dowodach; wykorzystanie wiedzy i metod w odpowiedzi na postrzegane ludzkie potrzeby lub wymagania; rozumienie zmian powodowanych przez działalność ludzką oraz odpowiedzialności za nie.

Te umiejętności są podstawą do tego, aby budować bardziej zaawansowane kompetencje i umiejętności specjalistyczne.

Kompetencje przekrojowe to umiejętności, które są przydatne w różnych kontekstach i dziedzinach życia. Obejmują umiejętności⁵²:

- cyfrowe;
- osobiste, społeczne i w zakresie uczenia się;
- obywatelskie;
- w zakresie przedsiębiorczości;
- w zakresie świadomości i ekspresji kulturalnej;

⁵¹ Ibidem.

⁵² Ibidem.

- w zakresie myślenia krytycznego i kompleksowego rozwiązywania problemów;
- w zakresie pracy zespołowej;
- zdolność adaptacji do nowych warunków;
- przywódcze;
- związane z wielokulturowością;
- związane z kreatywnością i innowacyjnością.

Cyfrowe kompetencje obejmują pewne, krytyczne i odpowiedzialne korzystanie z technologii cyfrowych w nauce, pracy i uczestnictwie w społeczeństwie. Poza tym obecność tego rodzaju umiejętności pozwala na swobodne i bezpieczne korzystania z informacji i danych, komunikację i współpracę, korzystanie z mediów, tworzenie treści cyfrowych (w tym programowanie), bezpieczeństwo cyfrowe, kwestie własności intelektualnej, rozwiązywanie problemów i krytyczne myślenie.

Kompetencje osobiste, społeczne i w zakresie uczenia się obejmują zdolność do autorefleksji, skutecznego zarządzania czasem i informacjami, konstruktywnej współpracy z innymi oraz zachowania odporności. Ważne jest zarządzanie własnym procesem edukacji i karierą, radzenie sobie z niepewnością i złożonością, wspieranie dobrostanu fizycznego i emocjonalnego, utrzymanie zdrowia fizycznego i psychicznego, prowadzenie prozdrowotnego trybu życia, odczuwanie empatii oraz zarządzanie konfliktami w inkluzywnym i wspierającym kontekście.

Kompetencje obywatelskie charakteryzują się zdolnością do działania jako odpowiedzialni obywatele, a także uprawniają do pełnego uczestnictwa w życiu obywatelskim i społecznym. Ten rodzaj umiejętności wyrasta ze zrozumienia pojęć i struktur społecznych, gospodarczych, prawnych i politycznych, a także wydarzeń globalnych i zrównoważonego rozwoju.

Kompetencje w zakresie przedsiębiorczości wiążą się zarówno ze zdolnością wykorzystywania szans i pomysłów, jak i przekształcania ich w wartość dla innych. To taka odmiana umiejętności, która opiera się na kreatywności, krytycznym myśleniu, rozwiązywaniu problemów, podejmowaniu inicjatywy, wytrwałości oraz zdolności do wspólnego działania przy planowaniu i zarządzaniu projektami o wartości kulturalnej, społecznej lub finansowej.

Świadomość i ekspresję kulturalną wyróżnia znajomość różnych kultur i sposobów ekspresji na poziomie lokalnym, regionalnym, krajowym, europejskim i światowym. Ważne jest zrozumienie, jak te sposoby wpływają zarówno na siebie nawzajem, jak

i na pomysły poszczególnych jednostek. Kompetencje w zakresie przedsiębiorczości tworzą różne formy przekazywania idei (np. teksty pisane, teatr, film, taniec, gry, sztuka, muzyka, rytuały i architektura, a także formy hybrydowe). Niezwykle istotne – w kontekście różnorodności kulturowej i funkcji pełnionej przez sztukę, a także jej oraz roli w postrzeganiu i kształtowaniu świata – jest również rozumienie własnej tożsamości twórczej i dziedzictwa kulturowego. Nie bez znaczenia pozostają także zdolności empatycznego wyrażania i interpretowania idei, doświadczeń i emocji w różnych formach sztuki, a także umiejętność wykorzystywania tych możliwości do uzyskania wartości osobistej.

Kompetencje w zakresie myślenia krytycznego i kompleksowego rozwiązywania problemów obejmują gotowość do przemyślanego rozpatrywania trudności lub zagadnień oraz znajomość i umiejętność stosowania logicznych metod rozumowania pojmowania wszelkich zawiłości i dociekania sposobów ich wyjaśnienia.

Kompetencje w zakresie pracy zespołowej koncentrują się na rozwijaniu umiejętności efektywnej pracy w grupach, dążeniu do wspólnego celu, zdolności do kompromisu, elastyczności, otwartości na pomoc innym, a także przyjęcie odpowiedzialności za wspólne wyniki i proces uczenia się.

Zdolność adaptacji do nowych warunków obejmuje szybkie przystosowanie się do odmiennych ról i obowiązków, umiejętność odnalezienia się w nowym zespole oraz efektywną pracę w zmieniających się warunkach i priorytetach.

Kompetencje przywódcze odnoszą się do:

- planowania i podejmowania działań pomagających w realizacji wyznaczonych celów;
- wykorzystania umiejętności interpersonalnych do rozwiązywania problemów;
- skutecznej realizacji działań;
- korzystania z wiedzy i doświadczenia praktycznego innych osób dla osiągnięcia wspólnego celu;
- odpowiedzialnego działania w interesie grupy;
- organizacji i prowadzenia pracy zespołowej.

Kompetencje związane z wielokulturowością wyróżnia otwarta postawa, produktywna i autentyczna współpraca z innymi, odwoływanie się do kolektywnej mądrości grupy, pokonywanie różnic kulturowych i analizowanie problemów z różnych perspektyw w celu podniesienia innowacyjności i jakości pracy.

Kompetencje związane z kreatywnością i innowacyjnością obejmują zdolność (także we współpracy) do tworzenia, wyrażania i stosowania nowych, wartościowych pomysłów, technik i perspektyw. Ta odmiana umiejętności obejmuje zarówno biegłość w wymyślaniu rozwiązań wykraczających poza schematy, jak i eksperymentowanie z nowatorskimi i niekonwencjonalnymi podejściami w celu osiągnięcia wartościowych rezultatów.

Kompetencje przekrojowe i podstawowe są niezbędne dla przygotowania uczniów do życia w szybko zmieniającym się świecie. Rozwijanie tego rodzaju umiejętności powinno być priorytetem w planowaniu i wdrażaniu zmian w edukacji. Wymaga to strategicznego podejścia, począwszy od diagnozy potrzeb (czyli identyfikacji obszarów, w których uczniowie potrzebują wsparcia), poprzez projektowanie programów nauczania, które będą integrowały rozwijanie kompetencji, szkolenia zapewniające nauczycielom odpowiednie narzędzia i metody nauczania, aż po monitorowanie i ewaluację podejmowanych działań i osiągniętych rezultatów.

Związki pomiędzy rozwijaniem kompetencji przekrojowych i podstawowych a planowaniem zmian w edukacji można poprzeć wieloma przykładami. Poniżej zamieszczono kilka najbardziej znaczących:

- w obszarze planowania zmian w edukacji istotne staje się wprowadzenie nowych metod nauczania i programów edukacyjnych wymagających kreatywnego podejścia i innowacyjnych rozwiązań, zaś analiza potrzeb edukacyjnych i ocena skuteczności różnych strategii wymaga krytycznego myślenia;
- w obszarze wdrażania zmian ważna jest praca zespołowa, co wymaga współpracy nauczycieli, administracji i uczniów, ponadto kadra nauczycielska i społeczność uczniowska muszą być elastyczni wobec nowych metod i technologii;
- w obszarze cyfryzacji niezwykle ważna jest integracja technologii cyfrowych i rozwijanie umiejętności korzystania z narzędzi internetowych;
- zmiany w edukacji często kładą nacisk na rozwój umiejętności interpersonalnych, zarządzania czasem i autorefleksji;
- edukacja uwzględniająca zmiany społeczne i globalne pomaga uczniom zrozumieć ich rolę jako obywateli świata, co sprzyja rozwijaniu kompetencji obywatelskich;
- bardzo ważne dla rozwijania przedsiębiorczości jest wdrażanie nowych projektów edukacyjnych, co z kolei wymaga inicjatywy i wytrwałości.

W wielu krajach wprowadzono już programy, które skutecznie integrują rozwijanie kompetencji przekrojowych i podstawowych. Przykładowo w Finlandii system edukacji kładzie duży nacisk na rozwijanie umiejętności krytycznego myślenia i współpracy już wśród najmłodszych dzieci. W Polsce to ZSU 2030 stanowi ramy dla rozwijania tych kompetencji na poziomie krajowym i regionalnym.

2. Cyberedukacja w centrum uwagi.

W dzisiejszym świecie technologie cyfrowe są obecne we wszystkich obszarach naszego życia (np. komunikacji i pracy, zdrowiu, dostępie do rozrywki). Dynamiczny rozwój technologii cyfrowych sprawia, że edukacja przechodzi rewolucję, która zmienia sposób uczenia przez nauczycieli, jak i uczenia się przez uczniów. Zatem w centrum uwagi pozostaje aktualnie cyberedukacja, czyli wykorzystanie nowoczesnych narzędzi i platform cyfrowych w procesie edukacyjnym. Proces ten znacznie przyspieszył w czasie pandemii COVID-19. Nastąpił wówczas znaczny wzrost z używania narzędzi edukacyjnych online oraz korzystania z platform umożliwiających zdalne nauczanie.

Wraz z rozwojem cyfryzacji zmieniają się metody nauczania. Edukacja nie polega już tylko na tradycyjnym przekazywaniu wiedzy, ale zostaje wzbogacona o rozwiązania oparte na technologii. Pojawiają się nowe sposoby pracy, których powodzenie jest uzależnione od technologii (np. webquest czy lekcja odwrócona). Te wszystkie elementy sprzyjają rozwijaniu kompetencji podstawowych i przekrojowych.

Do aktywizujących metod pracy z uczniami zostają włączane TIK, tym samym ukierunkowując działania na rozwijanie motywacji wewnętrznej społeczności uczniowskiej. Zagadnienie technologii w nauczaniu zostało opisane przez dr Rubena Puentedurę, który określił je jako model Substitution Augmentation Modification Redefinition (dalej SAMR).

S	substitution – podstawienie
A	augmentation - powiększenie
M	modification - modyfikacja
R	redefinition - redefinicja

Rysunek 1. Model SAMR.

Substitution – nowoczesne technologie zastępujące działania wykonywane tradycyjnie (np. używanie przez nauczyciela tablicy interaktywnej tylko do pisania, zastąpienie podręcznika papierowego jego wersją elektroniczną służącą wyłącznie do pozyskiwania informacji; przygotowywanie przez prowadzących prezentacji multimedialnych i wyświetlanie ich uczniom, ale połączone z tradycyjnym przekazywaniem informacji; zapisywanie przez nauczyciela treści zadania w pliku tekstowym, a następnie prezentowanie go uczniom za pomocą rzutnika multimedialnego). Na tym poziomie nauczyciel nadal pełni rolę klasyczną, jest bowiem w centrum uwagi, zaś uczniowie są nastawieni na odbiór wiedzy przekazywanej w taki sposób.

Augmentation – na tym poziomie zwiększa się zaangażowanie uczniów, a TIK wykorzystywany jest jako narzędzie rozwiązywania podstawowych problemów.

Modification – na tym poziomie TIK staje się konieczny do wykonania określonych zadań, a uczniowie są bezpośrednio angażowani w przygotowanie zadania.

Redefinition – w tym obszarze dochodzi do zamiany tradycyjnych ról nauczyciel – uczeń. Dzieci i młodzież znajdują się w centrum uwagi, stając się twórcami swojego procesu uczenia się. Ponadto rozwijają kreatywność i innowacyjność poprzez samodzielną decyzję o tym, co i w jaki sposób chcą robić. W tym modelu nauczyciel przyjmuje rolę moderatora. Ważnym elementem tego poziomu jest TIK.

Wraz z rozwojem technologii rośnie ryzyko cyberataków, oszustw internetowych, kradzieży danych czy cyberprzemocy. Cyberedukacja pozwala na dostęp do wiedzy i umiejętności w zakresie bezpieczeństwa w sieci. Uczy, jak skutecznie zabezpieczyć się przed zagrożeniami, jak wykryć oszustwo online i w jaki sposób najlepiej schronić

swoją prywatność. Zaś w związku z rosnącym wykorzystaniem danych generowanych i przechowywanych online, wprowadzane są nowe rozwiązania dotyczące ochrony danych (np. w większości krajów europejskich obowiązuje RODO). Cyberedukacja odgrywa niebagatelną rolę w ich wdrożeniu.

Cyberedukacja pomaga również zapobiegać wykluczeniu cyfrowemu, czyli sytuacji, w której określone grupy społeczne (np. osoby starsze, osoby z regionów wiejskich, czy z niepełnosprawnością) mają słaby dostęp do nowych technologii. Możliwości inicjatyw edukacyjnych, które koncentrują się na nauce korzystania z komputera i internetu zapobiegają temu wykluczeniu.

Podsumowanie

Zjawisko cyberedukacji z kilku istotnych powodów znajduje się w centrum zainteresowania:

- bezpieczeństwo w sieci – z uwagi na rosnącą liczbę zagrożeń edukacja w zakresie bezpieczeństwa staje się niezbędną;
- rozwój kompetencji cyfrowych – umiejętności cyfrowe stają się konieczne nie tylko w życiu osobistym, ale też zawodowym;
- przygotowanie do przyszłości – technologie odgrywają ważną rolę w edukacji i na rynku pracy;
- świadomość zagrożeń – rośnie świadomość zagrożeń i umiejętność bronić się przed nimi.

Na wyzwania związane z cyberedukacją odpowiadają instytucje państwowe. W 2022 roku – w ramach współpracy Ministerstwa Cyfryzacji oraz NASK – Państwowego Instytutu Badawczego – powstał projekt edukacyjny „CYBER lekcje”⁵³, kontynuowany także obecnie, który jest adresowany do nauczycieli pragnących promować zasady bezpiecznego poruszania się po internecie.

⁵³ Ministerstwo Cyfryzacji, NASK – Państwowy Instytut Badawczy, (2025), Projekt edukacyjny „CYBER lekcje”, Warszawa, zob. <https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji> [dostęp, online dn. 2.09.2025].

3. Dobre praktyki w zakresie cyfryzacji w zarządzaniu placówkami edukacyjnymi.

Współczesne zarządzanie szkołą, przedszkolem lub placówką oświatową nieodłącznie wiąże się z cyfryzacją. W dobie dynamicznego rozwoju technologii, wykorzystanie nowoczesnych narzędzi cyfrowych staje się nie tylko trendem, ale także koniecznością, umożliwiającą szkołom skuteczne zarządzanie, poprawę jakości nauczania oraz zaspokajanie rosnących oczekiwań uczniów, rodziców i nauczycieli.

Efektywnej organizacji pracy szkoły, przedszkola lub placówki oświatowej sprzyja zastosowanie w procesie zarządzania rozwiązań oferowanych przez platformy Microsoft 365 lub Google Workspace. Pozwalają one m.in. na:

- przechowywanie różnych plików (np. dokumentów, obrazów, arkuszy, filmów, podcastów związanych z funkcjonowaniem danej placówki oświatowej);
- współpracę przy opracowywaniu rozmaitych dokumentów dzięki możliwości współdzielenia plików;
- zbieranie informacji o pracy szkoły, przedszkola czy innej placówki jednostki edukacyjnej i potrzebach rozwojowych;
- komunikowanie się z innymi użytkownikami platformy;
- planowanie i przeprowadzanie spotkania online w czasie rzeczywistym;
- monitorowanie pracy nauczycieli i uczniów;
- organizowanie kształcenia zdalnego.

Z jakich funkcjonalności Microsoft 365 i Google Workspace możemy skorzystać usprawniając zarządzanie szkołą, przedszkolem lub placówką oświatową?

Zastosowanie	Google Workspace	Microsoft 365
Program pocztowy	Gmail	Outlook
Przechowywanie i współdzielenie plików	Dysk Google	One Drive
Przygotowanie ankiet i formularzy	Formularze Google	Forms
Przygotowanie dokumentów, formularzy, prezentacji	Dokumenty Google, arkusze Google, prezentacje Google	Word, Excel, Power Point

Zastosowanie	Google Workspace	Microsoft 365
Planowanie i przeprowadzanie spotkań	Meet	Teams
Organizowanie kształcenia zdalnego	Classroom i Meet	Teams

Z programów pocztowych (**Gmail lub Outlook**) można korzystać podczas komunikacji i wymiany informacji.

Dobre praktyki:

- 1) *każdy z pracowników posiada swój służbowy adres e-mail, który zawiera domenę szkoły;*
- 2) *adres e-mail pracownika pozwala na jego jednoznaczną identyfikację (tj. zawiera imię i nazwisko użytkownika, np. jan.kowalski@domenaszkoły.pl;*
- 3) *nauczyciele i inni pracownicy, którzy wykonują działania związane z pracą, używają tylko adresów służbowych;*
- 4) *dyrektor, drogą mailową, przekazuje ważne, bieżące informacje, starając się zachować odstępy czasowe (np. raz lub dwa razy w tygodniu); pamiętając o wysyłaniu e-maili wyłącznie w dni robocze przy uwzględnieniu godzin pracy (np. 7.30–15.30).*

Dysk Google i One Drive pozwalają na przechowywanie w chmurze plików w – specjalnie stworzonej do tego celu – strukturze folderów. Są one umieszczone na dyskach w chmurze. Zasoby te można udostępniać innym osobom, dając prawa do wyświetlania, recenzowania i edytowania. Jest także opcja współdzielenia plików z innymi osobami, co pozwala na współpracę przy tworzeniu materiałów. Treści te można także udostępniać w trybie recenzji. Polega to na tym, że współpracownicy nanoszą zmiany w formie komentarza, nie usuwając przy tym pierwotnych wpisów.

Dobre praktyki:

- 1) *w chmurze są umieszczane regulaminy, procedury i instrukcje obowiązujące w szkole, przedszkolu lub innej placówce oświatowej; udostępniane w trybie wyświetlania pozwalają współpracownikom na ich przeglądanie w dowolnym czasie i miejscu;*

- 2) *przed zebraniem rady pedagogicznej udostępnia się materiały do zapoznania się (np. sprawozdania z pracy, plany pracy do zaopiniowania czy zatwierdzenia, co usprawnia przebieg spotkania);*
- 3) *w folderze w chmurze umieszczane są wzory różnych formularzy do pobrania (np. arkusz obserwacji lekcji); materiały te są przygotowywane z wykorzystaniem specjalnych narzędzi (np. Excela lub Arkuszy Googla, Worda lub Dokumentów Googla);*
- 4) *przygotowanie – z wykorzystaniem arkuszy kalkulacyjnych – formularzy do zbierania informacji na temat bieżących działań szkoły (np. harmonogramu dostępności nauczycieli, formularza analizy wyników egzaminu, formularza monitorowania realizacji programu wychowawczo-profilaktycznego); formularze udostępnia się w trybie edycji, aby każdy zainteresowany mógł wpisać swoje informacje;*
- 5) *zbieranie wypełnionych formularzy z wykorzystaniem opcji Pliki Żądań, która jest dostępna w One Drive (np. sprawozdań z pracy, rozliczeń godzin ponadwymiarowych, samooceny pracy nauczyciela przed zaopiniowaniem jego dokonań przez dyrektora placówki); umieszczenie wypełnionych dokumentów w jednym folderze, sposobem na przeglądanie wypełnionych dokumentów materiałów tylko przez osobę tworzącą żądanie);*
- 6) *podejmowanie wspólnej pracy nad zmianami w wewnętrzzszkolnej dokumentacji z wykorzystaniem trybu recenzji w dokumentach; tym samym proponowanie zmian bez naruszenia zapisów w pierwotnym dokumencie (np. w statucie, wewnętrzzszkolnych regulaminach).*

Innym narzędziem, które z powodzeniem można wykorzystać do zbierania informacji, są formularze **Googla** lub **Forms**. Za ich pomocą tworzy się ankiety, sondaże, kwestionariusze do zbierania opinii na temat funkcjonowania danej placówki oświatowej. Przywołane typy formularzy w Office 365 dają możliwość zbierania informacji wraz z rejestrowaniem e-maili respondentów lub anonimowo. Zaletą obu tych rozwiązań jest szybka informacja zwrotna. Wraz z kolejno spływającymi odpowiedziami respondentów wyniki sumują się i jednocześnie powstaje ich wizualizacja (wykresy kołowe, słupkowe).

Dobre praktyki:

- 1) *przygotowanie ankiet i udostępnianie ich do wypełnienia nauczycielom, uczniom, rodzicom (np. ewaluacja programu wychowawczo-profilaktycznego);*
- 2) *odpowiednio przygotowany formularz może też być narzędziem samooceny nauczyciela dokonywanej (np. przed oceną pracy lub jako podsumowanie pracy w danym roku szkolnym);*
- 3) *wykorzystanie formularzy (anonimowe lub jawne) do przeprowadzenia sondaży, (np. dotyczących planowanych przedsięwzięć, zmian w wewnątrzszkolnym prawie, zmian w organizacji pracy szkoły, przedszkola lub innej placówki oświatowej);*
- 4) *w czasie przejścia szkoły, przedszkola lub innej jednostki edukacyjnej w tryb pracy zdalnej i gdy zebrania rady pedagogicznej są prowadzone także w takiej formie, można wykorzystać formularze Google lub Forms do realizacji niektórych zadań (np. monitorowania obecności osób na zebraniu i stwierdzania quorum lub przeprowadzania procedury głosowania i przyjmowania uchwał).*

Obie platformy dają możliwość planowania i przeprowadzania spotkań online w czasie rzeczywistym, wykorzystując w tym celu, np. narzędzia jak Meet lub Teams.

Dobre praktyki:

- 1) *przeprowadzanie spotkań tematycznych z nauczycielami (np. w celu analizowania wyników egzaminu zewnętrznego);*
- 2) *organizowanie spotkań w zespołach nauczycieli (np. w ramach zadań wynikających z pomocy psychologiczno-pedagogicznej;*
- 3) *organizowanie szkoleń i warsztatów;*
- 4) *organizowanie spotkań z rodzicami czy warsztatów dla rodziców;*
- 5) *organizowanie spotkań nauczycieli z uczniem i jego rodzicem (np. w celu podsumowania pracy w określonym czasie i udzielenia informacji zwrotnej o postępach dziecka i kierunkach rozwojowych).*

4. Dobre praktyki w jednostkach oświatowych w zakresie wykorzystania cyfryzacji w edukacji.

Konieczność rozwijania kompetencji podstawowych i kompetencji przekrojowych wynika z podstawy programowej kształcenia ogólnego. Zostały w niej określone cele i zadania odnoszące się do tych umiejętności. Wśród licznych zadań znajdują się te, które dotyczą rozwijania kompetencji cyfrowych.

„Szkoła ma stwarzać uczniom warunki do nabywania wiedzy i umiejętności potrzebnych do rozwiązywania problemów z wykorzystaniem metod i technik wywodzących się z informatyki, w tym logicznego i algorytmicznego myślenia, programowania, posługiwania się aplikacjami komputerowymi, wyszukiwania i wykorzystywania informacji z różnych źródeł, posługiwania się komputerem i podstawowymi urządzeniami cyfrowymi oraz stosowania tych umiejętności na zajęciach z różnych przedmiotów m.in. do pracy nad tekstem, wykonywania obliczeń, przetwarzania informacji i jej prezentacji w różnych postaciach. Jednostki edukacyjne mają również przygotowywać dzieci i młodzież do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w internecie, nauczyć krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej (w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci)”⁵⁴.

Zastosowanie technologii informacyjnych i komunikacyjnych (TIK) odgrywa istotną rolę w uczeniu się uczniów. Narzędzia te wpływają na efektywność uczenia się, dając dzieciom i młodzieży możliwość zarówno pracy grupowej, jak i indywidualnej.

⁵⁴ Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 roku w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dziennik Ustaw z 2018 roku pozycja 356), zob. D20170356.pdf; (Dziennik Ustaw z 2021 roku pozycja 1679), zob. D20211679.pdf; (Dziennik Ustaw z 2022 roku pozycja 1533), zob. D20221533L.pdf; (Dziennik Ustaw z 2023 roku pozycja 609), zob. D20230609.pdf; (Dziennik Ustaw z 2023 roku pozycja 1717), zob. D20231717L.pdf; (Dziennik Ustaw z 2024 roku pozycja 312), zob. D20240312L.pdf; (Dziennik Ustaw z 2024 roku pozycja 996), zob. D20240996.pdf; (Dziennik Ustaw z 2024 roku pozycja 1759), zob. D20241759.pdf [dostęp, online dn. 2.09.2025].

A to z kolei przekłada się na rozwój osobisty osób uczących się w placówkach edukacyjnych. Dzięki TIK rozbudza się u uczniów naturalną ciekawość poznawania, zwiększając tym samym ich zaangażowanie w podejmowane działania. TIK ułatwia pracę nauczycielom zarówno na etapie przygotowania lekcji, jak i jej prowadzenia, sprzyja monitorowaniu i ewaluacji procesu nauczania, a w aspektach organizacyjnych pozwala m.in. na zarządzanie pracą dzieci i młodzieży. Różnorodność e-zasobów jest dużym ułatwieniem dla uczniów w powtarzaniu wiedzy i doskonaleniu umiejętności.



Rysunek 2. Uczniowie Szkoły Podstawowej nr 10 w Zamościu podczas zajęć z lekcji języka polskiego z wykorzystaniem modułowych e-podręczników. Autorka zdjęcia: Dorota Pintal.

Przed zastosowaniem TIK warto sobie uświadomić, jakie cele chce się osiągnąć. Ta technologia uatrakcyjnia lekcję, ale nie przynosi efektów w postaci przyrostu wiedzy. Potrzebne są metody, które będzie wspierać. Zatem zastosowanie TIK ma większy sens, jeśli wspiera metody aktywizujące.

Narzędziem pomocnym w połączeniu technologii cyfrowych i aktywizujących metod pracy jest – opisany w rozdziale 2. – model SAMR.

Przykłady włączenia TIK w proces nauczania i / lub uczenia się na poszczególnych poziomach przedstawia poniższa tabela.

Substitution	– tablica interaktywna zamiast tradycyjnej; – e-podręczniki; – prezentacje multimedialne przygotowane przez nauczyciela.
Augmentation	– gry, quizy, kartkówki z wykorzystaniem rozmaitych narzędzi (np. Kahoot⁵⁵, formularza Google, Microsoft Forms); – zadania różnego typu rozwiązywane na Zintegrowanej Platformie Edukacyjnej⁵⁶; – gromadzenie pomysłów (np. w Mentimeter⁵⁷ lub Answergarden⁵⁸); – zbieranie informacji zwrotnej (np. w Mentimeter czy Microsoft Forms).
Modification	– tworzenie kolekcji zdjęć i ich opisywanie (np. w aplikacji Flickr); – łączenie obrazu, tekstu, dźwięku w iMovie; – tworzenie i korzystanie z kodów Quick Response Code (dalej QR⁵⁹); – zarządzanie plikami w chmurze (np. Dysk Google, OneDrive).
Redefinition	– projekty edukacyjne z wykorzystaniem TIK; – projekty STEAM.

Przykłady dobrych praktyk w zakresie włączania TIK do aktywizujących metod pracy na poziomie M (modification)

Przykład 1. Lekcja języka angielskiego w szkole podstawowej.

- Celem lekcji jest poznanie miejsc w Londynie, które są warte odwiedzenia.
- Uczniowie poznają niezbędne słownictwo, opisują miejsca, rozmawiają itp.
- Uczniowie pracują w parach, korzystają z tabletów lub smartfonów.
- Nauczyciel udostępnia pustą kolekcję w LearningApps⁶⁰.

⁵⁵ Kahoot. Bezpłatna platforma edukacyjna do tworzenia i prowadzenia interaktywnych quizów, gier i ankiet (w także w wersji polskiej), zob. <https://kahoot.com/pl/> [dostęp, online dn. 2.09.2025].

⁵⁶ Zintegrowana Platforma Edukacyjna, zob. <https://zpe.gov.pl> [dostęp, online dn. 2.09.2025].

⁵⁷ Mentimeter. Platforma internetowa do tworzenia interaktywnych prezentacji i ankiet, zob. <https://www.mentimeter.com> [dostęp, online dn. 2.09.2025].

⁵⁸ Answergarden. Bezpłatna aplikacja do szybkiego pozyskiwania odpowiedzi na zadane pytanie, zob. <https://answer-garden.ch> [dostęp, online 2.09.2025].

⁵⁹ QR-online.pl. Polski serwis internetowy do bezpłatnego tworzenia kodów QR, zob. <https://www.qr-online.pl/> [dostęp, online, dn. 2.09.2025].

⁶⁰ LearningApps. Bezpłatna aplikacja Web 2.0 do tworzenia i używania interaktywnych gier i ćwiczeń edukacyjnych przeznaczonych na różne etapy kształcenia, zob. <https://learningapps.org> [dostęp, online dn. 2.09.2025].

- Uczniowie tworzą gry na temat wybranego miejsca, wykorzystując dowolnie wybrane narzędzia LearningApps i poznane słownictwo.
- Na koniec lekcji uczniowie spędzają czas na przygotowanych przez siebie grach.

Przykład 2. Lekcja chemii w szkole podstawowej.

- Celem lekcji jest uporządkowanie poznanej wiedzy i doskonalenie nabytych umiejętności z działu „Woda i roztwory wodne”.
- Uczniowie pracują w zespołach.
- Każdy zespół opracowuje zadania do wskazanych przez nauczyciela zagadnień edukacyjnych do sprawdzianu (każda grupa otrzymuje inne zagadnienia).
- Uczniowie przygotowują zadania w formularzu Microsoft Forms, które sprawdzają stopień opanowania zagadnień opracowywanych przez dany zespół uczniowski. Na koniec lekcji uczniowie rozwiązują przygotowane przez siebie zadania.

Przykłady dobrych praktyk w zakresie włączania TIK do aktywizujących metod pracy na poziomie R (redefinition)

Przykład 1. Projekt interdyscyplinarny.

- Temat projektu: „W poszukiwaniu zdrowej żywności”.
- Projekt łączy elementy różnych dziedzin nauki: chemii, biologii, informatyki.
- Grupy uczniów wykonują zadania (więcej o projekcie „Wiem, co jem?” na stronie ZPE)⁶¹.
- Uczniowie przygotowują prezentację z wykorzystaniem różnych aplikacji.
- Mapa myśli obrazująca skład chemiczny substancji wchodzących w skład produktów żywnościowych (np. Free Mind).
- Infografika pokazująca produkty spożywcze (białka, tłuszcze, cukry); wykorzystanie aplikacji do tworzenia plakatów (np. Canva), slajdów i lub plakatów (PowerPoint, Prezi, edytory tekstu typu Word, dokumenty Google).
- Dokumentowanie doświadczenia badającego właściwości niektórych składników – nagranie filmu.
- Przygotowanie filmu na podstawie fotografii prezentujących etapy przygotowania zdrowego śniadania (np. Inshot).

⁶¹ Pintał D., (2022), *Czy wiem, co jem? Scenariusz interdyscyplinarnego projektu edukacyjnego do chemii dla II etapu edukacyjnego – szkoła podstawowa*, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://zpe.gov.pl/zestawy-narzedzi-edukacyjnych/> (ścieżka projektu: ZPE/Zestawy narzędzi edukacyjnych/Szkoła podstawowa IV-VIII/Chemia/Interdyscyplinarne projekty edukacyjne/Czy wiem co jem?) [dostęp, online dn. 2.09.2025].

- Opracowanie ankiety na temat zdrowego odżywiania (np. Microsoft Forms); zebranie danych i ich zaprezentowanie (wykorzystanie wizualizacji odpowiedzi z formularza Forms).

Przykład 2. Projekt interdyscyplinarny.

- Uczniowie pracując samodzielnie w zespołach, przygotowują grę miejską.
- Uczniowie opracowują zadania obejmujące różne dziedziny wiedzy.
- Uczniowie wykorzystują w swej pracy IT i AI.
- Uczniowie generują kody QR z zadaniami do wykonania.
- Uczniowie wyznaczają trasy (np. w Google Maps).
- Uczniowie przygotowują dokumentację gry do wykorzystania przez kolejne grupy uczniowskie (np. za pomocą Padletu, OneDrive, Dysku Googla).
- Pod koniec zajęć uczniowie nawzajem grają w swoje gry.

Przykład 3. Projekt STEAM.

STEAM to model edukacyjny łączący w jednym projekcie pięć kluczowych bloków:

- S – science (nauka);
- T – technology (technologia);
- E – engineering (inżynieria);
- A – arts (sztuka);
- M – mathematics (matematyka).
 - » Uczniowie wymyślają grę planszową.
 - » Uczniowie przygotowują planszę do gry, wykorzystując swoje umiejętności techniczne i matematyczne.
 - » Uczniowie projektują i przygotowują w druku 3D ruchome lub przestrzenne elementy gry (np. pionki, kostki).
 - » Uczniowie ozdabiają planszę rysunkami tematycznymi.
 - » Uczniowie w trakcie gry planszowej opracowują zadania, korzystając z posiadanej wiedzy z różnych obszarów nauki.

Wskazówki do organizacji projektu interdyscyplinarnego w formie tygodnia z projektem

- » Przez okres pięciu dni zajęcia odbywają się bez podziału na przedmioty, ale zgodnie z obowiązującym tygodniowym rozkładem zajęć.

- » Uczniowie pracują w zespołach (w tym także międzyoddziałowych), rozwiązując problemy łącznie różne dziedziny wiedzy.
- » Do zadań projektowych włączane są narzędzia TIK.
- » Jednym z zadań projektowych jest przygotowanie prezentacji lub fragmentu prezentacji z wykorzystaniem wybranego narzędzia.
- Poznanie nowego narzędzia jest jednym z zadań projektowych.
- Nauczyciele jako mentorzy – w ramach swojego czasu pracy – opiekują się daną grupą uczniów (na ogół nie zmieniają zespołów).

Rozwijanie kompetencji cyfrowych uczniów nie byłoby możliwe bez **nowoczesnej infrastruktury cyfrowej**. Rozwiązania strukturalne, które mogą wspierać te procesy to odpowiednie wyposażenie i sprawny internet.

Zapewnienie stabilnego i szybkiego dostępu do sieci oraz rozbudowa sieci internetowej w całej szkole, przedszkolu lub innej jednostce edukacyjnej stanowi punkt wyjścia do korzystania z zasobów cyfrowych, e-learningu i współpracy w chmurze. Odpowiednio wyposażone sale (np. w tablice interaktywne, monitory interaktywne, projektory) ułatwiają dynamiczne prezentowanie treści, angażowanie uczniów w interaktywną naukę, pomagają w prezentacjach i pracy grupowej. Włączanie TIK do aktywizujących metod pracy na lekcji na poziomie M i R w modelu SAMR wymaga wyposażenia sal lekcyjnych w laptopy lub tablety w takiej liczbie, aby umożliwiającej pracę indywidualną uczniów była możliwa.

Coraz większe znaczenie dla efektywnej edukacji mają bezpłatne platformy wspierające procesy uczenia się i nauczania (np. Moodle, Google Classroom czy Microsoft Teams). Warto zatem zadbać o ich dostępność dla społeczności uczniów uczniowskiej i nauczycielskiej.

W dobie cyfryzacji szkół kluczowe jest także zapewnienie **bezpieczeństwa, zrównoważonego rozwoju infrastruktury oraz odpowiedniego wsparcia technicznego**.

Ochrona sieci szkolnej przed zagrożeniami z internetu (np. wirusami lub atakami hakerskimi) wymaga zaawansowanych systemów zabezpieczeń. Instalacja zapór sieciowych, oprogramowania antywirusowego oraz monitorowanie ruchu sieciowego stanowią niezbędne kroki w zapewnieniu bezpieczeństwa uczniów i nauczycieli.

Jednak opanowanie narzędzi cyfrowych nie wystarczy, aby uniknąć zagrożeń w sieci. Szkolenia, które są organizowane dla nauczycieli i uczniów z zakresu bezpiecznego korzystania z technologii, pozwalają na świadome unikanie niebezpieczeństw, budowanie cyfrowych kompetencji, a także wzmacniają poczucie bezpieczeństwa w codziennym użytkowaniu narzędzi edukacyjnych.

Szkoły, przedszkola i inne placówki oświatowe – w miarę rozwoju technologii – muszą także dbać o zrównoważony rozwój infrastruktury, czyli regularną aktualizację sprzętu i oprogramowania. Systematyczne planowanie budżetu na modernizację technologii pomaga jednostkom edukacyjnym na bieżąco zapoznawać się z nowinkami technologicznymi, a tym samym zapewnić wydajność nauczania.

Warto też pamiętać, że niezwykle istotne jest także dostosowanie infrastruktury do specjalnych potrzeb dzieci i młodzieży szkolnej. Wprowadzenie sprzętu dla uczniów z niepełnosprawnościami (np. urządzeń wspomagających komunikację czy narzędzi ułatwiających naukę osobom z ograniczeniami) dla wszystkich jest gwarantem równego dostępu do edukacji.

Funkcjonowanie technologii w szkole wymaga sprawnej obsługi, dlatego ważną rolę odgrywa zespół IT, który zajmuje się utrzymaniem infrastruktury oraz rozwiązywaniem problemów technicznych. Dzięki temu nauczyciele mogą skupić się na nauczaniu, a nie na problemach ze sprzętem. Wdrożenie tych wszystkich rozwiązań może znacząco poprawić jakość nauczania, ułatwić dostęp do nowoczesnych zasobów edukacyjnych i wspierać rozwój umiejętności cyfrowych uczniów.

5. Możliwości i wyzwania dla sztucznej inteligencji w edukacji.

AI jest dziedziną naukowo-technologiczną zajmującą się tworzeniem systemów i maszyn zdolnych do wykonywania zadań wymagających ludzkiej inteligencji. Obejmuje to wiele zagadnień (np. rozumienie języka naturalnego, rozpoznawanie obrazów, uczenie się, rozwiązywanie problemów i adaptacja do nowych sytuacji⁶²).

⁶² Woropaj S., (2025), „Sztuczna inteligencja: Wszystko, co musisz wiedzieć od definicji do praktycznych zastosowań”, Kraków: Emerald Media Sp. z o. o., zob. <https://emeraldmedia.pl/sztuczna-inteligencja-wszystko-co-musisz-wiedziec-od-definicji-do-praktycznych-zastosowan/> [dostęp, online dn. 2.09.2025]

AI ma ogromny potencjał, ale jej rozwój i zastosowanie wymagają przemyślanego podejścia, aby zminimalizować ewentualne zagrożenia i maksymalizować korzyści, zarówno na poziomie indywidualnym, jak i społecznym.

Umiejętności związane z AI są pożądane na rynku pracy, ponieważ pozwalają na przebranżowienie się i pracę w nowych zawodach i specjalizacjach (np. inżynierowie uczenia maszynowego, analitycy danych, specjaliści do spraw etyki AI).

AI może automatyzować powtarzalne i czasochłonne codzienne zadania (np. kontrolowanie inteligentnego domu). Ta technologia wykorzystywana jest do diagnozowania chorób, personalizacji terapii. Pomaga w monitorowaniu i zarządzaniu zasobami naturalnymi.

Obecnie systemy i aplikacje, które posługują się AI, są bardzo popularne. Ludzie sięgają po nie, wykonując wiele codziennych czynności. Poniżej zamieszczono kilka przykładów:

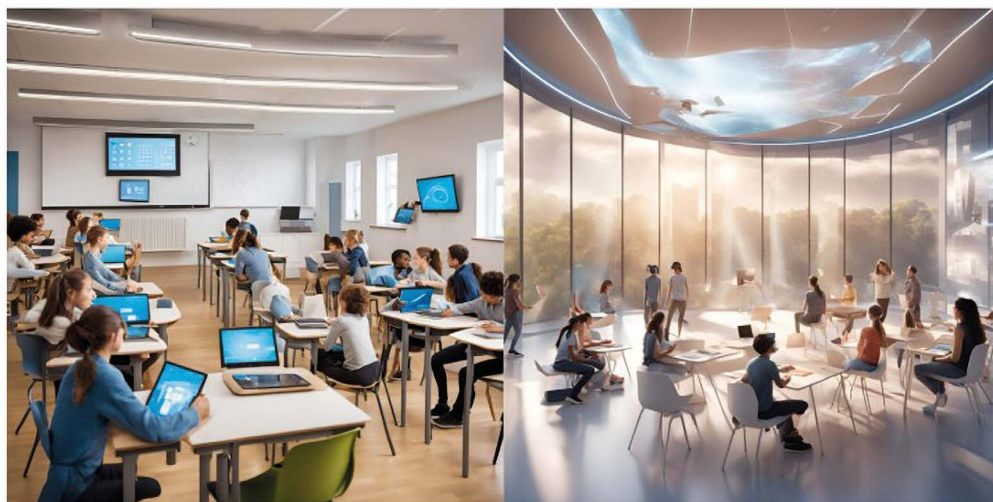
- asystenci głosowi i chatboty rozpoznające mowę, przetwarzające polecenia, wykonujące różne zadania (np. Siri, Google Assistant);
- rozpoznawanie mowy i tłumaczenia tekstów na różne języki (np. Google Translate, Microsoft Azure Speech);
- rozpoznawanie obrazu i oferowanie dodatkowych informacji (Google Lens);
- personalizacja treści (np. rekomendowanie filmów i muzyki – Netflix, Spotify, YouTube);
- systemy finansowe (oferujące rozwiązania płatnicze (np. Kup teraz!, Zapłać później!), czy wykrywające oszustwa finansowe (np. Klarna, PayPo, PayPal)).

AI odgrywa także coraz większą rolę w **procesach uczenia się i nauczania**. Technologię tę można wykorzystać do **personalizacji nauczania**, dostosowywując treści edukacyjne w czasie rzeczywistym, bazując na postępach ucznia (np. poprzez dodatkowe materiały i ćwiczenia). Chatboty i wirtualni asystenci mogą udzielać wsparcia dzieciom i młodzieży, odpowiadając na ich pytania, pomagając w rozwiązywaniu problemów. Narzędzia AI mogą rekomendować rozmaite zasoby edukacyjne (np. artykuły, filmy i kursy online), które są najlepiej dopasowane do poziomu i zainteresowań ucznia. Ponadto AI stwarza wiele funkcjonalności do tłumaczenia materiałów edukacyjnych z i na różne języki, a także dostosować te materiały dla dzieci i młodzieży z niepełnosprawnościami.

Dzięki AI **nauczyciele** mogą generować materiały edukacyjne, projektować lekcje, tworzyć narzędzia pomiaru dydaktycznego w wielu wersjach, czy zadania edukacyjne. Ten rodzaj cyfrowej inteligencji może analizować wyniki testów i inne dane, pomagając nauczycielom zidentyfikować wzorce i obszary wymagające interwencji. Systemy AI są doskonałym narzędziem do automatycznego oceniania prac domowych i testów, zapewniając szybkie i obiektywne wyniki.

Do narzędzi wspierających procesy edukacyjne należy Chat Generative Pre-trained Transformer⁶³ (dalej ChatGPT), który został opracowany przez firmę OpenAI poprzez wykorzystanie zaawansowanego modelu językowego GPT. Chat ten jest w stanie wygenerować odpowiedzi na różnorodne pytania i prowadzić rozmowy na wiele tematów. ChatGPT potrafi zarówno zrozumieć kontekst wypowiedzi oraz znaczenie słów i fraz, jak wychwycić ton komunikatu. Podobne funkcjonalności można odnaleźć w Microsoft Copilot⁶⁴. Jest to narzędzie oparte na AI, osobisty wirtualny asystent, który pomaga w rozwiązywaniu różnych zadań, wyszukuje informacje, tworzy treści.

Narzędzia bazujące na AI oferuje nauczycielom i uczniom także Canva⁶⁵. To narzędzie do projektowania graficznego online (dostępne w bezpłatnej i płatnej wersji) pozwala na stworzenie obrazu na podstawie wprowadzonego opisu. Jednym kliknięciem można poprawiać zdjęcia, zmieniać ich parametry (np. jasność, kontrast, dodawać filtry i style). Canva może również pomóc w tworzeniu tekstów.



Rysunek 3. Obrazy wygenerowane w Canvie „Rozwój cyfryzacji w edukacji”.

⁶³ ChatGPT, zob. <https://chatgpt.com> [dostęp, online dn. 2.09.2025].

⁶⁴ Copilot, zob. <https://copilot.cloud.microsoft> [dostęp dn. 2.09.2025].

⁶⁵ Canva, zob. <https://canva.com> [dostęp, online dn. 2.09.2025].

Inne przykłady narzędzi i aplikacji AI możliwe do zastosowania w edukacji zaprezentowano poniżej:

1) Inteligentni asystenci edukacyjni i personalizacja nauki

- **Socratic (Google)** – aplikacja oparta na AI, która pomaga uczniom w rozwiązywaniu problemów z matematyki, nauk ścisłych, literatury i innych przedmiotów. Dzieci i młodzież samodzielnie wykonują zdjęcie zadania, a Socratic analizuje problem i sugeruje rozwiązania.
- **Brainly** – platforma edukacyjna, która z pomocą AI umożliwia uczniom zadawanie pytań i uzyskiwanie odpowiedzi od uczniów innych dzieci, młodzieży lub ekspertów. Algorytmy AI sugerują podobne pytania i optymalne rozwiązania.
- **Khan Academy** – platforma edukacyjna wykorzystująca AI do personalizacji nauki. System – na podstawie wyników testów i wcześniejszych odpowiedzi – dostosowuje tempo i zakres materiału do indywidualnych potrzeb ucznia.

2) Automatyzacja oceny i generowanie materiałów

- **Gradescope** – narzędzie wspomagające nauczycieli w ocenie prac pisemnych, testów i zadań. AI analizuje odpowiedzi uczniów, automatyzuje ocenianie i sugeruje poprawki, co przyspiesza cały proces.
- **Turnitin** – aplikacja do wykrywania plagiatu, która dzięki AI potrafi analizować prace dzieci i młodzieży, identyfikować nieoryginalne treści i porównywać je z bazą danych publikacji akademickich.
- **Quillionz** – narzędzie oparte na AI, które – na podstawie dostarczonych materiałów tekstowych – pomaga nauczycielom tworzyć różnego typu pytania do testów i quizów (w tym otwarte i zamknięte).

3) Adaptacyjne platformy e-learningowe

- **Coursera** – platforma e-learningowa, która dzięki AI wskazuje kursy i materiały dostosowane do poziomu wiedzy oraz zainteresowań ucznia. Na podstawie interakcji i postępów w nauce system personalizuje ścieżkę nauki.
- **Edmodo** – platforma społecznościowa dla edukatorów, uczniów i rodziców, która wykorzystuje AI do analizy postępów w nauce i sugerowania dodatkowych materiałów edukacyjnych.
- **Smart Sparrow** – adaptacyjna platforma e-learningowa posługująca się narzędziami AI do personalizacji materiałów dydaktycznych, warunkując dbór treści i poziom trudności od postępów ucznia.

4) Wirtualni nauczyciele i chatboty edukacyjne

- **AI Dungeon (Latitude)** – platforma wykorzystująca AI do interaktywnego uczenia poprzez gry fabularne. Dzieci i uczniowie mogą ćwiczyć kreatywne pisanie, rozwiązywać problemy i podejmować decyzje w interaktywnych scenariuszach.
- **Mika (Pearson)** – wirtualny asystent edukacyjny wspierający uczniów w nauce matematyki. AI analizuje błędy dzieci i młodzieży, dostarcza spersonalizowane odpowiedzi, aby pomóc im zrozumieć dane zagadnienie matematyczne.
- **Duolingo** – aplikacja do nauki języków obcych, która wykorzystuje AI do personalizacji lekcji. Algorytmy analizują postępy ucznia i na tej podstawie dostosowują poziom trudności oraz tematykę kolejnych lekcji.

5) Narzędzia wspierające naukę umiejętności technicznych

- **CodeSignal** – platforma do nauki programowania, która z pomocą AI dostarcza zadania dopasowane do poziomu umiejętności ucznia. AI analizuje postępy, ocenia kod i sugeruje, jakie tematy należy przyswoić.
- **Codio** – platforma e-learningowa pomocna uczniom w nauce programowania. Dzięki narzędziom AI aplikacja ta automatycznie ocenia zadania kodowe i proponuje ścieżki rozwoju.
- **Century Tech** – narzędzie edukacyjne oparte na AI, które wspiera naukę programowania, nauk ścisłych i technologii, dostosowując materiał do potrzeb indywidualnych uczniów, a także generując automatyczne raporty dla nauczycieli.

6) Aplikacje wspomagające rozwój kompetencji miękkich

- **Elsa Speak** – aplikacja do nauki wymowy języka angielskiego, która za pomocą AI analizuje wymowę ucznia i wskazuje miejsca wymagające poprawy. AI dostosowuje ćwiczenia fonetyczne do poziomu ucznia.
- **Querium** – platforma edukacyjna wspomagająca rozwój umiejętności rozwiązywania problemów w matematyce i naukach ścisłych. AI monitoruje postępy ucznia i oferuje spersonalizowane wskazówki.
- **Cerego** - aplikacja edukacyjna wykorzystująca AI do tworzenia indywidualnych planów nauki i wspierania w zapamiętywaniu informacji. System uczy się od użytkowników, sugerując optymalne momenty na powtórki materiału.

7) Virtual Reality – rzeczywistość wirtualna (dalej VR) i Augmented Reality – rzeczywistość rozszerzona (dalej AR) wspomagane przez AI

- **Google Expeditions** – platforma edukacyjna umożliwiająca korzystanie z technologii VR / AR w celu wizualizowania miejsc i sytuacji w trój wymiarze (dalej 3D). AI pomaga w tworzeniu spersonalizowanych wycieczek wirtualnych, dostosowując materiał do kontekstu nauczania.
- **ClassVR** – narzędzie edukacyjne, które wykorzystuje VR i AI do stworzenia interaktywnych lekcji wirtualnych, w których uczniowie mogą badać różne tematy (nood historii po biologię) w realistycznych środowiskach 3D.

8) Systemy zarządzania nauczaniem Learning Management System (dalej LMS)

- **Moodle z AI** – popularna platforma LMS wykorzystuje sztuczną inteligencję do analizy postępów uczniów i proponowania materiałów oraz zadań dostosowanych do ich potrzeb.
- **Canvas** – platforma LMS, która z pomocą AI umożliwia nauczycielom śledzenie postępów dzieci oraz młodzieży, dostosowanie materiałów i zadań oraz automatyzację niektórych procesów oceny.
- **Knewton** – la narzędzie zintegrowane z systemami LMS, które wykorzystuje AI do personalizacji doświadczeń edukacyjnych uczniów, analizując dane dotyczące postępów i dostosowując materiały dydaktyczne w czasie rzeczywistym.

9) Aplikacje wspomagające zarządzanie szkołami

- **Brightspace (wcześniej znany jako Desire2Learn, dalej D2L)** – platforma edukacyjna dla szkół i uczelni korzystająca z AI do monitorowania postępów uczniów oraz studentów, a także sugerująca interwencje edukacyjne i konieczność dostosowania planów nauczania.
- **DreamBox** – system nauki matematyki online, który – dostosowując zadania do poziomu każdego ucznia – automatycznie ocenia jego wyniki. Platforma wspiera nauczycieli w monitorowaniu postępów i dostarczaniu spersonalizowanego wsparcia.
- **Third Space Learning** – platforma oferująca zajęcia online z matematyki z wykorzystaniem AI, w ten sposób pomagając uczniom rozwijać umiejętności poprzez spersonalizowane korepetycje.

AI oferuje nieskończone możliwości. Jednak wraz z nimi pojawiają się również liczne wyzwania i zagrożenia, które trzeba zrozumieć i odpowiednio nimi zarządzać.

Do niebezpieczeństw związanych z rozwojem AI można zaliczyć tzw. **deepfake**. Ta technologia umożliwia tworzenie realistycznych, ale fałszywych obrazów i filmów. Istnieje obawa, że stanie się to źródłem dezinformacji, oszustw i szantażu, co może mieć poważne konsekwencje dla demokracji. AI może być wykorzystywana do przeprowadzania zaawansowanych **ataków cybernetycznych**. Algorytmy, analizując luki w systemach zabezpieczeń, automatycznie mogą je wykorzystując, co zwiększa ryzyko dla firm i instytucji. Wykorzystanie AI w diagnostyce medycznej stwarza szansę na powstanie dylematów etycznych. Algorytmy mogą podejmować decyzje o leczeniu pacjentów na podstawie danych, które nie są do końca obiektywne lub kompletne. A to z kolei może wpływać na jakość opieki zdrowotnej.

Rozwój autonomicznych dronów i robotów bojowych budzi obawy o przyszłość konfliktów zbrojnych. Istnieje ryzyko, że takie **autonomiczne systemy militarne** mogą działać bez odpowiedniej kontroli ludzkiej, co rodzi obawy przed nieprzewidywalnymi i niebezpiecznymi sytuacjami.

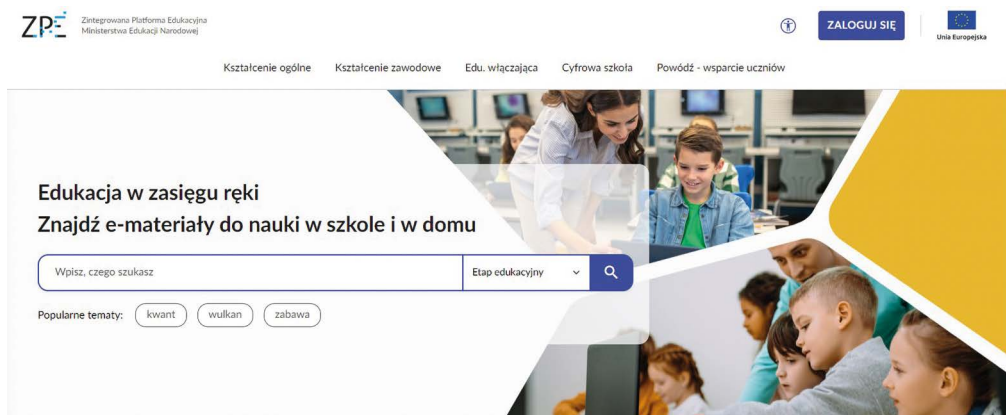
Duże korporacje technologiczne dysponują dostępem do ogromnych zasobów danych i mocy obliczeniowej, co daje im przewagę w rozwoju AI. A to może doprowadzić do **monopolizacji rynku i ograniczenia innowacji**.

AI może poprzez fakt gromadzenia i analizowania ogromnych ilości danych osobowych wywoływać niepokój ze względu na kwestię ich **prywatności i bezpieczeństwa**. Z kolei automatyzacja i robotyzacja mogą prowadzić do utraty miejsc pracy w niektórych sektorach, czyli do **bezrobocia technologicznego**.

6. Inspiracje do organizowania procesu edukacyjnego z wykorzystaniem Zintegrowanej Platformy Edukacyjnej.

ZPE jest nowoczesnym narzędziem wspierającym proces nauczania, które zostało uruchomione w lutym 2019 roku. Jest to profesjonalne, przyjazne i bezpieczne środowisko edukacyjne rekomendowane przez MEN do wykorzystania przez szkoły, przedszkola i inne jednostki oświatowe⁶⁶. Dostępna jest pod adresem

⁶⁶ Zintegrowana Platforma Edukacyjna, zob. <https://zpe.gov.pl/> [dostęp, online dn. 2.09.2025].



Rysunek 4. Strona główna ZPE.

ZPE oferuje różnorodne bezpłatne materiały edukacyjne dla uczniów i nauczycieli (np. ćwiczenia interaktywne, filmy, wirtualne podróże i eksperymenty. Materiały te są zgodne z podstawą programową dla szkoły podstawowej i ponadpodstawowej, a udostępnia się je na otwartej licencji Creative Commons. Pozwala ona – zgodnie z określonymi zapisami – na wykorzystywanie, drukowanie, kopiowanie materiałów. ZPE zawiera – adekwatne do standardów dostępności WCAG – zasoby dostosowane dla dzieci i młodzieży ze specjalnymi potrzebami edukacyjnymi. ZPE korzysta z danych SIO dotyczących szkół, przedszkoli, jednostek oświatowych, ale także nauczycieli i uczniów. Dzięki temu możliwy jest import klas i odwzorowywanie ich struktury, co ułatwia tworzenie grup uczniów, a także zapewnia bezpieczeństwo danych.

Swoim użytkownikom platforma ZPE umożliwia m.in.:

- korzystanie z gotowych materiałów (np. treści, filmów, grafik, zadań, testów);
- tworzenie własnych e-materiałów z wykorzystaniem kreatora;
- modyfikację gotowych e-materiałów, ale też dostosowanie ich do zróżnicowanych potrzeb uczniów;
- udostępnianie e-materiałów dzieciom i młodzieży;
- monitorowanie i ocenianie postępów uczniów;
- komunikowanie się z uczniami (w tym w czasie rzeczywistym);
- planowanie i przeprowadzanie wideokonferencji;
- udostępnianie w kalendarzu linku do spotkań;

Dzięki współpracy MEN i platformy Canva – za pośrednictwem ZPE – nauczyciele mogą korzystać z pełnej wersji Canva dla edukacji.

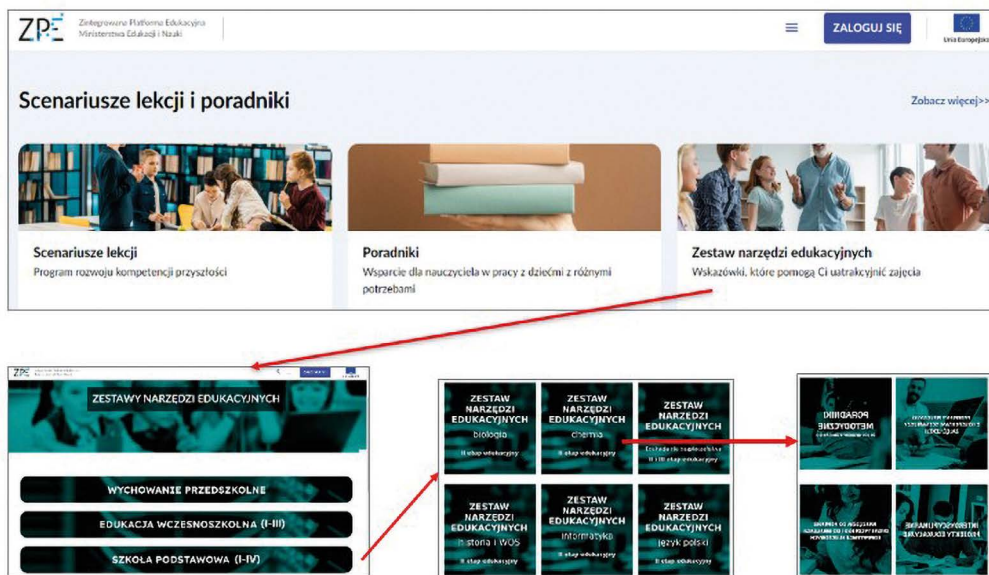
Canva jest platformą do projektowania graficznego. Pozwala na tworzenie m.in. prezentacji, infografik, plakatów, map myśli, diagramów, banerów, planerów. Nauczyciele, projektując własne materiały edukacyjne na ZPE, z powodzeniem mogą wykorzystywać możliwości Canvy do wzbogacania tych materiałów (w tym o treści wizualne).

Na Zintegrowanej Platformie Edukacyjnej (dalej ZPE) nauczyciele znajdują wiele inspiracji do planowania i prowadzenia zajęć edukacyjnych.

Inspiracją dla nauczycieli mogą być gotowe **materiały edukacyjne**, które zawierają różnorodne multimedia, interaktywne ćwiczenia, treści odnoszące się do podstawy programowej. Z tych treści z powodzeniem podczas lekcji mogą korzystać uczniowie, pracując z tabletem, własnym smartfonem, laptopem czy na tablicy interaktywnej.

Na platformie znajdziemy też **materiały interaktywne** będące wirtualnymi laboratoriami. Platforma oferuje **zestaw narzędzi edukacyjnych** (opracowanych przez ekspertów) dla wychowania przedszkolnego, edukacji wczesnoszkolnej, szkoły podstawowej (IV –VIII), liceów ogólnokształcących i techników oraz szkół branżowych I i II stopnia. Na narzędzia edukacyjne wykorzystywane podczas rozmaitych zajęć edukacyjnych składają się:

- programy nauczania z przykładowymi scenariuszami lekcji;
- poradniki metodyczne dla nauczycieli;
- przykładowe scenariusze interdyscyplinarnych projektów edukacyjnych;
- narzędzia do pomiaru dydaktycznego i ewaluacji procesu rozwijania kompetencji kluczowych (np. testy diagnostyczne, testy badające przyrost umiejętności, arkusze samooceny i oceny koleżeńskiej, arkusze formatywnej i sumującej ewaluacji, arkusze ewaluacji kompetencji kluczowych).



Rysunek 5. ZPE. Ścieżka do narzędzi edukacyjnych.

Na ZPE nauczyciele mają dostęp do **scenariuszy lekcji opracowanych przez swoich kolegów pedagogów (np. w ramach projektu „Lekcja:Enter”)**. Materiały te uwzględniają włączanie technologii informacyjnych i komunikacyjnych do aktywizujących metod pracy. W scenariuszach zaproponowano przebieg lekcji uwzględniający kolejne etapy cyklu Kolba⁶⁷.

ZPE wychodzi naprzeciw **zróżnicowanym potrzebom edukacyjnym uczniów**. Na tej platformie znajdują się **teksty łatwe do czytania i zrozumienia (easy to read and understand; dalej ETR)**. To uproszczona forma komunikacji, która jest przeznaczona dla osób z niepełnosprawnością intelektualną lub dla osób mających problemy z czytaniem i rozumieniem. Na ETR składają się następujące elementy:

- dobór słów;
- sposób formułowania zdań;
- kompozycję tekstu;
- rodzaj i rozmiar użytej czcionki;
- zastosowanie odpowiednich ilustracji lub symboli.

⁶⁷ Projekt Dawida Kolba to niezwykła technika edukacji, czterofazowa, która opisuje sposób uczenia się ludzi: a) doświadczenie; b) refleksję; c) teorię; d) zastosowanie.

Kolejnym rozwiązaniem, jakie można znaleźć na ZPE, a które uwzględnia zróżnicowane potrzeby swoich użytkowników, są **lektury dostępne**. To multimedialne książki do edukacji językowej i polonistycznej wraz z materiałami ćwiczeniowymi.

Do każdej takiej lektury dodano:

- pakiet składający się z nagrań video z tłumaczeniem tekstu na polski języki migowy;
- tekst łatwy do czytania (ETR);
- opracowanie graficzne w formie komiksu, kart pracy, kart pracy z symbolami Picture Communication Symbols (dalej PCS – system obrazkowych symboli graficznych używanych w komunikacji wspomagającej).

Zróżnicowane potrzeby uczniów zostały także uwzględnione w **Generatorze kart pracy**, dostępnym na ZPE tuż po zalogowaniu się użytkownika. Narzędzie to umożliwia tworzenie spersonalizowanych arkuszy z zadaniami i ćwiczeniami dla dzieci i uczniów o zróżnicowanych potrzebach edukacyjnych. Platforma wspiera też nauczycieli w ich **pracy wychowawczej oraz w udzielaniu uczniom pomocy psychologiczno-pedagogicznej**.

Jak możemy wdrożyć ZPE w szkole? Oto kilka wskazówek:

- przeprowadzenie dla nauczycieli szkolenia prezentującego zasoby platformy;
- przeprowadzenie warsztatu w zakresie praktycznego wykorzystania możliwości platformy;
- organizowanie wymiany doświadczeń;
- prowadzenie zajęć pokazowych;
- stworzenie szkolnego banku pomysłów na lekcje z wykorzystaniem ZPE;
- wspieranie nauczycieli poprzez konsultacje udzielane przez kolegów lub koleżanki po fachu, którzy posiadają bardziej zaawansowane umiejętności.

7. Cyberzagrożenia w edukacji.

W dobie dynamicznego rozwoju technologii informatycznych, bezpieczeństwo cyfrowe staje się jednym z najważniejszych aspektów ludzkiej codzienności. Jest ona (w tym także dane wrażliwe) we wszystkich jej obszarach niemal każdego dnia (np. zaczynając od bankowości internetowej, a kończąc na mediach społecznościowych) nieustannie narażone na różnego rodzaju zagrożenia.

Bezpieczeństwo cyfrowe obejmuje szeroki zakres działań mających na celu ochronę naszych danych i systemów przed nieautoryzowanym dostępem, atakami cybernetycznymi oraz innymi formami niebezpieczeństw. Cyberzagrożenia są także coraz bardziej powszechne w edukacji. Mogą mieć poważne konsekwencje dla uczniów, nauczycieli oraz samych instytucji edukacyjnych. Poniżej przedstawiono kilka najczęściej spotykanych zagrożeń w edukacji.

- **Phishing.** Ataki phishingowe polegają na podszywaniu się pod zaufane instytucje w celu wyłudzenia poufnych informacji (np. haseł czy danych osobowych). Uczniowie i nauczyciele mogą otrzymywać fałszywe e-maile lub wiadomości, które wyglądają na autentyczne.
- **Malware.** Złośliwe oprogramowanie (np. wirusy, trojany czy ransomware) może uszkodzić systemy komputerowe, ukraść dane lub blokować dostęp do ważnych plików.
- **Ransomware.** Rodzaj malware, który blokuje dostęp do systemu lub danych i żąda okupu za ich odblokowanie.
- **Ataki DDoS.** Przeciążenie serwera następuje poprzez dużą liczbę żądań, co prowadzi do jego awarii.
- **Cyberprzemoc.** Uczniowie mogą być ofiarami cyberprzemocy, która obejmuje nękanie, zastraszanie i upokarzanie za pomocą technologii cyfrowych. Taka sytuacja może mieć poważne skutki psychiczne i emocjonalne dla ofiar.
- **Nieautoryzowany dostęp.** Hakerzy mogą podejmować próby uzyskania dostępu do szkolnych systemów, w celu kradzieży danych osobowych, zmiany ocen czy wprowadzania fałszywych informacji do systemu.
- **Wyciek danych.** W szkołach, przedszkolach lub innych placówkach edukacyjnych przechowywane są wiele poufnych informacji, w tym dane osobowe. Wycieki danych mogą prowadzić do poważnych konsekwencji związanych z ochroną danych osobowych.
- **Niebezpieczne treści.** Uczniowie mogą natrafić w sieci na szkodliwe treści, (np. pornografię, przemoc, treści promujące nienawiść).
- **Nadużywanie technologii.** Zbyt częste używanie technologii cyfrowych może prowadzić do problemów zdrowotnych.

Skuteczna ochrona przed zagrożeniami wymaga stosowania w codziennym funkcjonowaniu zasad bezpieczeństwa. Należą do nich m.in.:

- aktualizacje systemów operacyjnych i aplikacji eliminujących luki bezpieczeństwa;

- używanie unikalnych i skomplikowanych haseł dla różnych kont oraz regularna zmiana kodu dostępu;
- stosowanie dwuskładnikowego uwierzytelniania kont (np. dodatkowo za pomocą kodu SMS);
- tworzenie kopii zapasowych;
- unikanie klikania w linki i załączniki podejrzanego pochodzenia, korzystanie z zaufanych źródeł informacji;
- korzystanie z platform edukacyjnych oferujących zaawansowane zabezpieczenia (dwuskładnikowe uwierzytelnianie i szyfrowanie danych);
- instalowanie filtrów internetowych blokujących dostęp do nieodpowiednich treści, a także korzystanie z oprogramowania zabezpieczającego przed malware i innymi zagrożeniami;
- wdrażanie systemów zarządzania hasłami, położenie nacisku na tworzenie i przechowywanie silnych haseł;
- opracowanie i wdrożenie polityk bezpieczeństwa określającego zasady korzystania z technologii w szkole, przedszkolu lub innej jednostce edukacyjnej;
- regularne szkolenia z zakresu bezpieczeństwa cyfrowego przygotowujące do rozpoznawania zagrożenia i poznania sposobu radzenia sobie z nimi;
- regularne monitorowanie sieci szkolnej oraz przeprowadzanie audytów bezpieczeństwa w celu wczesnego wykrycia i reagowania na potencjalne zagrożenia;
- przestrzeganie zasad ochrony danych osobowych uczniów (np. nieudostępnianie ich danych bez zgody oraz stosowanie pseudonimizacji);
- uczenie uczniów, jak bezpiecznie korzystać z internetu w tym unikanie podejrzanych stron i linków oraz nieudostępnianie swoich danych osobowych.

Dobre praktyki w zakresie zapobiegania cyberzagrożeniom

*Tytuł programu edukacyjnego **Urzędu Ochrony Danych Osobowych (dalej UODO) brzmi: „Twoje dane – Twoja sprawa”**⁶⁸.*

Elementem programu są m.in. szkolenia dla nauczycieli dotyczące poprawnego przetwarzania danych osobowych, pomagające zrozumieć, w jaki sposób bezpiecznie to robić, a także jakie są najnowsze zagrożenia. Poradnik dotyczący przetwarzania

⁶⁸ Serwis Samorządowy PAP, (2024), „Jak chronić dane osobowe w szkołach? Rusza nabór do programu „Twoje dane – Twoja sprawa” (regulamin)”, Warszawa, zob. Jak chronić dane osobowe w szkołach? Rusza nabór do programu „Twoje dane – Twoja sprawa” (regulamin) | Serwis Samorządowy PAP [dostęp, online dn. 2.09.2025].

danych osobowych w szkołach i placówkach oświatowych⁶⁹ został przygotowany przez UODO we współpracy z MEN. Zawiera praktyczne wskazówki i zasady, które pomagają dyrektorom i nauczycielom w codziennej pracy.

Poradniki pomagające w bezpiecznym korzystaniu z narzędzi do nauki zdalnej⁷⁰ zostały opracowane przez UODO. Znajdują się w nich wskazówki dotyczące ochrony danych osobowych uczniów i nauczycieli podczas korzystania z platform edukacyjnych.

W ramach rozmaitych programów naukowych przeprowadza się specjalistyczne szkolenia i webinaria, które omawiają najnowsze zagadnienia z zakresu ochrony danych osobowych. Dzięki temu nauczyciele i uczniowie mogą być na bieżąco z najnowszymi trendami i technologiami.

Szkoły coraz częściej inwestują w zaawansowane technologie zabezpieczające (np. systemy zarządzania tożsamością i dostępem, czyli Identity and Access Management (dalej IAM), a także narzędzia do monitorowania i wykrywania zagrożeń). Te narzędzia pomagają w ochronie danych przed nieautoryzowanym dostępem i atakami cybernetycznymi.

Bezpieczeństwo cyfrowe to nie tylko kwestia technologii, ale także świadomości i odpowiedzialności użytkowników. W erze cyfrowej, gdzie nasze życie coraz bardziej przenika się z technologią, dbanie o bezpieczeństwo naszych danych jest kluczowe. Pamiętajmy, że nawet najprostsze działania mogą znacząco zwiększyć nasze bezpieczeństwo w sieci. Bądźmy czujni i świadomi zagrożeń, aby cieszyć się korzyściami płynącymi z technologii bez obaw o nasze dane.

8. Bibliografia.

Answergarden. Bezpłatna aplikacja do szybkiego pozyskiwania odpowiedzi na zadane pytanie, zob. <https://answergarden.ch> [dostęp, online 2.09.2025].

Canva, zob. <https://canva.com> [dostęp, online dn. 2.09.2025].

⁶⁹ UODO, MEN, (2018), „Ochrona danych osobowych w szkołach i placówkach oświatowych. Poradnik”, Warszawa, zob. <https://uodo.gov.pl/pl/201/481> [dostęp, online dn. 2.09.2025].

⁷⁰ Ministerstwo Edukacji Narodowej, (2020), „Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół”, Warszawa, zob. <https://www.gov.pl/web/edukacja/zdalne-nauczanie-uodo> [dostęp, online dn. 2.09.2025].

Copilot, zob. <https://copilot.cloud.microsoft> [dostęp dn. 2.09.2025].

ChatGPT, zob. <https://chatgpt.com> [dostęp, online dn. 2.09.2025].

Czerkawska B., Pintał D., Witkowski J., (2022), „Jak rozwijać kompetencje proinnowacyjne w szkole? Przewodnik i rekomendacje dla dyrekcji”, Warszawa: Centrum Edukacji Obywatelskiej, zob. <https://szkoladlainnowatora.ceo.org.pl/publikacje/> [dostęp, online dn. 2.09.2025].

Idzik R., (2022), „Wspieranie szkół w rozwijaniu kompetencji proinnowacyjnych Rekomendacje dla jednostek samorządu terytorialnego”, Warszawa: Centrum Edukacji Obywatelskiej, zob. <https://szkoladlainnowatora.ceo.org.pl/publikacje/> [dostęp, online dn. 2.09.2025].

Kahoot. Bezpłatna platforma edukacyjna do tworzenia i prowadzenia interaktywnych quizów, gier i ankiet (także w wersji polskiej), zob. <https://kahoot.com/pl/> [dostęp, online dn. 2.09.2025].

LearningApps. Bezpłatna aplikacja Web 2.0 do tworzenia i używania interaktywnych gier i ćwiczeń edukacyjnych przeznaczonych na różne etapy kształcenia, zob. <https://learningapps.org> [dostęp, online dn. 2.09. 2025].

Mentimeter. Platforma internetowa do tworzenia interaktywnych prezentacji i ankiet, zob. <https://www.mentimeter.com> [dostęp, online dn. 2.09. 2025].

Ministerstwo Cyfryzacji, NASK – Państwowy Instytut Badawczy, (2025), „Projekt edukacyjny «CYBER lekcje»”, Warszawa, zob. <https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji> [dostęp, online dn. 2.09.2025].

Ministerstwo Edukacji Narodowej. Departament Innowacji i Rozwoju, (2020), „Zintegrowana Strategia Umiejętności 2030”, Warszawa, zob. <https://zsu2030.mein.gov.pl/#zsu> [dostęp, online dn. 2.09.2025].

Ministerstwo Edukacji Narodowej, (2020), „Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół”, Warszawa, zob. <https://www.gov.pl/web/edukacja/zdalne-nauczanie-uodo> [dostęp, online dn. 2.09.2025].

Najwyższa Izba Kontroli, (2022), „Informacja o wynikach kontroli. Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa”, zob. <https://www.nik.gov.pl/plik/id,25577,vp,28343.pdf> [dostęp, online dn. 2.09.2025].

Pintal D., (2019), „Przewodnik i narzędziownik dla dyrektorów szkół”, Warszawa: Fundacja Rozwoju Społeczeństwa Informacyjnego w ramach projektu „Lekcja:Enter”.

Pintal D., Tomaszewicz D., (2020), „Jak wdrożyć Office 365 lub G-Suite w 10 dni?”, Warszawa: Fundacja Rozwoju Społeczeństwa Informacyjnego w ramach projektu „Lekcja:Enter”.

Pintal D., (2022), „Czy wiem, co jem? Scenariusz interdyscyplinarnego projektu edukacyjnego do chemii dla II etapu edukacyjnego – szkoła podstawowa”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://zpe.gov.pl/zestawy-narzedzi-edukacyjnych/> (ścieżka projektu: ZPE/Zestawy narzędzi edukacyjnych/Szkoła podstawowa IV-VIII/Chemia/Interdyscyplinarne projekty edukacyjne/Czy wiem co jem?) [dostęp, online dn. 2.09.2025].

Polak M., (2014), „Model SAMR, czyli o technologii w nauczaniu, Portal o nowoczesnej edukacji”, Warszawa: EduNews, zob. <https://edunews.pl/badania-i-debaty/badania/2736-model-samr-czyli-o-technologii-w-nauczaniu> [dostęp, online dn. 2.09.2025].

Qr-online.pl. Polski serwis internetowy do bezpłatnego tworzenia kodów QR, zob. <https://www.qr-online.pl/> [dostęp, online, dn.2.09.2025].

Rada Europejska, (2018), „Zalecenie Rady z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie”, „Dziennik Urzędowy Unii Europejskiej” nr 2018/C 189/01, zob. <https://op.europa.eu/pl/publication-detail/-/publication/6fda126a-67c9-11e8-ab9c-01aa75ed71a1> [dostęp, online dn. 2.09.2025].

Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dziennik Ustaw z 2018 roku pozycja 356), zob. D20170356.pdf [dostęp, online dn. 2.09.2025].

Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 roku w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów

z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dziennik Ustaw z 2018 roku pozycja 356), zob. D20170356.pdf; (Dziennik Ustaw z 2021 roku pozycja 1679), zob. D20211679.pdf; (Dziennik Ustaw z 2022 roku pozycja 1533), zob. D20221533L.pdf; (Dziennik Ustaw z 2023 roku pozycja 609), zob. D20230609.pdf; (Dziennik Ustaw z 2023 roku pozycja 1717), zob. D20231717L.pdf; (Dziennik Ustaw z 2024 roku pozycja 312), zob. D20240312L.pdf; (Dziennik Ustaw z 2024 roku pozycja 996), zob. D20240996.pdf; (Dziennik Ustaw z 2024 roku pozycja 1759), zob. D20241759.pdf [dostęp, online dn. 2.09.2025].

Serwis Samorządowy PAP, (2024), „Jak chronić dane osobowe w szkołach? Rusza nabór do programu „Twoje dane – Twoja sprawa” (regulamin)”, Warszawa, zob. Jak chronić dane osobowe w szkołach? Rusza nabór do programu „Twoje dane – Twoja sprawa” (regulamin) | Serwis Samorządowy PAP [dostęp, online dn. 2.09.2025].

Urząd Ochrony Danych Osobowych, Ministerstwo Edukacji Narodowej, (2018), „Ochrona danych osobowych w szkołach i placówkach oświatowych. Poradnik”, Warszawa, zob. <https://uodo.gov.pl/pl/201/481> [dostęp, online dn. 2.09.2025].

Urząd Ochrony Danych Osobowych, (2025), „XVI edycja programu «Twoje dane – Twoja sprawa» w roku szkolnym 2025/2026”, Warszawa, zob. <https://uodo.gov.pl/612/384> [dostęp, online dn. 2.09.2025].

Witkowski J. (red.), (2022), „Dydaktyka kompetencji proinnowacyjnych”, Centrum Edukacji Obywatelskiej, Warszawa, zob. <https://szkoladlainnowatora.ceo.org.pl/publikacje/> [dostęp, online dn. 2.09.2025].

Woropaj S., (2025), „Sztuczna inteligencja: Wszystko, co musisz wiedzieć od definicji do praktycznych zastosowań”, Kraków: Emerald Media Sp. z o. o., zob. <https://emeraldmedia.pl/sztuczna-inteligencja-wszystko-co-musisz-wiedziec-od-definicji-do-praktycznych-zastosowan> [dostęp, online dn. 2.09.2025].

Zintegrowana Platforma Edukacyjna, zob. <https://zpe.gov.pl> [dostęp, online dn. 2.09.2025].

Ministerstwo Edukacji Narodowej. Departament Innowacji i Rozwoju, (2020), „Zintegrowana Strategia Umiejętności 2030”, Warszawa, zob. <https://zsu2030.mein.gov.pl/#zsu> [dostęp, online dn. 2.09.2025].

MATERIAŁ 6. ZARZĄDZANIE CYFRYZACJĄ W OŚWIACIE W KONTEKŚCIE WYZWAŃ PSYCHOSPOŁECZNYCH



Zofia Domaradzka-Grochowalska

Ważne!

Materiał 6. jest inspiracją do warsztatów i wykładów zaplanowanych w „Programie szkoleniowo-doradczym”. Porusza tematykę związaną z systemowym rozwojem organizacji oraz rolą lidera w zarządzaniu zmianą w kontekście cyfrowych wyzwań. Ponadto materiał ten stanowi studium refleksji, który odnosi się do tematu związanego ze zdrowiem psychicznym dzieci, młodzieży i dorosłych. W ramach diagnozy społecznej w trakcie realizacji pilotażu przeprowadzono 51 spotkań lokalnych dotyczących stanu cyfryzacji oświaty. Wnioski i zalecenia wynikające z przeprowadzonych dyskusji dotyczyły m.in. nie tylko stosowania technologii, dostępu do internetu, sprzętu, ale również wskazywały na potrzebę działań w zakresie budowania dobrostanu psychicznego.

Wprowadzenie

Niniejsze opracowanie jest próbą odpowiedzi na jedno z kluczowych wyzwań współczesnej edukacji – świadome i odpowiedzialne zarządzanie procesem cyfryzacji w oświacie. Prawdziwa transformacja cyfrowa jest procesem, który zaczyna się tam, gdzie technologia spotyka się z refleksją, odpowiedzialnością i troską o rozwój człowieka. W publikacji zestawiono podejście popularnonaukowe z praktycznym spojrzeniem na rzeczywistość polskiej edukacji. W przygotowanym materiale zamieszczono zarówno

analizę kluczowych psychospołecznych wyzwań, jak i konkretne modele, metody oraz narzędzia wsparcia. Mogą one pomóc w skutecznym przeprowadzaniu pożądanych zmian. Podejmując próbę refleksji nad obecnym stanem cyfryzacji w edukacji, warto skłonić samorządowców oraz dyrektorów szkół, przedszkoli i placówek edukacyjnych do wnikliwej analizy wyników przeprowadzonych diagnoz stanu cyfryzacji lokalnej oświaty i wyciągania wniosków dotyczących planowanych działań rozwojowych. Ważne jest jednak, aby nie tylko dostrzegać istniejące problemy, ale przede wszystkim inicjować zmiany, które skutecznie odpowiedzą na współczesne – nie tylko globalne, ale i lokalne wyzwania. Autorka ma nadzieję, że analiza opracowanych treści stanie się inspiracją do dalszych działań, refleksji, a także mądrego towarzyszenia procesowi cyfrowej transformacji (zarówno na poziomie samorządów, jak i szkół oraz indywidualnych nauczycieli).

1. Funkcja cyfryzacji w oświacie.

Cyfryzacja w edukacji jest efektem zarządzania zarówno na poziomie globalnym, jak i lokalnym. Jednocześnie jest to zagadnienie, które tylko pozornie łączy się wyłącznie z technicznym i finansowym aspektem. Tak naprawdę bowiem cyfryzacja oświaty jest niezwykle pojemnym obszarem łączący ze sobą szereg różnych ujęć i perspektyw. Jaki jest cel całościowego włączanie technologii cyfrowych, metod dydaktycznych i zasobów do procesu nauczania? Czy cyfryzacja jest procesem, czy może rezultatem zmian zachodzących w świecie?

Cyfryzację można określić mianem procesu, ponieważ cechuje ją m.in.:

- dynamizm — to nie jest jednorazowa zmiana, ale ciągły ruch w kierunku coraz większego wykorzystania technologii cyfrowych;
- wymaga adaptacji, uczenia się, zmian mentalnych i organizacyjnych, a te rozciągają się w czasie;
- zmienia się technologia, ale też przeobrażeniom ulega powszechne nastawienie ludzi do zagadnień informatycznych.

Z perspektywy psychospołecznej, uznanie cyfryzacji za proces jest szczególnie ważne, ponieważ pozwala:

- lepiej zrozumieć opór, lęk, potrzebę wsparcia;

- dać sobie (i innym) przestrzeń na adaptację;
- myśleć o rozwoju kompetencji i relacji jako drogi, a nie punktu do odhaczenia.

Cyfryzację można określić mianem rezultatu, ponieważ m.in.: odzwierciedla dokonane już zmiany technologiczne, organizacyjne i kulturowe w systemie edukacji. Obecne postrzeganie technologii cyfrowych stanowi efekt wprowadzonych rozwiązań, które przekształciły sposób funkcjonowania szkół, przedszkoli, jednostek oświatowych, komunikacji i dostępu do wiedzy. To cyfrowy krajobraz, w którym dziś poruszają się uczniowie, nauczyciele i dyrektorzy. Cyfryzacja w oświacie to proces zastosowania technologii cyfrowych do różnych obszarów funkcjonowania instytucji edukacyjnych zarówno w wymiarze dydaktycznym (np. e-learning, platformy edukacyjne, cyfrowe narzędzia pracy nauczyciela), jak i organizacyjnym (np. elektroniczny obieg dokumentów, cyfrowe dzienniki, zarządzanie danymi). Równocześnie rozwój technologii informacyjnych w oświacie jest zjawiskiem wieloaspektowym, nie ogranicza się wyłącznie do technicznej modernizacji. Cyfryzację można określić głęboką zmianą kultury edukacyjnej, która wpływa na role społeczne uczniów, nauczycieli i dyrektorów, na sposób komunikacji, podejście do wiedzy, a nawet na tożsamość szkoły jako wspólnoty.

Wprowadzenie cyfryzacji do oświaty niesie za sobą wiele potencjalnych korzyści, wśród których należy wymienić m.in.:

- lepszy dostęp do wiedzy — zasoby edukacyjne dostępne online zwiększają możliwości uczenia się dla wszystkich uczniów, bez względu na miejsce zamieszkania czy status ekonomiczny;
- personalizację nauczania — technologie pozwalają dostosować tempo i styl uczenia się do indywidualnych potrzeb uczniów;
- rozwój kompetencji przyszłości (np. krytyczne myślenie, współpraca w środowisku cyfrowym, kreatywność i umiejętność rozwiązywania problemów);
- wzrost zaangażowania uczniów — interaktywne metody nauczania mogą zwiększyć motywację i aktywność młodych ludzi;
- wsparcie terapeutyczne z wykorzystaniem specjalistycznego oprogramowania dla uczniów z różnego rodzaju deficytami.

Technologia cyfrowa w edukacji jest także przestrzenią pełną trudności i niełatwych wyzwań. Jednymi z nich są te o charakterze psychospołecznym. Wśród tych najczęściej występujących należy wskazać m.in.:

- nierówny dostęp do technologii – problem wykluczenia cyfrowego nadal dotyka wielu uczniów i nauczycieli;
- ryzyko nadużywania technologii – nadmierne korzystanie z urządzeń elektronicznych może prowadzić do problemów zdrowotnych i społecznych (co znalazło odzwierciedlenie w licznych raportach);
- brak kompetencji cyfrowych – jest zjawiskiem, które dotyka zarówno uczniów, jak i kadrę nauczycielską, które w dalszej perspektywie może ograniczać efektywność wykorzystania nowoczesnych narzędzi;
- korzystanie z technologii w celach nieetycznych, a czasem wręcz szkodliwych i niebezpiecznych.

Pozostałe zagadnienia z tego obszaru zostaną szerzej zaprezentowane w rozdziale podejmującym pogłębioną analizę kluczowych wyzwań psychospołecznych w obszarze zarządzania cyfryzacją w oświacie.

Już na samym początku warto sobie uświadomić, że cyfryzacja w edukacji nie jest celem sama w sobie. Technologia informatyczna stanowi bowiem narzędzie służące do tego, aby polska szkoła i placówki oświatowe nie pozostały w tyle za zmieniającym się światem. To także sposób na to, aby edukacja była bliżej życia codziennego młodych ludzi, ich przyszłych wyzwań i możliwości. Cyfryzacji nie należy się obawiać. Wielu sympatyków tradycyjnego modelu nauczania boi się, że technologia informatyczna odbierze pracę nauczycielowi, że przyczyni się do powstania podziałów. A jest wręcz odwrotnie. Cyfryzacja w oświacie otwiera przed ludźmi (w tym wypadku dziećmi, młodzieżą oraz nauczycielami) nowe możliwości uczenia się, tworzenia i zmieniania świata na lepsze.

2. Transformacja cyfrowa a transformacja myślenia.

Prawdziwa transformacja cyfrowa w oświacie wymaga nie tylko odpowiedniego sprzętu, ale i odwagi, aby zmienić sposób myślenia o nauczaniu, uczeniu się i roli szkoły we współczesnym świecie. To zmiana sposobu myślenia o edukacji, roli nauczyciela, ucznia i samej szkoły w procesie kształcenia. To nie tylko wdrażanie technologii, ale

przede wszystkim zmiana kultury organizacyjnej, wartości, praktyk i przekonań, które kierują codzienną pracą placówki edukacyjnej. Z badań przeprowadzonych przez Instytutu Badań Edukacyjnych⁷¹ (dalej IBE), wynika, że cyfryzacja w szkołach bywa wdrażana technicznie, bez towarzyszącej jej zmiany w mentalności użytkowników zasobów i narzędzi cyfrowych. Niestety nadal w wielu polskich szkołach i placówkach edukacyjnych wszelkie oprogramowania informatyczne postrzegane są jako coś złego i niepotrzebnego. Dzieje się tak dlatego, że:

- technologię traktuje się jako dodatek, narzędzie na specjalne okazje (np. projekty, prezentacje multimedialne);
- cyfryzację ogranicza się jedynie do aspektu formalnego (np. zakupu sprzętu), ale w istocie podejście do nowych technologii jako metody dydaktycznej wcale się nie zmienia;
- nauczycieli i kadrę zarządzającą cechuje niski poziom kompetencji cyfrowych;
- nauczyciele i dyrektorzy szkół oraz placówek edukacyjnych obawiają się zmian wynikających z braku przygotowania lub złych wcześniejszych doświadczeń;
- nauczyciele i kadra dyrektorska nie są przekonani do zasadności zmiany metod nauczania.

Natomiast idealnie byłoby, gdyby szkoły, przedszkola i placówki oświatowe stałyby się taką przestrzenią, w której:

- technologia stanowiłaby integralny element codziennego procesu nauczania i uczenia się, a nie pełniłaby wyłącznie funkcji okazjonalnego dodatku;
- nauczyciele i uczniowie stali się partnerami w procesie eksploracji wiedzy;
- rozwój kompetencji przyszłości (np. myślenie krytyczne, umiejętność pracy zespołowej w środowisku cyfrowym, rozwiązywanie problemów) stałby się czymś naturalnie pożądanym;
- nauczyciele i dyrektor potrafiliby elastycznie reagować na zmieniające się potrzeby społeczne i technologiczne.

Warto podkreślić, że mianem stanu pożądanego określa taką sytuację w szkole, przedszkolu lub placówce oświatowej, w której technologię informatyczną traktuje się jako naturalne środowisko pracy i uczenia się, a nie jako dodatek lub zagrożenie. Stworzenie tak wzorcowego środowiska wymaga jednak transformacji myślenia na wielu poziomach:

⁷¹ Instytut Badań Edukacyjnych, (2021), „Kompetencje cyfrowe uczniów i nauczycieli – wyniki badań w Polsce”, Warszawa: Instytut Badań Edukacyjnych.

- **na poziomie indywidualnym** – nauczyciele i dyrektorzy muszą zmienić sposób postrzegania swojej roli. Powinni zrozumieć, że nie mogą nadal być wyłącznie dawcami wiedzy, ale mentorami, przewodnikami po świecie informacji;
- **na poziomie organizacyjnym** – szkoła jako instytucja musi stworzyć warunki do eksperymentowania i wspólnego tworzenia innowacji;
- **na poziomie systemowym** – samorządy i władze oświatowe muszą budować strategię, które nie tylko koncentrują się na finansowaniu technologii, ale także wspierają rozwój kompetencji i zmiany mentalności.

Dla obecności cyfryzacji w szkole równie istotne jest rozpoznanie barier mentalnych utrudniających proces transformacji. Wśród nich można wskazać następujące czynniki:

- przekonanie, że technologia nie zastąpi tradycyjnej edukacji;
- obawa nauczycieli i dyrektorów przed utratą autorytetu w cyfrowym świecie;
- strach nauczycieli i dyrektorów przed nieznanym i przed porażką.

Z drugiej strony trzeba sobie uświadomić, że istnieje wiele inspirujących szkół, które są przykładem tego, że zmiana – przy odpowiednim wsparciu, otwartości na uczenie się i gotowości do podjęcia ryzyka – jest możliwa. Dlatego też kluczowym etapem w procesie cyfryzacji oświaty jest inwestowanie nie tylko w sprzęt, ale przede wszystkim zmiana sposobu myślenia o edukacji i o roli wszystkich uczestników procesu edukacyjnego w epoce cyfrowej.

Podsumowanie

Przemyślane wykorzystanie technologii wymaga odwagi do porzucenia utartych schematów, otwartości na nowe modele uczenia się i nauczania oraz refleksji nad tym, w jaki sposób kształtować postawy gotowe na wyzwania XXI wieku. A w centrum tej transformacji zawsze musi pozostawać człowiek (jego potrzeby, wartości, możliwości i odpowiedzialność). Bowiem tak naprawdę to nie technologia informatyczna, ale ludzie zmieniają edukację, traktując cyfryzację jako narzędzie budowania lepszego, bardziej świadomego świata. Z kolei transformacja cyfrowa w edukacji stanowi szansę na stworzenie świata, w którym technologia nie oddziela ludzi od siebie, lecz buduje przestrzeń do wspólnego spotykania się, współpracy i rozwoju. To od współczesnych nauczycieli i dyrektorów zależy, czy wykorzystają możliwości cyfryzacji, aby uczyć młodych ludzi nie tylko sprawnego korzystania z narzędzi informatycznych, ale przede wszystkim odpowiedzialnego, mądrego życia w świecie pełnym zmian.

Każda zmiana zaczyna się w myśleniu – i – jak często podkreśla Jacek Walkiewicz⁷², to „[...] odwaga jest początkiem wszystkiego”. W tej drodze technologia jest tylko narzędziem. Najważniejszym architektem zmiany pozostaje człowiek (jego serce, świadomość, wizja). A przecież każda wielka zmiana zaczyna się od tej jednej myśli, że możliwe jest osiągnięcie czegoś więcej.

3. Identyfikacja i analiza głównych wyzwań psychospołecznych wyzwań w procesie zarządzania cyfryzacją w oświacie.

Ten rozdział podejmuje niezwykle ważne zagadnienie psychospołecznych wyzwań w obszarze zarządzania cyfryzacją w oświacie. Natalia Hatałska, założycielka instytutu⁷³ badań nad przyszłością (infuture.institute) i autorka bestsellerowej książki „Wiek Paradoksów. Czy technologia nas ocali?” napisała w niej: „Jednym z największych paradoksów rozwijających się technologii jest to, że nie można ich uregulować, zanim nie zostaną wdrożone – bo czy można było uregulować internet, zanim zaczęliśmy z niego korzystać?”. W swej wypowiedzi autorka podejmuje próbę zrozumienia, w jaki sposób technologia kształtuje codzienne doświadczenia, wpływając na relacje oraz struktury społeczne. a podejmowane analizy wprost zaprowadzą nas do powiązań omawianych Zdaniem Hatałskiej współcześni ludzie nie są już tylko użytkownikami technologii, ale stali się jej częścią. Takie postawienie sprawy rodzi wiele pytań, na które nie ma jeszcze odpowiedzi. W swej publikacji „Wiek Paradoksów. Czy technologia nas ocali?” autorka podejmuje wnikliwą analizę skoncentrowaną wokół następujących zagadnień:

- **Paradoks postępu** – zdaniem Hatałskiej technologia z jednej strony oferuje ogromne możliwości i potencjał do rozwiązywania różnorodnych problemów, ale jednocześnie stwarza nowe wyzwania i niepewności. Autorka wskazuje na sprzeczności wynikające z rozwoju technologicznego (technologie mają ułatwiać życie, ale często prowadzą do izolacji, dezinformacji i manipulacji).

⁷² Jacek Walkiewicz – autor bestsellerowych książek z zakresu rozwoju osobistego (np. „Pełna MOC możliwości” i „Pełna MOC życia. Jeśli o czymś w życiu marzysz – sięgnij po to”), psycholog i trener.

⁷³ Hatałska N., (2021), „Wiek Paradoksów. Czy technologia nas ocali?”, Kraków: Wydawnictwo ZNAK, s. 281–282.

- **Przyszłość pracy i edukacji** – autorka rozważa, w jaki sposób – pod wpływem automatyzacji i AI – zmieniający się rynek pracy zdeterminuje wybór ścieżki kariery i jakie główne kompetencje okażą się kluczowe w przyszłości. Podkreśla także potrzebę adaptacji systemów edukacji do nowych realiów.
- **Samotność w erze cyfrowej** – założycielka instytutu przyszłości analizuje, w jaki sposób narzędzia cyfrowe – zamiast łączyć ludzi – niejednokrotnie pogłębiają ich poczucie samotności i alienacji.
- **Informacyjny chaos i polaryzacja** – Hatałska ma świadomość, że świat cyfrowy zrodził nowe problemy. A są nimi: nadmiar informacji, fake newsy i bańki informacyjne, które przyczyniają się do polaryzacji społeczeństw i utrudniają budowanie wspólnego zrozumienia.
- **Granice postępu technologicznego** – autorka próbuje wyjaśnić, czy istnieją granice, których technologia nie powinna przekraczać, a także jakie są konsekwencje ich ewentualnego przekraczania.
- **Etyczne dylematy technologii** – założycielka instytutu przyszłości zajmuje się także kwestią granic wykorzystywania AI, ingerencją w ludzkie ciało i umysł (biohacking), a także podejmuje temat prywatności i bezpieczeństwa danych.

To tylko niektóre zagadnienia, wokół których Natalia Hatałska koncentruje swoją analizę. W książce „Wiek Paradoksów. Czy technologia nas ocali?” autorka stawia fundamentalne pytanie o rolę człowieka w świecie zdominowanym przez technologię. Czy cyfryzacja dla współczesnych będzie ocaleniem czy przekleństwem? Założycielka instytutu przyszłości nie oferuje prostych rozwiązań, lecz zachęca do refleksji i krytycznego myślenia o roli technologii w ludzkim życiu. Dlatego w tym rozdziale wnikliwsza analiza poszczególnych zagadnień pozwoli na poszerzenie własnego zrozumienia psychospołecznych wyzwań, które – w sposób bezpośredni lub mniej oczywisty – są powiązane z oświatą. W dalszym fragmencie niniejszego rozdziału zostaną omówione główne wyzwania psychospołeczne wiążące się z zarządzaniem cyfryzacją w edukacji.

Analiza obejmie zarówno zjawiska bezpośrednio związane z funkcjonowaniem osób i grup w środowisku cyfrowym, jak i te dotyczące tożsamości szkoły, równowagi psychicznej oraz jakości relacji. Każdy z omawianych aspektów (począwszy od przeciążenia informacyjnego, przez lęk przed zmianą, aż po kryzys wspólnotowości) odsłania nie tylko problemy techniczny, ale także ludzki wymiar transformacji dokonującej się we współczesnym świecie. Refleksja nad tymi wyzwaniami jest

konieczna, ponieważ stanowi niezbędny krok ku tworzeniu edukacji przyszłości (opartej nie tylko na technologii, ale i na trosce o dobrostan człowieka).

Wspomniane przemiany nie rozgrywają się w próżni, mają bardzo konkretne konsekwencje w codziennym funkcjonowaniu szkół i placówek edukacyjnych. Wymagają od nauczycieli, uczniów, dyrektorów i całych społeczności edukacyjnych mierzenia się z nowymi, często trudnymi doświadczeniami, które wpływają na ich samopoczucie psychiczne, relacje oraz poczucie sensu życia.

Poniżej zamieszczono katalog dziesięciu kluczowych psychospołecznych wyzwań, które zdaniem Zofii Domaradzkiej-Grochowalskiej – ujawniają się w procesie zarządzania cyfryzacją w środowisku oświatowym. Każde z nich dotyczy innego aspektu (poznawczego, emocjonalnego, relacyjnego lub strukturalnego), ale razem tworzą spójną mapę potrzeb, które powinny być uwzględnione przy projektowaniu systemowych rozwiązań, a tym bardziej przy planowaniu lokalnych strategii zarządzania cyfryzacją w oświacie. Poniżej zaprezentowano wybrane zagrożenia wynikające związane z obecnością technologii informatycznych w życiu współczesnych ludzi:

- **Nierówności w dostępie do technologii** – brak równego dostępu do sprzętu, internetu i kompetencji cyfrowych pogłębia wykluczenie społeczne, zarówno wśród uczniów, jak i nauczycieli.
- **Przeciążenie informacyjne (infobezwładność)** – nadmiar bodźców i komunikatów cyfrowych prowadzi do zmęczenia poznawczego, dekoncentracji i spadku efektywności uczenia się i nauczania.
- **Lęk przed technologią i opór wobec zmian** – jest on typowy szczególnie wśród starszych nauczycieli, którzy mają obawy związane z nieznaną narzędzi cyfrowych, koniecznością ciągłej adaptacji, a także lękiem przed ciągłym ocenianiem.
- **Spadek poczucia sensu pracy nauczyciela** – automatyzacja, standaryzacja i presja cyfrowych wskaźników mogą prowadzić do wypalenia, utraty autonomii i obniżenia motywacji wewnętrznej.
- **Kryzys tożsamości szkoły** – cyfryzacja redefiniuje misję szkoły jako miejsca społecznego spotkania, wspólnoty, kultury i wychowania. Pojawia się też pytanie o to, jaką rolę i funkcję mają pełnić jednostki edukacyjne w erze cyfrowej.
- **Osamotnienie i dezintegracja relacji** – w środowisku cyfrowym relacje ludzkie osłabiają się (w tym także te: nauczyciel – uczeń, uczeń – uczeń czy nauczyciel

- nauczyciel). Dzieje się tak m.in., że bardzo często brakuje przestrzeni na spontaniczne interakcje i emocjonalną obecność.
- **Obniżona odporność emocjonalna dzieci i młodzieży** – ciągła obecność uczniów w środowisku internetowym wpływa negatywnie na zdolność radzenia sobie z frustracją, samotnością i porażką. Wśród młodych ludzi wzrastają lęk, niepokój, a zachowania unikowe stają się normą.
- **Napięcia w komunikacji między nauczycielami a rodzicami** - przeniesienie kontaktu do kanałów cyfrowych często prowadzi do nieporozumień, skrótowości, braku empatii lub nadmiernej kontroli.
- **Brak systemowego wsparcia psychospołecznego** – zarządzanie cyfryzacją często koncentruje się na technice, zaniedbując przygotowanie ludzi. Okazuje się bowiem, że tym całym procesie brakuje przestrzeni na refleksję, superwizję, wsparcie emocjonalne i relacyjne.
- **Rozmycie granic między pracą a życiem prywatnym** – nauczanie zdalne i hybrydowe prowadzi do trudności w oddzieleniu czasu prywatnego od zawodowego czy szkolnego. Taka sytuacja obciąża psychicznie i prowadzi do chronicznego zmęczenia.

Zestawienie tych dziesięciu obszarów ma stanowić intelektualne narzędzie, które będzie pomocne w refleksji nad jakością procesu cyfryzacji w szkołach i planowanych programach wdrożeniowych w zakresie cyfryzacji oświaty w JST (Harmonogramach Działań Rozwojowych – dalej HDR). Każde z zagadnień przedstawionych powyżej wiąże się z konkretnymi mechanizmami psychologicznymi i społecznymi, które powinny zostać wzięte pod uwagę w praktyce zarządzania zmianą. Powinno się tak stać nie tylko w celu uniknięcia zagrożeń, ale po to, aby tworzyć edukację przyszłości zakorzenioną w ludzkich potrzebach.

Szanse i zagrożenia wynikające z obecności cyfryzacji w życiu psychospołecznym

Nierówności w dostępie do technologii

Mimo swego potencjału cyfryzacja edukacji ujawnia i pogłębia istniejące nierówności społeczne i edukacyjne. Jednym z najważniejszych problemów w tym zakresie jest nierówny dostęp do technologii cyfrowych zarówno w aspekcie sprzętowym (komputery, tablety, stabilne łącze internetowe), jak i kompetencyjnym (umiejętność korzystania z narzędzi, wsparcie rodziny, poziom cyfrowego obycia). Dla niektórych

uczniów (zwł. osób z mniejszych miejscowości, środowisk defaworyzowanych lub wielodzietnych rodzin) nauka zdalna i hybrydowa wiąże się z realnymi barierami w dostępie do edukacji. Podobne wyzwania dotyczą nauczycieli, którzy niejednokrotnie korzystają z przestarzałego sprzętu lub nie mają warunków domowych do pracy online. Zagadnienie nierówności w dostępie do technologii ma ścisły związek z wykluczeniem cyfrowym, o którym szeroko pisano w raporcie Fundacji Orange „Wykluczenie społeczno-cyfrowe w Polsce. Stan zjawiska, trendy i rekomendacje”⁷⁴. Materiał ten podkreślał, że wykluczenie cyfrowe nie ogranicza się jedynie do braku dostępu do sprzętu czy internetu, ale obejmuje również deficyty kompetencyjne i motywacyjne, które prowadzą do pogłębiania nierówności społecznych. Autorzy tego dokumentu wskazują na istnienie „błędnego koła nierówności”, w którym brak umiejętności cyfrowych i dostępu do technologii wzajemnie się wzmacniają, prowadząc do marginalizacji jednostek i społeczności. Warto jednak podkreślić, że od czasu publikacji tego podsumowania poprawiła się sytuacja wyposażenia uczniów i nauczycieli w laptopy, co było wynikiem rządowych programów (np. „Laptop dla ucznia”, „Laptop dla nauczyciela”). Niestety nadal jednak pojawiają się utrudnienia w wykorzystywaniu tych sprzętów ze względu na utrudnienia mające związek z dostępem do internetu.

Mechanizmy i skutki psychospołeczne

Brak dostępu do technologii nie jest jednak wyłącznie problemem technicznym, ponieważ powoduje także konkretne skutki psychologiczne i społeczne m.in.:

- wykluczenie i poczucie gorszości wśród uczniów, którzy nie mogą uczestniczyć na równych zasadach w zajęciach;
- wzrost napięcia i stresu u dzieci oraz młodzieży, którzy nie nadążają za tempem zadań lub nie rozumieją oczekiwań technologicznych;
- obniżenie motywacji i narastanie przekonania, że jest się słabszym lub mniej zdolnym od innych w klasie, a tak naprawdę okazuje się, że trudności mają charakter systemowy a nie indywidualny;
- utrudniona współpraca z rodzicami – szczególnie w środowiskach o niższym poziomie kompetencji cyfrowych lub językowych.

W kontekście placówek oświatowych prowadzi to do rozwarstwienia edukacyjnego, a także pogłębiania różnic w osiągnięciach i wpływa negatywnie na zjawisko

⁷⁴ Fundacja Orange (2021), „Wykluczenie społeczno-cyfrowe w Polsce. Stan zjawiska, trendy i rekomendacje”, Warszawa: Fundacja Orange, zob. <https://fundacja.orange.pl/strefa-wiedzy/post/wykluczenie-spoleczo-cyfrowe-w-polsce-2021> [dostęp, online dn. 2.09.2025].

dezintegracji społeczności danej szkoły, przedszkola, innego podmiotu edukacyjnego czy jednostki samorządowej.

Konsekwencje dla zarządzania

Brak równych szans dostępu do technologii – z perspektywy zarządzania cyfryzacją – stawia przed szkołami, przedszkolami, placówkami edukacyjnymi i JST konkretne wyzwania:

- W jaki sposób diagnozować rzeczywiste potrzeby uczniów i nauczycieli?
- Jak przeciwdziałać stygmatyzacji osób wykluczonych technologicznie?
- W jaki sposób rozdzielać zasoby w sposób sprawiedliwy i efektywny?
- Jak projektować cyfrową transformację w duchu inkluzji, a nie tylko nowoczesności?

Dobre praktyki i strategie wyrównywania szans

W odpowiedzi na konieczność stworzenia jednolitego systemu dostępu do technologii jednostki oświatowe i samorządy mogą wprowadzić następujące działania:

- mapowanie dostępności sprzętu i łączy wśród uczniów oraz nauczycieli (np. w formie anonimowych ankiet lub wywiadów środowiskowych);
- utworzenie banków sprzętu szkolnego (np. wypożyczalni komputerów, tabletów, routerów);
- indywidualizacja wsparcia dla uczniów zagrożonych wykluczeniem cyfrowym (np. zajęcia stacjonarne, opieka tutoringowa);
- organizowanie szkoleń dla rodziców i nauczycieli w celu rozwijania kompetencji i budowania poczucia wspólnoty oraz zaufania.

Przeciążenie informacyjne (infobezwładność⁷⁵)

W erze powszechnego dostępu do technologii cyfrowych uczniowie i nauczyciele funkcjonują w środowisku przesycanym bodźcami, komunikatami i danymi. Przeciążenie informacyjne (określane też mianem infobezwładności) jest stanem, w którym ilość napływających treści przekracza możliwości poznawcze jednostki. Taka sytuacja prowadzi do zmęczenia, dekoncentracji, utraty motywacji i obniżenia

⁷⁵ Infobezwładność – pojęcie określające stan przeciążenia informacyjnego, które prowadzi do bezwładności decyzyjnej. Terminu tego użyto w książce „Człowiek – Media – Edukacja”, aby scharakteryzować wyczerpanie i zmęczenie na skutek nadmiaru treści informatycznych. Por. Morańska D., Morbitzer J., Musiał E., Wojciechowski J., (red. nauk.), (2017), „Człowiek – Media – Edukacja”, Dąbrowa Górnicza: Wydawnictwo Naukowe Wyższa Szkoła Biznesu, s. xxx.

efektywności pracy umysłowej. W środowisku szkolnym zjawisko infobezwładności objawia się m.in. przez:

- przytłoczenie uczniów liczbą platform, narzędzi, komunikatów, zadań;
- nadmiar wymagań przekazywanych cyfrowo (np. przez e-dzienniki, czaty, e-maile);
- przeciążenie nauczycieli koniecznością ciągłego reagowania i przetwarzania informacji z różnych źródeł jednocześnie.

Taka sytuacja powoduje, że technologia cyfrowa – zamiast wspierać proces edukacyjny – staje się czynnikiem destabilizującym rytm i strukturę dnia szkolnego. Jest to szczególnie widoczne w szczególnie tych środowiskach, gdzie nie wprowadzono zasad higieny cyfrowej. Raport Cyfrowa Szkoła 4.0⁷⁶ podkreśla, że zarówno uczniowie, jak i nauczyciele nie posiadają wystarczających kompetencji zarządzania informacją i czasem w środowisku cyfrowym. Niektóre osoby z kadry nauczycielskiej deklarują, że codziennie korzystają z kilku różnych platform do komunikacji (w tym również do prowadzenia zajęć lub uczestniczenia w nich podczas szkoleń online). Taki natłok rozmaitych informacji prowadzi do przeciążenia. Na podobne zjawisko zwrócono również uwagę w raporcie Fundacji Orange⁷⁷, podkreślając, że poczucie wyobcowania cyfrowego wynika nie tylko z braku sprzętu, ale także nieumiejętności w selekcjonowaniu informacji i radzenia sobie z ich nadmiarem. Taka wygląda nowe oblicze informacyjnej nierówności edukacyjnej.

Psychologiczne skutki przeciążenia

Infobezwładność wpływa nie tylko na poznawcze możliwości uczniów i nauczycieli, ale również na ich dobrostan psychiczny i emocjonalny. Tym samym prowadzi do:

- trudności w koncentracji i uczeniu się;
- zmęczenia informacyjnego i zniechęcenia;
- niepokoju, napięcia i wzrostu lęku przed ciągłą koniecznością, aby z wszystkimi wiadomościami być na bieżąco i nie przegapić czegoś ważnego – Fear of Missing Out (dalej FOMO);
- spadku satysfakcji z pracy i poczucia sensu nauki;

⁷⁶ Związek Cyfrowa Polska, (2024), „Cyfrowa szkoła 4.0. Raport. Szkoła”. Warszawa: Cyfrowa Polska.

⁷⁷ Fundacja Orange (2021), „Wykluczenie społeczno-cyfrowe w Polsce. Stan zjawiska, trendy i rekomendacje”, Warszawa: Fundacja Orange, zob. <https://fundacja.orange.pl/strefa-wiedzy/post/wykluczenie-spolesno-cyfrowe-w-polsce-2021> [dostęp, online dn. 2.09.2025].

- zwiększonego poziomu stresu u nauczycieli, który wyrasta z presji stałej dostępności w sieci (np. dla uczniów, ich rodziców czy dyrekcji placówki).

Kierunki odpowiedzialnego zarządzania

W celu zapobiegania zjawisku infobezwładności w środowisku edukacyjnym szkoły, przedszkola, inne podmioty oświatowe i samorządowe mogą podjąć następujące działania:

- wprowadzać zasady higieny informacyjnej (np. ograniczenie liczby kanałów komunikacji, ustalone terminy dostępności, minimalizm cyfrowy polegający na celowym, świadomym i jakościowym – a nie przypadkowym i zbyt częstym korzystaniu z narzędzi cyfrowych);
- uczyć krytycznego odbioru informacji poprzez wyjaśnienie istoty dezinformacji, selekcję źródeł i filtrowanie treści;
- promować uważność cyfrową (np. praktyki skupienia, pauz, refleksji w trakcie dnia szkolnego);
- organizować przestrzeń do pracy głębokiej i offline;
- wspierać nauczycieli w zarządzaniu cyfrowym stresem (np. przez szkolenia, superwizje, planowanie pracy z technologią).

Lęk przed technologią i opór wobec zmian

Wdrażanie technologii cyfrowych w oświacie niesie ze sobą wiele zmian organizacyjnych, kulturowych i interpersonalnych. Jednymi z najczęściej obserwowanych zjawisk towarzyszących tym procesom są zarówno lęk przed technologią cyfrową (określany także jako technofobia), jak i wynikający z niego opór wobec zmian. Zjawisko to szczególnie silnie dotyka te osoby spośród kadry nauczycielskiej lub z grona pracowników administracyjnych, które odczuwają brak kompetencji cyfrowych, niepewność wobec nowych narzędzi, a także obawę przed utratą kontroli nad dotychczasowym sposobem pracy. W placówkach edukacyjnych, która przez lata były przestrzeniami bazującymi na przewidywalności i powtarzalności, gwałtowna digitalizacja bywa postrzegana jako destabilizująca i zagrażająca.

Psychospołeczne mechanizmy oporu

Opór wobec zmian technologicznych – z perspektywy psychologicznej – może być rozumiany jako naturalna reakcja adaptacyjna w sytuacji niepewności. Mechanizmy te obejmują m.in.:

- lęk poznawczy (przed nieznanym, przed oceną, przed utratą statusu eksperta);
- lęk społeczny (przed kompromitacją, wyśmianiem, niezrozumieniem);
- mechanizmy obronne (minimalizowanie znaczenia cyfryzacji, racjonalizacja, unikanie);
- utożsamianie tożsamości zawodowej z tradycyjnymi metodami pracy, co sprawia, że każda zmiana technologiczna jest przeżywana jako zagrożenie dla poczucia sensu i wartości.

Opór wobec narzędzi cyfrowych może mieć charakter jawny (sprzeciw wobec nowych rozwiązań, krytyka, bunt), ale również ukryty (bierność, „milczące sabotowanie” wdrożeń, pozorne wprowadzanie technologii). Bez wsparcia kompetencyjnego użytkowników prowadzi on często do frustracji, dalszego buntu oraz spadku efektywności procesów edukacyjnych. Z raportu Fundacji Orange z 2023 roku⁷⁸, wynika, że aż 38 proc. nauczycieli odczuwa niepewność wobec nowych technologii, co wpływa na ich zaangażowanie w proces transformacji cyfrowej.

Konsekwencje dla procesu zarządzania cyfryzacją

Lęk i opór wobec zmian technologicznych mogą znacząco utrudniać proces cyfryzacji, prowadząc do:

- obniżenia zaangażowania nauczycieli w procesy transformacyjne;
- pogłębienia polaryzacji zespołów (wyraźny podział na cyfrowych pionierów i tradycjonalistów);
- spowolnienia wprowadzania nowych rozwiązań lub ich wdrażania bez przekonania i refleksji pedagogicznej;
- zaniżenia efektywności szkoleń i rozwoju kompetencji cyfrowych;
- wzrostu napięcia relacyjnego w środowisku szkolnym.

Strategie wsparcia i środki zaradcze

Zagadnienia dotyczące zarządzania zmianą były dotychczas szeroko podejmowane w ORE, czego dowodem są liczne materiały szkoleniowe oraz publikacje na ten temat. Poniżej

⁷⁸ Fundacja Orange, (2023), „Raport o edukacji cyfrowej w Polsce: Trendy i wyzwania”, Warszawa: Fundacja Orange.

zamieszczono tylko wybrane zagadnienia, czyniąc z nich inspirację dalszego pogłębiania. W celu przeciwdziałania lękowi przed technologią i oporowi wobec zmian niezwykle ważne są następujące działania:

- **prowadzenie procesów zmiany w sposób partycypacyjny** – angażowanie zespołów w podejmowanie decyzji;
- **zapewnienie bezpiecznej przestrzeni do nauki** – inicjowanie szkoleń w atmosferze wolnej od oceny i presji;
- **wsparcie emocjonalne i mentoring** – budowanie środowiska zaufania, w którym można mówić o trudnościach i obawach;
- **docenienie i włączenie różnorodnych perspektyw** – jest to szczególnie ważny aspekt dla osób z mniejszymi kompetencjami technologicznymi;
- **narracja osadzona w sensie i wartościach** – wyjaśnianie roli i funkcji cyfryzacji (jej istoty), a nie wyłącznie skupianie się na kwestiach technicznych związanych z wdrożeniem tego narzędzia cyfrowego.

Spadek poczucia sensu pracy nauczyciela

Z obserwacji autorki niniejszego opracowania wynika, że w ostatnich latach coraz częściej słyszy się o braku szacunku do pracy nauczycieli, o ich wypaleniu zawodowym. Być może taka sytuacja ma miejsce m.in. dlatego, że w procesie cyfryzacji oświaty jednym z rzadziej diagnozowanych, lecz wyjątkowo istotnych zjawisk, jest utrata sensu wykonywania swojej pracy odczuwana przez wielu nauczycieli. Transformacja technologiczna w szkołach i placówkach edukacyjnych – szczególnie w warunkach presji systemowej i dynamicznych zmian – prowadzi do zakwestionowania dotychczasowych metod nauczania, osłabienia relacyjnej strony zawodu i poczucia wpływu na proces edukacyjny. Coraz częściej nauczyciele deklarują, że czują się bardziej operatorami narzędzi i realizatorami cyfrowych programów niż wychowawcami i towarzyszami w rozwoju ucznia.

Psychospołeczne mechanizmy i konsekwencje

Utrata sensu pracy zawodowej jest zjawiskiem złożonym, który ściśle się wiąże z następującymi aspektami:

- **obniżeniem poczucia autonomii** – nauczyciele czują, że coraz więcej decyzji jest narzucanych z zewnątrz (np. przez systemy, aplikacje, wymagania zdalnych platform);

- **brakiem widocznych rezultatów pracy** – szczególnie w nauczaniu online trudno o natychmiastowy, emocjonalny komentarz zwrotny, który – w tradycyjnym pojmowaniu pracy nauczyciela – stanowił o istocie jego pracy;
- **wypaleniem relacyjnym** – brak codziennego, spontanicznego kontaktu z uczniem, rozmów pomiędzy zajęciami (np. na przerwie czy wycieczce), żartów, które wcześniej stanowiły źródło energii i satysfakcji nauczycielskiej;
- **presją wyników i technologicznej sprawności** – nauczyciele, żyjąc w ciągłej presji, aby dobrze wypaść przed uczniami, ich rodzicami czy kadrą kierowniczą placówki, zagubili emocjonalny aspekt swojej pracy (np. zamiast pytać dzieci i młodzież o ich samopoczucie, to koncentrują się na kwestiach związanych z obsługą narzędzi cyfrowych. Dociekają i stresują się tym, czy wszystko się nagrało, czy jakiś plik właściwie został zapisany itp.

Jeżeli przywołane powyżej sytuacje skumulują w codzienności nauczyciela, to niestety prowadzą do zjawiska wypalenia zawodowego, a w niektórych przypadkach nawet do decyzji o odejściu z zawodu.

Kontekst zarządzania cyfryzacją

W procesie zarządzania zmianą cyfrową w placówkach edukacyjnych często pomija się aspekt tożsamości zawodowej nauczyciela, gdyż więcej uwagi poświęca się kwestiom technicznym i infrastrukturze. W takiej sytuacji bardzo łatwo przeoczyć pytania, na które warto wspólnie poszukać odpowiedzi:

- Jakie miejsce w cyfrowym świecie dostrzega dla siebie nauczyciel?
- Czy nadal czuje się potrzebny i sprawczy?
- Jaki wpływ – z perspektywy nauczyciela – pełni cyfryzacja w jego codziennej pracy?
- W jakim stopniu cyfryzacja wspiera nauczycielską misję, a w jakim ją osłabia?

Więcej informacji na ten temat zamieszczono w podrozdziale „Związek między kompetencjami osób zarządzających jednostkami edukacyjnymi a przebiegiem procesu cyfryzacji”. Placówki oświatowe, które pragną wprowadzać technologie w sposób dojrzały i holistyczny, powinny zaopiekować się emocjonalnym i tożsamościowym wymiarem pracy pedagogicznej.

Strategie wsparcia

Należy podejmować wszelkie inicjatywy, aby przeciwdziałać sytuacjom, w których nauczyciele utracą sens pracy w środowisku cyfrowym. Dlatego tak wartościowe są następujące inicjatywy:

- **superwizje zespołowe i indywidualne**, które pozwalają nauczycielom kadry nauczycielskiej na refleksję nad własnym doświadczeniem i przekształcanie kryzysu w rozwój;
- **budowanie kultury uznania** – mówienie o tym, co wartościowe w pracy nauczyciela (w tym również w warunkach cyfrowych);
- **łączone formy nauczania** – wprowadzanie – tam, gdzie to tylko możliwe – elementów obecności i bezpośrednich relacji (opartych na szczerości, otwartości, empatii, aktywnego słuchania, zaufania);
- **dzielenie się dobrymi praktykami i wzajemne wspieranie w zespołach nauczycielskich** – wymienianie się sprawdzonymi i efektywnymi metodami działania, które przynosząc dobre wyniki, są trwałe i powtarzalne, a tym samym mogą być stosowane w innych placówkach edukacyjnych i przez innych nauczycieli;
- **wzmacnianie narracji o sensie zawodu** nie tylko jako transmisji wiedzy, ale towarzyszenia, obecności i współtworzenia doświadczenia edukacyjnego.

Kryzys tożsamości szkoły

Cyfryzacja w edukacji to nie tylko zmiana narzędzi, ale również głęboka transformacja funkcji i wizerunku placówek edukacyjnych. W szczególności było to widoczne w okresie pandemii Covid-19, kiedy nauka przeniosła się do internetu. W czasach obecnych funkcjonowanie technologii informatycznych w polskiej szkole jest nadal niezwykle istotne, ponieważ często zachodzi konieczność nauczania zdalnego, edukacji hybrydowej i powszechnego dostępu do wiedzy online. Powszechność dostępu do narzędzi cyfryzacyjnych prowadzi do tego, że jednostki edukacyjne przestają być wyłącznym źródłem informacji i instytucjami przekazu wiedzy. Wobec tego warto sobie zadać pytania, jaka jest rola i funkcja szkoły, co buduje jej tożsamość:

- Czym współcześnie ma być szkoła, skoro wiedza jest dostępna wszędzie?
- Jaką wartość niesie wspólnota szkolna, jeśli relacje przenoszą się do przestrzeni cyfrowej?
- Na czym polega wychowanie w środowisku rozproszonym przez technologie?

Zarówno z obserwacji autorki niniejszego rozdziału, jak i wnioski wypływające z dyskusji w środowisku oświatowym wynika, że wiele szkół w Polsce doświadcza kryzysu tożsamości. Placówki te bezskutecznie próbuje odnaleźć się w nowej rzeczywistości, niejako miotając się pomiędzy dawną funkcją wychowawczo-społeczną a nowymi oczekiwaniami, które związanymi wiążą się z efektywnością, elastycznością i innowacyjnością.

Psychospołeczne wymiary kryzysu

Kryzys tożsamości placówek oświatowych ujawnia się na kilku poziomach:

- symbolicznym – szkoła traci status „świątyni wiedzy”, a staje się symbolem platformy usług edukacyjnych;
- społecznym – osłabieniu ulegają więzi między nauczycielami, uczniami i rodzicami (zwłaszcza w środowisku cyfrowym);
- egzystencjalnym – osoby pracujące w szkole (dyrektorzy, pedagodzy, nauczyciele) doświadczają niepewności co do sensu i kierunku swojego działania.

Konsekwencje dla zarządzania cyfryzacją

Zarządzanie szkołą w dobie cyfryzacji wymaga świadomego prowadzenia instytucji przez proces redefinicji jej tożsamości. Dlatego w całym procesie nie chodzi wyłącznie o efektywne wdrożenie sprzętu czy platform edukacyjnych, ale o uświadomienie sobie, **jaką wspólnotę chce się budować** dzięki technologii informatycznej. Jeśli cyfryzacja ma być trwałą częścią edukacji, szkoły muszą odnaleźć nowy sens bycia miejscem spotkania, wychowania, obecności i troski. W świecie cyfrowym nie ma przestrzeni na tradycyjne formy wspólnoty (np. apele, wycieczki, nieformalne rozmowy na przerwach). To zaś może pogłębiać poczucie rozproszenia i utraty zakorzenienia w środowisku. Cyfrowe narzędzia, choć są wydajne, często nie wspierają głębokiego doświadczenia przynależności, które jest pierwotną potrzebą rozwoju psychospołecznego każdego człowieka.

Możliwe kierunki odpowiedzi

W odpowiedzi na kryzys tożsamości szkoły oraz instytucje edukacyjne mogą:

- tworzyć – także w środowisku cyfrowym – nowe rytuały wspólnotowe (np. cyfrowe święta, grupy refleksyjne, inicjatywy społeczne);
- wzmacniać rolę szkoły jako przestrzeni formacyjnej i wychowawczej nawet wówczas, gdy część zajęć odbywa się online;
- wprowadzać do pracy dydaktycznej elementy pedagogiki obecności i relacji (np. „emocjonalne momenty zatrzymania”, wspólne refleksje);

- inwestować w kompetencje tożsamościowe liderów szkoły w taki sposób, aby potrafili łączyć cele cyfrowe z misją społeczną.

Zagadnienie kryzysu tożsamości szkoły jest jednym z tych wyzwań psychospołecznych, które ściśle nawiązuje do cytatu, od którego rozpoczyna się ten rozdział. Nie znamy jeszcze odpowiedzi na pytania o to jak będzie ewoluowała tożsamość szkoły w dobie cyfryzacji.

Osamotnienie i dezintegracja relacji

Jednym z najbardziej dotkliwych i długofalowych skutków cyfryzacji edukacji – szczególnie w okresie pandemii, ale również w modelach nauczania hybrydowego – jest poczucie osamotnienia wśród uczniów, nauczycieli i całych społeczności szkolnych. Przeniesienie zajęć do przestrzeni cyfrowej osłabiło naturalne kanały kontaktu międzyludzkiego, w których rodzi się wzajemne zaufanie, empatia, poczucie wspólnoty i przynależności. I choć technologia informatyczna umożliwia komunikację, często dzieje się to bez głębi relacyjnej (z pominięciem gestów, spojrzeń, ciszy czy wspólnego bycia). Uczniowie, którzy są pozbawieni codziennych interakcji rówieśniczych, częściej doświadczają izolacji. Z kolei nauczyciele deklarują brak więzi nie tylko z uczniami, ale także w samym środowisku nauczycielskim. Szkoła – dotychczas przestrzeń społecznego dojrzewania – staje się coraz bardziej funkcjonalna i zadaniowa.

Psychospołeczne skutki osamotnienia

Osamotnienie i dezintegracja relacji w środowisku edukacyjnym niosą szereg wiele negatywnych konsekwencji:

- **u uczniów:** spadek motywacji, trudności emocjonalne, wzrost lęku i zachowań unikowych, osłabienie kompetencji społecznych (np. rozwiązywania konfliktów);
- **u nauczycieli:** poczucie oderwania od misji wychowawczej, utrata satysfakcji zawodowej, brak oparcia w zespole;
- **na poziomie szkoły:** rozluźnienie więzi instytucjonalnych, wzrost indywidualizmu i braku odpowiedzialności za wspólne dobro.

Nikogo już to nie dziwi, że relacje cyfrowe często mają charakter transakcyjny, służąc przekazowi treści, a nie współobecności. Brakuje przestrzeni na „międzyczas” (spontaniczne rozmowy, śmiech, ciszę, nieformalny kontakt), który buduje wspólnotę.

Znaczenie tego wyzwania w zarządzaniu

Zarządzanie cyfryzacją szkoły nie może opierać się wyłącznie na wdrażaniu platform, aplikacji i systemów. Kryzys relacyjny towarzyszący technologizacji edukacji musi być

uznany za strategiczne wyzwanie, które wpływa na klimat placówki edukacyjnej, dobrostan, zaangażowanie i efektywność. Szkoły, które chcą się cyfryzować odpowiedzialnie, muszą zadbać o społeczny wymiar edukacji – zarówno w sferze dydaktycznej, jak i wychowawczej.

Możliwe odpowiedzi i działania

W celu przeciwdziałania osamotnieniu i dezintegracji relacji szkoły mogą podejmować następujące działania:

- **tworzyć struktury obecności** – „check-iny emocjonalne”, refleksje na koniec lekcji, „rundy empatii”;
- **organizować wspólne aktywności hybrydowe** – włączając uczniów we wspólne inicjatywy online i offline (np. wspólne akcje społeczne, projektowe);
- **wzmacniać relacje w zespołach nauczycielskich** – m.in. poprzez regularne spotkania nie tylko służbowe, ale też wspierające (superwizje, kręgi);
- **włączać uczniów do współtworzenia szkoły cyfrowej** – dając im głos i poczucie wpływu na rzeczywistość;
- **uczyć relacyjności w środowisku cyfrowym** – zwracając uwagę, np. na sposoby okazywania sympatii przez ekran i budowania relacji bez fizycznej obecności.

Obniżona odporność emocjonalna dzieci i młodzieży

W czasach obecnych – wraz z rosnącą obecnością technologii cyfrowych w życiu dzieci i młodzieży – można zaobserwować narastające zjawisko obniżonej odporności emocjonalnej. Postrzega się ją jako trudność w radzeniu sobie z frustracją, stresem, samotnością czy porażką. Zmiana środowiska edukacyjnego z realnego na cyfrowe pozbawiła uczniów wielu codziennych sytuacji społecznych, w których naturalnie rozwijają się mechanizmy samoregulacji i dojrzałości emocjonalnej. Ten trend został potwierdzony w ogólnopolskim badaniu Fundacji UNAWEZA „Młode Głowy”⁷⁹, które objęło ponad 180 tysięcy uczniów. Raport pokazał skalę trudności psychicznych młodzieży w Polsce:

- 42,7 proc. młodych osób nie odczuwa radości z życia;
- 39,7 proc. uczniów nie czuje się potrzebnych;
- ponad jedna trzecia młodych osób doświadcza myśli rezygnacyjnych lub autodestrukcyjnych.

⁷⁹ „Młode Głowy” – to program profilaktyczny, który powstał z inicjatywy Fundacji UNAWEZA w 2023 roku. Projekt ten koncentruje się na kwestii zdrowia psychicznego, poczucia własnej wartości i sprawczości wśród młodych ludzi, zob. <https://www.unaweza.org/komu-pomagamy/mlode-glowsy> [dostęp, online dn. 2.09.2025].

Szczególnie niepokojące i alarmujące są dane, z których wynika, że 38,4 proc. uczniów, nie ma z kim porozmawiać o swoich problemach. Taka sytuacja powoduje, że ci młodzi ludzie są jeszcze bardziej podatni na przeciążenie psychiczne w środowisku edukacyjnym i cyfrowym.

Psychologiczne mechanizmy i objawy

Obniżona odporność emocjonalna ujawnia się w następujących zachowaniach:

- szybka rezygnacja z trudnych zadań (komunikaty typu: *nie rozumiem, nie robię*);
- unikanie kontaktu (brak włączania kamery, nieodpowiadanie na wiadomości);
- wybuchy emocjonalne, trudności z koncentracją, drażliwość;
- pogłębiające się poczucie bezsilności i niska samoocena.

Z badań wynika, że ciągła obecność w środowisku online wiąże się z większym ryzykiem lęków, zaburzeń nastroju, uzależnień behawioralnych i trudności z budowaniem tożsamości. Raport „Młode Głowy” wskazuje również, że młodzież często nie wierzy w siebie, swoje możliwości ani wpływ na rzeczywistość. To zjawisko można rozumieć jako wyuczoną bezradność, której korzenie tkwią zarówno w środowisku domowym, jak i edukacyjnym (pozbawionym przestrzeni na rozmowę o emocjach i doświadczeniach wewnętrznych). W efekcie przeprowadzonych analiz wyłonił się obraz kondycji psychicznej dzieci i młodzieży, który obrazuje poniższa ilustracja.



Rysunek 1. Triada kryzysu psychicznego dzieci i młodzieży sporządzona na podstawie raportu „MŁODE GŁOWY. Otwarcie o zdrowiu psychicznym”. Opracowanie własne.

Obraz kryzysu psychicznego młodych ludzi dopełnia jeszcze niski poziom zaufania społecznego, brak wiary w skuteczność profesjonalnej pomocy oraz skala doświadczanej przemocy rówieśniczej, domowej i hejtu. Dzieci w kryzysie psychicznym to osoby przekonane, że nic nie znaczą, niczego nie potrafią i dla nikogo nie są ważne.

Jaki związek jest pomiędzy edukacją cyfrową a emocjami dzieci i młodzieży? Cyfrowe środowisko uczenia się (zdalne nauczanie) często jest pozbawione subtelnych sygnałów niewerbalnych (np. mimiki, tonu głosu, mikroreakcji grupy). Uczniowie pozostają w informacyjnym kontakcie, ale bez emocjonalnego oparcia. Zdarza się, że nauczyciel na ekranie monitora widzi jedynie ikonę ucznia, nie mając żadnej informacji zwrotnej o jego stanie psychofizycznym. Ponadto tempo, natężenie bodźców i styl komunikacji w środowisku cyfrowym często wywołują przeciążenie emocjonalne, którego uczniowie nie potrafią nazwać ani przepracować. Młodzi ludzie coraz częściej przeżywają swoje emocje w izolacji, bez języka, wsparcia i relacji, które umożliwiałyby im oswojenie trudnych stanów.

Kierunki działań i wsparcia

Placówki edukacyjne jako instytucje wychowawcze – celem przeciwdziałania osłabieniu odporności emocjonalnej – są zobowiązane, aby:

- wprowadzać edukację emocjonalną jako stały element programowy, niezależnie od formy nauczania;
- stosować elementy check-inów emocjonalnych, rozmów refleksyjnych i pracy z emocjami w czasie lekcji;
- zapewniać dostęp do specjalistycznego wsparcia psychologicznego i pedagogicznego (również online);
- rozwijać empatię cyfrową wśród nauczycieli i uczniów (polegająca na rozpoznawaniu emocji w środowisku zapośredniczonym);
- tworzyć rytuały bezpieczeństwa: przewidywalność, uzgodnione zasady, wspólne otwieranie i zamykanie zajęć.

Napięcia w komunikacji między nauczycielami a rodzicami

Wraz z cyfryzacją edukacji istotnie zmienił się sposób komunikacji pomiędzy nauczycielami, a rodzicami. Narzędzia informatyczne (np. e-dzienniki, aplikacje klasowe, komunikatory czy wiadomości mailowe) zwiększyły częstotliwość i natychmiastowość kontaktu, ale równocześnie doprowadziły do nowych napięć i nieporozumień na linii

szkoła – dom. Cyfrowe narzędzia nierzadko wypierają bezpośredni dialog a skrótowy styl komunikacji pisemnej (pozbawiony tonu głosu, kontekstu i emocji) sprzyja błędnym interpretacjom, nadinterpretacjom i eskalacji konfliktów. Rodzice częściej wchodzą w rolę „kontrolerów”, a nauczyciele – w rolę „nadawców informacji” bez realnej przestrzeni do wyjaśnienia swoich decyzji i działań.

Psychospołeczne źródła napięć

Zjawisko napięcia w komunikacji między nauczycielami a rodzicami ma głębokie podłoże psychospołeczne. Przyczynami takiej negatywnej sytuacji mogą być:

- **Różne oczekiwania wobec roli szkoły i nauczyciela** – rodzice oczekują szybkich odpowiedzi, indywidualnego traktowania, rozwiązywania problemów w trybie natychmiastowym.
- **Brak wspólnej przestrzeni relacyjnej** – cyfrowa forma kontaktu rzadko daje szansę na autentyczne poznanie się, budowanie zaufania i wzajemnego szacunku.
- **Zderzenie emocji** – rodzic działa z poziomu troski i niepokoju, gdy tymczasem nauczyciel – z poziomu odpowiedzialności i obciążenia. Bez uważnego pośrednictwa często dochodzi do frustracji po obu stronach.
- **Brak jasnych reguł i granic komunikacyjnych** – wielu nauczycieli otrzymuje wiadomości elektroniczne wieczorami, w weekendy, w inne dni wolne od pracy (np. w święta) z oczekiwaniem nadawcy do natychmiastowej odpowiedzi.

Konsekwencje dla dobrostanu i funkcjonowania szkoły

Długotrwałe napięcia w komunikacji na linii nauczyciel – rodzic mogą skutkować:

- wypaleniem emocjonalnym nauczycieli, którzy czują się oceniani i atakowani;
- narastaniem nieufności i antagonizmów między gronem pedagogicznym a rodzicami;
- utratą poczucia wspólnej odpowiedzialności za wychowanie i edukację dziecka;
- obniżeniem jakości współpracy, co bezpośrednio odbija się na dobrostanie uczniów;
- narastającą falą wzajemnej niechęci;
- przenoszenia napięć pomiędzy dorosłymi na kontakty z uczniami;
- odreagowywanie w domu wszelkich problemów i konfliktów dotyczących kontaktu ze szkołą, co może utrwalać nieprzyjazną szkole narrację.

Kierunki działań i dobre praktyki

Placówki oświatowe w celu zredukowania napięcia i zbudowania zdrowej komunikacji w erze cyfrowej mogą podejmować następujące działania:

- wspólnie z rodzicami ustalić zasady komunikacji cyfrowej – godziny, zakres tematów, czas reakcji;
- organizować spotkania w formule dialogowej (np. kręgi naprawcze rodzic – nauczyciel), które budują i wzmacniają relacje oparte na wzajemnym słuchaniu;
- szkolić nauczycieli w zakresie komunikacji empatycznej i asertywnej (zwł. w sytuacjach konfliktowych);
- promować język szacunku i konstruktywnej informacji zwrotnej zarówno w komunikatach szkolnych, jak rodzicielskich;
- tworzyć przestrzeń wspólnego działania (np. projekty klasowe, wspólne inicjatywy solidaryzujące i angażujące wszystkie osoby).

Brak systemowego wsparcia psychospołecznego

Choć cyfryzacja edukacji wiąże się z licznymi wymaganiami wobec uczniów, nauczycieli i całych społeczności szkolnych, systemowe wsparcie w zakresie zdrowia psychicznego i dobrostanu emocjonalnego nadal pozostaje ograniczone, fragmentaryczne i niewystarczające. Przemiany technologiczne zachodzą szybciej niż rozwój narzędzi, struktur i polityk publicznych, które miałyby chronić ludzi przed psychospołecznymi kosztami tej zmiany. W praktyce oznacza to więc, że często placówki edukacyjne nie otrzymują żadnego wsparcia i same muszą mierzyć się z następującymi trudnościami:

- problemami emocjonalnymi i psychicznymi uczniów;
- przeciążeniami i wypaleniem zawodowym nauczycieli;
- napięciami w relacjach między rodzicami a personelem szkolnym;
- brakiem narzędzi do pracy z kryzysem, traumą, przeciążeniem informacyjnym.

W Polsce liczba psychologów szkolnych, pedagogów i specjalistów wspierających nie jest adekwatna do potrzeb. Dlatego też wiele obowiązków, które są związane z dobrostanem uczniów, spoczywa głównie na nauczycielach i wychowawcach. Warto też sobie uzmysłwić, że nie istnieją ujednolicone programy przeciwdziałania wypaleniu zawodowemu nauczycieli, brakuje stałych funduszy na superwizję, interwizję czy interwencje kryzysowe w jednostkach oświatowych. Ponadto szkolenia dla nauczycieli z zakresu wsparcia emocjonalnego mają charakter jednorazowy a nie cykliczny.

Psychospołeczne konsekwencje braku wsparcia

Brak systemowego wsparcia prowadzi do:

- przeciążenia emocjonalnego kadry pedagogicznej, która nie ma przestrzeni na refleksję i regenerację;
- nieskutecznych lub reaktywnych działań pomocowych, uruchamianych dopiero w sytuacjach kryzysowych;
- poczucia osamotnienia i bezradności zarówno wśród nauczycieli, jak i uczniów;
- braku spójnych standardów pomocy psychologiczno-pedagogicznej, co skutkuje nierównościami wsparcia w różnych szkołach i regionach.

Zalecenia w sprawie stworzenia wsparcia psychospołecznego

W celu stworzenia realnego, systemowego wsparcia psychospołecznego w kontekście cyfryzacji oświaty należy położyć nacisk na następujące działania:

- stałe finansowanie w szkołach etatów specjalistów (psychologów, terapeutów, mediatorów);
- włączenie wsparcia psychicznego i emocjonalnego do polityki zarządzania oświatą, nie tylko jako dodatku, ale jako jej istotnego komponentu;
- tworzenie regionalnych centrów wsparcia psychospołecznego dla szkół i oferowanie superwizji, konsultacji, interwencji kryzysowych;
- szkolenia dla liderów oświaty z zakresu zarządzania dobrostanem, budowania odporności i troski o zdrowie psychiczne zespołów;
- obowiązkowe komponenty psychoedukacyjne w programach nauczania (nie tylko jako treści wychowawcze, ale zintegrowane z codziennym funkcjonowaniem szkoły).

Rozmycie granic między pracą a życiem prywatnym

Cyfryzacja edukacji niesie za sobą rewolucyjną zmianę w organizacji pracy nauczyciela i ucznia. Jednym z jej najgłębszych skutków psychospołecznych jest rozmycie granic między przestrzenią zawodową a osobistą (zwł. w kontekście pracy zdalnej, hybrydowej i całodobowej dostępności przez narzędzia cyfrowe). Nauczyciele coraz częściej wykonują obowiązki poza godzinami pracy, odpowiadając na wiadomości od rodziców wieczorami, poprawiając nocami sprawdziany, przygotowując materiały w weekendy. Uczniowie z kolei funkcjonują w świecie nieustannego dostępu do

zadań domowych, wiadomości i przypomnień. Niestety obecność narzędzi cyfrowych w edukacji sprzyja zacieraniu granic poprzez następujące czynniki:

- brak fizycznej separacji miejsca pracy i domu (co było zwłaszcza typowe dla w czasie nauki zdalnej podczas pandemii);
- ciągłe powiadomienia i dostępność komunikacyjna;
- presję społeczną bycia responsywnym i stale dostępnym;
- brak ustalonych ram czasowych dla zadań i komunikacji (np. metaforycznie traktowany brak godzin pracy);

Psychospołeczne skutki zacierania się granic

Brak wyraźnego oddzielenia pracy od życia prywatnego prowadzi do:

- przewlekłego zmęczenia i wypalenia zawodowego;
- utraty poczucia czasu wolnego i regeneracji;
- obniżenia jakości życia rodzinnego i relacji osobistych;
- poczucia winy i napięcia związanego z ciągłym brakiem czasu na wykonanie wszystkich potrzebnych zadań lub nadążania za czymś, co dzieje się zbyt szybko;
- trudności w wyłączeniu się z roli zawodowej (w tym także emocjonalnie i psychicznie).

Dla nauczycieli, których zawód już wcześniej był obciążony wysokim poziomem odpowiedzialności i stresu, cyfrowe przenikanie się ról może prowadzić do poważnych konsekwencji zdrowotnych i egzystencjalnych.

Strategie zaradcze

Placówki oświatowe w celu zapewnienia swoim pracownikom ochrony granic między pracą w szkole a ich życiem prywatnym powinny:

- tworzyć i egzekwować polityki higieny cyfrowej (np. zrezygnować z wysyłania wiadomości elektronicznych po określonej godzinie);
- wspierać nauczycieli w planowaniu pracy i zarządzaniu czasem cyfrowym;
- organizować warsztaty dla uczniów i rodziców na temat granic psychologicznych i cyfrowych;
- wprowadzać praktyki regeneracyjne (np. przerwy, oddechowe momenty offline, pracę głęboką zamiast reaktywną);
- modelować równowagę przez postawę liderów – dyrekcja i wychowawcy przykładem zdrowego dystansu do pracy.

Podsumowanie

W procesie cyfryzacji oświaty wiele miejsca poświęca się kwestiom technicznym, a tak niewiele uwagi koncentruje się na człowieku. Dyskusja na temat platform, sprzętu i systemów spycha na margines to, co jest najbardziej poruszające, czyli kondycję psychofizyczną dzieci i młodzieży, nauczycieli, innych pracowników szkoły oraz kadry zarządczej. W powszechnej świadomości problem praktycznie nie istnieje, bo go nie widać. A przecież na co dzień można zaobserwować, że lęk, przeciążenie, osamotnienie, rozmycie granic, napięcia w relacjach, utrata sensu wykonywanej pracy to zjawiska, które naprawdę istnieją. Dzieją się w przestrzeniach delikatnych, intymnych, wymagających szczególnej uważności, bo wewnątrz ludzi i pomiędzy nimi.

Dlatego właśnie ta część publikacji – opisująca dziesięć psychospołecznych wyzwań cyfryzacji – nie ma formy listy problemów, lecz stanowi zaproszenie do innego spojrzenia na szkołę i placówki edukacyjne. Warto zauważyć, że podmioty edukacyjne przypominają żywy organizm. Są wspólnotą, która doświadcza kryzysu, ale także ma w sobie ogromny potencjał regeneracji. Może to się jednak tylko wówczas, gdy zostanie otoczona troską, wsparciem i mądrym zarządzaniem. Każde z tych wyzwań może być odrębnym pytaniem na temat tego, jaki model przywództwa będzie rozwijany w placówkach edukacyjnych. Czy będzie to obszar, w którym zarządzanie odbywa się przez biurokrację, czy środowisko, w którym główny nacisk kładzie się na relacje międzyludzkie. Warto też rozważyć rolę JST w procesie cyfryzacji. Czy organy samorządowe zaangażują się wyłącznie w innowację technologiczną, czy przede wszystkim skoncentrują się na człowieku. Tak naprawdę to przecież on zarządza technologią i ją obsługuje. I dlatego być może dlatego w centrum transformacji cyfrowej polskiej szkoły powinno się pojawić pytanie dotyczące nie tyle technicznego sposobu przeprowadzenia całej operacji, ale precyzyjnego określenia, kto jest jej adresatem. Czy osoby te w szkole lub innej placówce oświatowej czują się zauważone, wysłuchane i potrzebne.

4. Modele zarządzania cyfryzacją w oświacie wobec transformacji myślenia o współczesnej edukacji.

Autorce niniejszego rozdziału – podczas opracowywania koncepcji tej publikacji – zależało na tym, aby wykazać związek między wyzwaniami psychospołecznymi a modelami zarządzania i kultury organizacyjnej na poziomie JST oraz placówek edukacyjnych. Tym samym chciała skoncentrować uwagę czytelników na głębi systemową podejmowanych tematów. Okazuje się bowiem, że czynniki psychospołeczne nie są tylko nieistotnym tłem, ale stanowią główne elementami, które gwarantują powodzenie transformacji cyfrowej w edukacji. Sama szkoła i inne placówki oświatowe stały się środowiskiem głębokich przemian zarówno w sposobie myślenia, pojmowania relacji międzyludzkich, odpowiedzialności i własnej tożsamości. Zatem trzeba sobie uzmysłowić, że o powodzeniu cyfryzacji w podmiotach oświatowych i samorządowych nie decyduje więc wyłącznie infrastruktura techniczna, ale przede wszystkim kultura organizacyjna oraz model zarządzania (zarówno na poziomie szkoły, jak i JST). Dziesięć autorskich psychospołecznych wyzwań cyfryzacji w oświacie, które zaprezentowano powyżej, dowodzą, że problemy technologiczne nierozzerwalnie wiążą się ze sposobem zarządzania jednostką oświatową, a także pojmowania roli liderów edukacyjnych.

Związek między wyzwaniami psychospołecznymi a kulturą i zarządzaniem w szkole i placówce edukacyjnej

Nierówności w dostępie do technologii

Modele zarządzania na poziomie JST powinny uwzględniać mapę lokalnych nierówności i rozpowszechniać zasoby zgodnie z realnymi potrzebami szkół, przedszkoli i jednostek edukacyjnych. Dlatego tak potrzebne są **kultury organizacyjne oparte na solidarności**. Punktem wyjścia jest operacyjna rzetelność w pomiarze inwentaryzacyjnym między stanem posiadania a oczekiwaniami.

Lęk przed technologią i opór wobec zmian

Transformacja cyfrowa wymaga zarządzania opartego na zaufaniu i wspólnym uczeniu się, a nie na przymusie. Jednostki edukacyjne i JST, które umożliwiają eksperymentowanie, nie tylko wdrażają zmiany, ale zapraszają do ich współtworzenia. To **fundament zarządzania partycypacyjnego**.

Przeciążenie informacyjne (infobezwładność)

Model zarządzania oparty na przejrzystości, **ograniczaniu nadmiaru**, prostocie i spójności komunikacji staje się warunkiem zdrowia cyfrowego szkoły. Modele zarządzania muszą sprzyjać cyfrowej optymalizacji i **racjonalnej dystrybucji informacji**. JST mogą wspierać szkoły i podmioty oświatowe we wdrażaniu zasad higieny cyfrowej jako standardu jakości edukacji.

Spadek poczucia sensu pracy nauczyciela

Kultura szkoły, która nie traktuje pracy nauczyciela jako misji i refleksyjnej profesji, pogłębia wypalenie zawodowe przedstawicieli tej profesji. Dyrekcja jako lider sensu (a nie wyłącznie menager zadań) odgrywa istotne znaczenie. JST mogą tę sytuację wspierać lub blokować w zależności od tego, w jaki sposób postrzegają rolę szkoły (jako instytucji usługowej czy wspólnoty?). Wyzwanie to wymaga **modelu zarządzania refleksyjnego i wspierającego**. Tylko placówki edukacyjne z kulturą sensu i misji, w których dyrektor pełni rolę lidera humanistycznego, będą w stanie utrzymać zaangażowanie kadry w warunkach zmiany cyfrowej. JST powinny promować rozwój zawodowy i uznanie roli nauczyciela jako przewodnika, a nie tylko wykonawcy.

Kryzys tożsamości szkoły

Gdy cyfryzacja podważa tradycyjne funkcje szkoły, tylko liderzy tożsamościowi (na poziomie szkół i samorządów) mogą pomóc nadać nowy sens wspólnemu byciu razem. Modele zarządzania muszą wspierać szkołę i placówki oświatowe jako wspólnoty wychowujące i kształtujące obywatelstwo, a nie tylko ślepo realizujące założenia podstawy programowej. Kultura organizacyjna powinna tworzyć przestrzeń na redefinicję istoty placówki oświatowej. **Wymaga przywództwa tożsamościowego** na poziomie szkoły i samorządu.

Osamotnienie i dezintegracja relacji

Szkoły potrzebują stylu kierowania, który promuje relacje, empatię, obecność. JST powinny inwestować nie tylko w infrastrukturę, ale i w programy wspólnototwórcze, sieciowanie szkół, kręgi refleksji. To zaś wymaga **modelu kultury relacyjnej i współobecności**. Zarządzanie, które nie traktuje relacji jako zasobu, a jedynie postrzega ją jako dodatek, powoduje erozję więzi. Jednostki edukacyjne, które inwestują w kulturę obecności i troski, przeciwdziałają samotności cyfrowej. JST **mogą to wzmacniać poprzez tworzenie wspólnotowych programów i przestrzeni relacyjnych**.

Obniżona odporność emocjonalna dzieci i młodzieży

Kultura szkoły musi uwzględniać elementy zdrowia psychicznego, uważności, edukacji emocjonalnej. JST powinny traktować zadowolenie z życia jako element polityki publicznej, a nie wyłącznie jako gest dobrej woli. Tylko zarządzanie traktujące dobrostan jako wartość strategiczną (a nie jedynie interwencyjną) zapobiegnie skutkom przeciążenia emocjonalnego. Szkoły potrzebują systemowego wsparcia (superwizji, edukacji emocjonalnej), a także dyrekcji postrzegającej emocje jako integralny element edukacji. Takie podejście wymaga **modelu zarządzania troską i wrażliwością systemową**.

Napięcia w komunikacji między nauczycielami a rodzicami

Kultura organizacyjna szkoły powinna opierać się na dialogu i granicach, a nie presji i natychmiastowości. JST mogą wspierać placówki oświatowe w budowaniu kultury zaufania społecznego (np. przez mediacje, warsztaty komunikacyjne). Transformacja cyfrowa się powinna bazować na kulturze współzarządzania relacjami, a nie dominacji jednej ze stron. Szkoła jako wspólnota wychowująca młodych ludzi potrzebuje liderów dialogu (dyrekcji i samorządów dostrzegających wartość w komunikacji empatycznej, a koncentrujących się wyłącznie na komunikacji proceduralnej). To wymaga **modelu współzarządzania relacją szkoła – rodzina**.

Brak systemowego wsparcia psychospołecznego

To wyzwanie **wymaga instytucjonalnego modelu wsparcia systemowego i międzysektorowego**. Niestety przekracza ono kompetencje samej szkoły. JST

jako jednostki zarządzające edukacją lokalnie mają decydującą rolę w budowaniu sieci specjalistów, programów profilaktyki, standardów opieki i mechanizmów finansowania. Jednak bez strukturalnego i długofalowego wsparcia (etatów psychologów, mechanizmów supervizji, programów dobrostanu) cyfryzacja oświaty stanie się źródłem kryzysów. Dlatego organy samorządowe w tym procesie transformacji cyfrowej odgrywają kluczową rolę. Mm bowiem stworzyć system, który stanie się tarczą ochronną, a nie tylko dodatkiem.

Rozmycie granic między pracą a życiem prywatnym

To ostatnie wyzwanie psychospołeczne wymaga **kultury zarządzania opartej na szacunku do rytmu pracy człowieka**. Dyrekcja szkoły, którą wspiera JST, może modelować kulturę organizacyjną (chroniącą czas wolny, wprowadzającą zasady cyfrowe i przeciwdziałającą wypaleniu). Modele liderstwa powinny promować równowagę, a nie promować ciągłej dostępności. Kultura organizacyjna oparta na respekcie dla rytmu życia, odpoczynku i granic, staje się jednym z najważniejszych wskaźników dojrzałości instytucjonalnej szkoły, przedszkoli i innych placówek oświatowych. Dyrektorzy mogą tę sytuację modelować, ale tylko wówczas, gdy sami są chronieni przez mądre modele zarządzania ze strony JST.

Podsumowanie

Celem niniejszej publikacji było wywołanie refleksji na temat tego, że psychospołeczne wyzwania cyfryzacji nie są marginesem transformacji, ale wskaźnikiem dojrzałości modeli zarządzania i kultury organizacyjnej. Tylko systemy oparte na zaufaniu, trosce, partycypacji i sprawiedliwości będą w stanie przeprowadzić rzeczywistą, nie tylko technologiczną transformację edukacji. Każde z przedstawionych psychospołecznych wyzwań cyfryzacji oświaty stawia pytanie nie tyle o to, czy wprowadza się technologię, ale jaką wspólnotę i środowisko chce się stworzyć dzięki niej. Modele zarządzania i kultury organizacyjnej (zarówno na poziomie szkoły, jak i samorządu) są zwierciadłem wartości wyznawanych przez ludzi. I takie założenie decyduje o tym, czy cyfryzacja będzie emancypacją, czy nową formą wykluczenia.

W dalszej części niniejszego opracowania zostanie zaprezentowany autorski model Wartościowego Zarządzania®, który jest odpowiedzią na kierowanie psychospołecznymi wyzwaniami z jego różnorodnymi kontekstami.

5. Identyfikacja sieci powiązań i odpowiedzialności w kontekście pożądanых kierunków zmiany w edukacji.

W procesie transformacji cyfrowej żaden uczestnik systemu oświaty nie działa w izolacji. Sukces zależy od świadomego budowania sieci współpracy, gdzie każda strona rozumie swoją rolę i wpływ na zmianę. System wzajemnych powiązań i współzależności jest podstawą do myślenia o edukacji – nie jako o sumie jednostkowych decyzji – ale jako o złożonym ekosystemie. Jeśli więc cyfryzacja ma być rzeczywiście zmianą jakościową, nie może być redukowana do technologicznych wdrożeń lub jednostkowych inicjatyw. Jest raczej procesem systemowym, który rozgrywa się w sieci wzajemnych relacji, zależności i wpływów (pomiędzy szkołą, organem prowadzącym, uczniami, rodzinami, środowiskiem lokalnym, instytucjami wsparcia, organizacjami społecznymi i rynkiem). W tej perspektywie ważne staje się rozpoznanie, jakie funkcje pełnią poszczególne osoby pracujące w danej placówce edukacyjnej (np. Kto jest wykonawcą jakiegoś zadania i kto za nie ponosi odpowiedzialność? Kto i z kim współpracuje? Kto i dla kogo jest wsparciem? Jakie są zależności między personelem placówki oświatowej? Co jest płaszczyzną sporów i kłótni? Jakie są obszary wzajemnego niezrozumienia?).

W tym aspekcie warto sobie uzmysłowić, że szkoła – choć bywa postrzegana jako jednostka autonomiczna – jest silnie osadzona w sieci kontekstów:

- JST jako organ prowadzący wpływa na priorytety rozwojowe, inwestycje, kadry;
- rodzice – jako społeczność oczekująca jakości i komunikacji;
- uczniowie – jako partnerzy zmiany i beneficjenci procesów edukacyjnych;
- instytucje wspierające – poradnie, organizacje pozarządowe, uczelnie;
- system prawny i polityczny – jako ramy funkcjonowania, ale też często bariera elastyczności.

Ta sieć powiązań wymaga świadomego zarządzania zależnościami, ale nie ograniczającej się wyłącznie do logiki odpowiedzialności jednostronnej (np. w myśl której podmiotem odpowiadającym za wszystko jest dyrektor), ale w duchu współodpowiedzialności rozproszonej. Tylko taka struktura umożliwia prawdziwe współtworzenie zmiany.

Podczas planowania strategii zarządzania procesem cyfryzacji (w tym każdą inną strategią oświatową) warto wyobrazić sobie edukację jako system naczyń połączonych, w którym każda decyzja (nawet lokalna i drobna) wpływa na inne elementy:

- sposób komunikacji dyrektora z nauczycielami rzutuje na kształt ich relacji z uczniami;
- wsparcie JST dla dyrektora kształtuje jego gotowość do podejmowania innowacji;
- otwartość szkoły na rodziców wpływa na klimat relacji w klasach i odbiór zmiany przez uczniów.

Zarządzanie w takiej sieci wymaga nie tylko umiejętności decyzyjnych, ale **kompetencji systemowego widzenia**: dostrzegania wzajemnych oddziaływań, potrzeb synchronizacji i delikatnych punktów napięcia. W obliczu takiego rozumienia systemu oświaty, warto mieć świadomość, że **współzależność stanowi fundament kultury organizacyjnej**.

Wzajemne współzależności:

- szkoła potrzebuje wsparcia ze strony samorządu (infrastruktura, programy rozwojowe);
- samorząd potrzebuje informacji zwrotnej od szkół, aby lepiej dostosowywać strategię wsparcia;
- rodzice i społeczność lokalna mogą być sojusznikami lub hamulcowymi zmian, dlatego warto ich angażować.

Warto sobie uzmysłowić, że bez świadomego zbudowania tej sieci zależności, działania na rzecz cyfryzacji mogą być niespójne, nieskuteczne lub napotykać na niepotrzebne bariery. Nowoczesna kultura organizacyjna w oświacie zarówno na poziomie szkoły, jak i JST powinna wyrastać z przekonania, że **nie ma zmiany bez relacji**. Oznacza to:

- odejście od myślenia silosowego (nieangażującego się, wyrastającego z braku zainteresowania tematem);
- rozwijanie struktur współpracy poziomej i pionowej;
- tworzenie przestrzeni do wspólnego rozpoznawania potrzeb i kierunków zmiany.

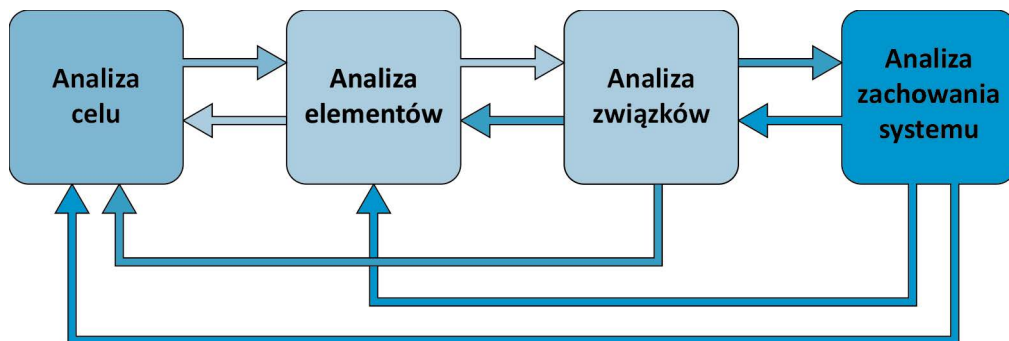
Model dobrego przywództwa w tym kontekście to **lider sieciowy**, czyli taki, który nie dominuje, ale łączy. Nie kontroluje, ale synchronizuje. Nie wyznacza kierunku samotnie,

ale go uzgadnia z innymi. Natomiast transformacja cyfrowa, jeżeli ma prowadzić do dobra wspólnego, musi być zakorzeniona **w poczuciu współodpowiedzialności**.

Odpowiedzialności poszczególnych podmiotów:

- JST – za struktury, zasoby i ramy systemowe;
- dyrekcji szkół – za klimat, kulturę i styl zarządzania;
- nauczycieli – za jakość relacji i treści dydaktyczne;
- uczniów i rodziców – za aktywne uczestnictwo i kształtowanie oczekiwań.

W procesie cyfryzacji szkoły bardzo ważną rolę odgrywa mapa powiązań i wspólna narracja zmiany (każdy z podmiotów związanych z daną jednostką edukacyjną nie tylko doskonale zna swoją rolę i funkcję, ale także rozumie perspektywę innych. Tylko wówczas jest możliwa synchronizacja działań i trwałość efektów. Kompetencje zarządzania z uwzględnieniem sieci powiązań i współzależności są warunkiem koniecznym w procesach zarządzania jakąkolwiek zmianą. Tę sytuację obrazuje ilustracja zamieszczona poniżej. Model ten jest ściśle powiązany z kompetencjami nabywanymi na kursie „Wartościowego Zarządzania”⁸⁰, którego idea i opis zostanie zaprezentowana w kolejnej części opracowania.



Rysunek 1. Etapy analizy systemowej (Za: „Myślenie systemowe w coachingu”⁸⁰).

Podsumowanie

We współczesnym świecie, w którym coraz więcej decyzji podejmuje się szybko i pod presją technologii, warto podjąć refleksję na temat ludzkiego funkcjonowania jako sieć. Czy współcześnie są w stanie dostrzec, co łączy ich z innymi ludźmi? Czy potrafią wskazać, co jest źródłem nieporozumień? Warto też pamiętać, że **zmiana systemowa**

⁸⁰ Pilipczuk K., (red.), (2013), *Myślenie systemowe w coachingu*, Warszawa: Pracownia Satysfakcji.

nie polega na tym, aby każdy człowiek robił wyłącznie to, co do niego należy. W procesie cyfryzacji istotą jest zrozumienie, że tak naprawdę liczy się to, co ludzie potrafią i chcą wykonać dla siebie wspólnie.

6. Związek między kompetencjami osób zarządzających jednostkami edukacyjnymi a przebiegiem procesu cyfryzacji.

Transformacja cyfrowa w oświacie nie uda się bez osób, które potrafią nie tylko zarządzać procesami, ale prowadzić ludzi przez zmianę z uważnością, poczuciem sensu i troską o relacje. W tym kontekście dominującą inspiracją staje się koncepcja wartościowego zarządzania w edukacji, która jest zakorzeniona w idei szkoły jako wspólnoty osób, a nie wyłącznie pojmowanej jako organizacja zadaniowa. Kurs Wartościowego Zarządzania® jest autorskim pomysłem Zofii Domaradzkiej-Grochowalskiej (autorki niniejszego rozdziału) oraz Doroty Tomaszewicz.

Kurs „Wartościowego Zarządzania”® stanowi unikatowy program rozwojowy skierowany do dyrektorów szkół i przedszkoli, liderów instytucji otoczenia szkoły oraz przedstawicieli samorządów lokalnych. Program ten powstał z myślą o osobach, które prowadzą innych przez zmianę, często w warunkach niepewności, napięcia i presji systemowej. Kurs ma strukturę procesową, której rytm odzwierciedla naturalną drogę rozwoju lidera:

- od zarządzania sobą;
- przez zarządzanie zespołem;
- aż po kształtowanie kultury całej organizacji.

Trzy poziomy kursu:

Poziom podstawowy – Zarządzanie sobą i jednostką

Rozwój samoświadomości, wartości osobistych, odporności psychicznej, zarządzania własną energią i odpowiedzialnością.

Poziom zaawansowany – Zarządzanie zespołem

Budowanie zespołu bazując na zaufaniu, współpracy i komunikacji. Ukierunkowanie się na pracę z dynamiką grupy, odpowiedzialnością rozproszoną, motywacją wewnętrzną.

Poziom master – Zarządzanie organizacją jako całością

Tworzenie kultury organizacyjnej opartej na wartościach, zarządzanie w zmianie, kształtowanie wizji i tożsamości instytucji edukacyjnej.



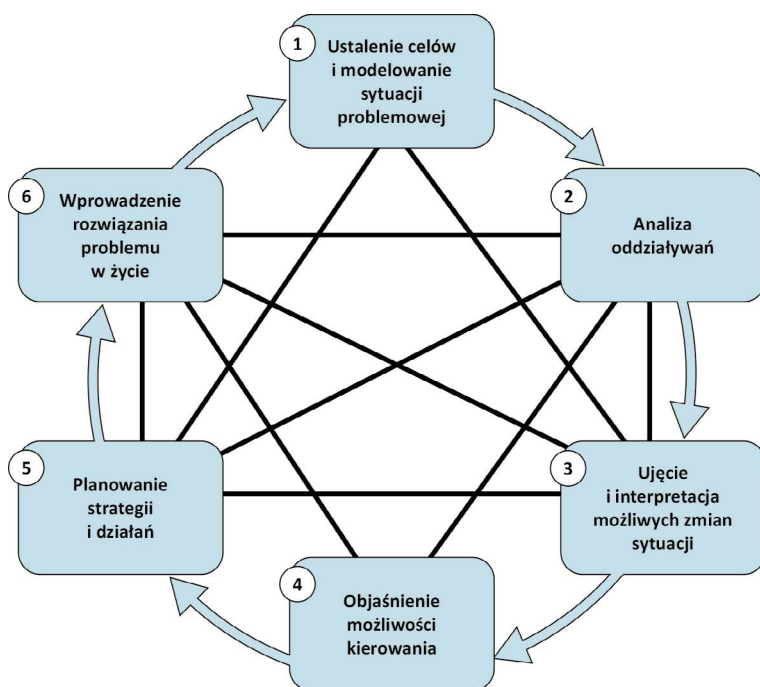
Rysunek 2. Schemat kursu Wartościowego Zarządzania® wraz z logotypem obrazującym przesłanie kursu.

Kurs „Wartościowego Zarządzania®” proponuje nowy sposób myślenia o przywództwie w oświacie. Szkolenie to zachęca liderów szkół, aby – zamiast skupiać się na narzędziach i procedurach – w praktyce doskonalić nieoczywiste, ale konieczne kompetencje zarządcze. One bowiem skłonią do:

- odkrywania i nazywania osobistego systemu wartości;
- tworzenia kultury organizacyjnej opartej na zaufaniu, szacunku i odpowiedzialności;
- budowania zespołów traktujących relacje międzyludzkie z efektami swojej pracy;
- prowadzenia zespołu z poziomu sensu a nie kontroli.

Zarządzający szkołą przestaje być jedynie realizatorem polityk oświatowych, a staje się liderem integralnym (łączącym wewnętrzną spójność z odwagą bycia

w relacji). Kurs ma charakter coachingowo-mentoringowy – uczestnicy są nie tylko odbiorcami treści, ale aktywnymi współtwórcami procesu. Pracują na realnych dylematach, prowadzą refleksję nad sobą jako liderem i uczą się wspólnotowego podejścia do zmiany. W centrum tej koncepcji znajduje się człowiek w relacji a nie system (nie procedura, ale też nie narzędzie). To szkolenie, które uczy nie tylko zarządzania, ale przede wszystkim prowadzenia innych z miejsca sensu, uważności i odwagi. Uczestnicy kursu kończą go z kompetencjami osadzonymi w metodyce myślenia sieciowego, które jest typowe dla oświaty.



Rysunek 3. Metodyka myślenia sieciowego (Za: „Myślenie systemowe w coachingu”⁸¹).

Dlaczego warto inwestować w kompetencje liderów zmiany?

Liderzy oświaty zarządzający procesem cyfryzacji stoją obecnie przed wyjątkowym wyzwaniem. Oto bowiem mają prowadzić ludzi przez zmianę, która nie ma końca, a jej kierunek często wyznaczają nie oni sami, lecz okoliczności zewnętrzne. W takim kontekście kompetencje twarde nie wystarczają. Potrzebne są konkretne kompetencje.

⁸¹ Ibidem.

Przedstawienie inspiracji w postaci kursu „Wartościowego Zarządzania®” podyktowana jest tym, że to kompleksowe szkolenie obejmuje zbiór kluczowych obszarów kompetencyjnych, które – zdaniem autorki niniejszej publikacji – powinny być przedmiotem rozwoju osób zarządzających zmianą w oświacie. Są to nimi następujące umiejętności:

Kompetencje przywództwa wartościowego

- umiejętność zarządzania z poziomu osobistego systemu wartości;
- spójność wewnętrzna i odwaga do podejmowania decyzji zgodnych z etosem edukacyjnym;
- autentyczność i budowanie zaufania w relacjach.

Kompetencje zarządzania zmianą

- rozumienie dynamiki procesów zmiany (w tym oporu, faz przejścia, lęku i niepewności);
- projektowanie i wdrażanie procesów zmiany krok po kroku;
- komunikowanie zmiany z empatią i klarownością.

Kompetencje relacyjne i dialogowe

- umiejętność prowadzenia trudnych rozmów;
- słuchanie empatyczne i budowanie porozumienia mimo różnic;
- rozwijanie zespołów opartych na współodpowiedzialności i zaufaniu.

Kompetencje zarządzania sobą

- odporność psychiczna i emocjonalna;
- umiejętność regulowania stresu i zachowywania klarowności myślenia w sytuacjach napięcia;
- dbanie o równowagę między rolą zawodową a życiem osobistym.

Kompetencje zarządzania zespołem

- budowanie zespołów różnorodnych i zintegrowanych wokół celu;
- tworzenie kultury współpracy i uczenia się;
- delegowanie, motywowanie, rozwiązywanie konfliktów.

Kompetencje systemowego widzenia i analizy

- postrzeganie szkoły jako systemu naczyń połączonych;
- identyfikacja zależności, przepływów i punktów napięcia;
- tworzenie sieci współpracy poziomej i międzysektorowej (z JST, instytucjami wspierającymi, rodzicami).

Kompetencje cyfrowe w zarządzaniu

- krytyczne podejście do narzędzi technologicznych (nie tylko znajomość, ale świadome użycie);
- projektowanie rozwiązań cyfrowych z myślą o człowieku (a nie tylko ich funkcji);
- wdrażanie zasad higieny cyfrowej w pracy własnej i zespołu.

Kompetencje refleksyjne i strategiczne

- umiejętność zatrzymania się i prowadzenia autorefleksji;
- planowanie długofalowe w warunkach zmienności;
- ewaluacja jakości zmiany (określenie, w jakim stopniu cyfryzacja jest tylko wdrożeniem, a w jakim transformacją sensu).

Podsumowanie

Transformacja cyfrowa w edukacji może być jedynie modernizacją sprzętu albo stanie się okazją do głębokiej przemiany kultury zarządzania i przywództwa. Od ludzi, którzy tę zmianę prowadzą, zależy wybór odpowiedniej drogi. Trzeba pamiętać o tym, że szkoła lub inna jednostka oświatowa, która działa dla wartości, potrafi też zmieniać się w zgodzie z wartościami.

7. Związek między zjawiskiem higieny cyfrowej i dojrzałości cyfrowej.

Tytułowe zagadnienia tego rozdziału wskazują, że w świecie technologii nie wystarczy tylko umieć obsługiwać urządzenia. Potrzebna jest mądrość w ich wykorzystywaniu – dla własnego dobra i rozwoju innych. Zagadnienia higieny i dojrzałości cyfrowej pojawiały się już wcześniej (szczególnie w kontekście przeciążenia informacyjnego, rozmycia granic i napięć w relacjach), ale – zdaniem Zofia Domaradzka-Grochowalska

– warto pochylić się nad tytułowym zagadnieniem. I potraktować je nie jako część problemu, lecz jako osobny, strategiczny obszar kompetencji i kultury organizacyjnej szkoły.

Transformacja cyfrowa oświaty zazwyczaj kojarzy się z nowymi narzędziami, metodami pracy czy zarządzaniem zmianą. Jednak równie istotne, choć często niedostrzegane, są kwestie związane z higieną i dojrzałością cyfrową wszystkich uczestników procesu edukacyjnego. Świadome podejście do technologii nie polega bowiem wyłącznie na jej wykorzystaniu w pracy i nauce, ale także na umiejętnym zarządzaniu jej wpływem na życie psychiczne, emocjonalne i społeczne człowieka. A współcześnie cyfryzacja jest już zjawiskiem powszechnym. Wpływa na rytm pracy, relacje, koncentrację, zdrowie psychiczne, styl uczenia się, a nawet na sposób, w jaki definiuje się obecność, uważność czy sens pracy. W takim kontekście higiena i dojrzałość cyfrowa przestają być umiejętnościami miękkimi, ponieważ stają się centralnymi kategoriami zarządzania jakością życia w szkole, przedszkolu czy innej placówce edukacyjnej.

Czym jest dojrzałość cyfrowa?

Dojrzałość cyfrowa wyraża się nie tylko w biegłości technologicznej, ale łączy w sobie wiele innych umiejętności:

- krytyczne korzystanie z narzędzi (a nie podlegania im);
- rozumienie ich wpływu na psychikę i relacje;
- integrowanie technologii z misją szkoły, a nie zastępowania nią sensu;
- podejmowanie świadomych decyzji o wdrożeniach, zgodnie z wartościami organizacji.

Dojrzałość cyfrowa to kompetencja systemowa, która swoim zasięgiem obejmuje dzieci i młodzież, nauczycieli, dyrekcję, JST, stając się jednocześnie gwarantem powodzenia każdej transformacji.

Czym jest higiena cyfrowa i dlaczego ma znaczenie?

Higiena cyfrowa to połączenie świadomych nawyków i działań, które pomagają zachować zdrową równowagę między światem online i offline. Obejmuje m.in.:

- racjonalne zarządzanie czasem spędzanym przed ekranami;
- umiejętność ochrony prywatności i bezpieczeństwa w sieci;
- krytyczną ocenę informacji napływających z internetu;

- świadome korzystanie z technologii w sposób wspierający rozwój, a nie uzależniający.

Wybrane wyzwania psychospołeczne, które przywołano we wcześniejszej części niniejszego opracowania, są powiązane bezpośrednio lub pośrednio z higieną i dojrzałością cyfrową. Odzwierciedla to zestawienie znajdujące się poniżej.

Wyzwania psychospołeczne	Związek z higieną i dojrzałością cyfrową
Przeciążenie informacyjne (infobezwładność)	Higiena cyfrowa pozwala selekcjonować, filtrować i porządkować informacje.
Rozmycie granic między pracą a życiem prywatnym	Ustalanie ram czasowych i rytuałów cyfrowych przywraca granice.
Spadek sensu pracy nauczyciela	Świadome użycie technologii w zgodzie z misją szkoły sprzyja przywracaniu sensu działania.
Napięcia w relacjach z rodzicami	Dojrzałość cyfrowa zespołu pozwala ustalać reguły komunikacji i zapobiega eskalacjom.
Obniżona odporność emocjonalna uczniów	Praktyki cyfrowej równowagi wspierają dobrostan i zdolność do skupienia, odpoczynku, relacji.

Zdaniem dr Macieja Dębskiego⁸² higiena cyfrowa jest dziś kompetencją społeczną. Definiuje ją zestaw świadomych praktyk, które pomagają utrzymać równowagę między życiem online a offline. Badacz podkreśla, że nie chodzi o całkowite wyeliminowanie technologii, lecz o umiejętne i świadome jej wykorzystywanie, które nie zakłóca codziennego funkcjonowania i relacji międzyludzkich. W swoich badaniach dr Dębski zwraca uwagę na zjawisko fonoholizmu, czyli uzależnienia od korzystania ze smartfona. Przeprowadzone przez jego fundację badania wykazały, że 2–3 proc. młodzieży wykazuje symptomy uzależnienia (np. ciągła potrzeba bycia online, lęk przed utratą dostępu do telefonu czy zaniedbywanie obowiązków na rzecz korzystania z urządzeń mobilnych). Dr Dębski podkreśla znaczenie edukacji w zakresie higieny cyfrowej, zarówno w rodzinie, jak i w systemie edukacyjnym. Zachęca rodziców do ustalania jasnych zasad korzystania z technologii w domu oraz do bycia wzorem w odpowiedzialnym korzystaniu z urządzeń elektronicznych. W edukacji

⁸² Dr Maciej Dębski – socjolog i założyciel Fundacji „Dbam o Mój Z@sięg”; jest jednym z głównych ekspertów w Polsce w dziedzinie higieny cyfrowej i fonoholizmu. Jego prace koncentrują się na badaniu wpływu technologii na życie społeczne (zwłaszcza w kontekście młodzieży i rodzin), zob. <https://dbamomojzasieg.pl/> [dostęp, online dn. 2.09.2025].

szkolnej zaleca wprowadzenie programów uczących dzieci i młodzież świadomego i bezpiecznego korzystania z technologii.

Z raportu „Młode Głowy. Otwarcie o zdrowiu psychicznym”⁸³, którego współautorem jest dr Maciej Dębski, wynika, że:

- 62,4 proc. uczniów czuje się przytłoczonych ilością informacji i presją bycia cały czas online;
- 45 proc. badanych nastolatków ma trudność z odróżnieniem, kiedy korzystają z technologii dla relaksu, a kiedy z przymusu;
- co trzecie dziecko deklaruje problemy z koncentracją, których powodem jest nadmierne korzystanie z urządzeń ekranowych;
- aż 70 proc. uczniów nie rozmawia z nikim o swoim cyfrowym samopoczuciu i nie mają świadomości, że to, czego doświadczają, może mieć związek z przebudzcowaniem.

Te dane jednoznacznie wskazują, że brak higieny cyfrowej staje się realnym zagrożeniem dla dobrostanu psychicznego uczniów, a także znacząco wpływa na ich relacje, samoocenę i zdolność do uczenia się. Wprowadzenie do szkół zasad higieny cyfrowej oraz rozwijanie dojrzałości cyfrowej (pojmowanej nie tylko jako zestaw umiejętności technicznych, ale także jako świadomość wpływu technologii na życie wewnętrzne człowieka), staje się obecnie zatem koniecznością wychowawczą i profilaktyczną.

Rekomendacje dla szkół, przedszkoli, placówek oświatowych i JST:

- audyt dojrzałości cyfrowej szkoły – pojmowanej nie jako ocena techniczna, ale analiza wpływu technologii na życie szkolne;
- kultura cyfrowej odpowiedzialności – określenie wartości i zasad korzystania z technologii jako część polityki szkoły;
- edukacja cyfrowa jako edukacja etyczna i relacyjna – nie tylko umiejętność, ale świadomość i refleksyjność;
- włączenie higieny cyfrowej do programów wychowawczych i rozwoju zawodowego – nie jako element opcjonalny, ale standard.

Podsumowanie

Być może prawdziwa transformacja cyfrowa nie polega na wprowadzeniu technologii, lecz na tym, że trzeba się nauczyć nią zarządzać w sposób odpowiedzialny, mądry

⁸³ „Młode Głowy”, op. cit.

i wspierający człowieczeństwo. A higiena cyfrowa i dojrzałość cyfrowa są nie tyle dodatkiem do edukacji, ale nową kompetencją cywilizacyjną, od której zależy jakość życia szkolnego. Jednak faktyczne rozumienie funkcji i roli tych zagadnień jest kwestią indywidualną każdego człowieka.

8. Rola profilaktyki i psychoedukacji w świecie rzeczywistym i wirtualnym.

Współczesna szkoła nie może już oddzielać wychowania i profilaktyki od rzeczywistości cyfrowej. Młodzi ludzie żyją dziś jednocześnie w dwóch światach (realnym i wirtualnym), doświadczając w nich podobnych emocji, relacji i niebezpieczeństw. Dlatego profilaktyka, która pomija kontekst cyfrowy, traci kontakt z rzeczywistością uczniów, a psychoedukacja skupiona wyłącznie na offline'owych schematach nie dociera do tych obszarów życia, które młodzież uznaje za najważniejsze.

Dlaczego kwestie zdrowia psychicznego młodych ludzi jest tak istotna?

Z raportu „Młode Głowy. Otwarcie o zdrowiu psychicznym” wynika, że:

- co drugi nastolatek doświadcza przemocy słownej lub emocjonalnej w internecie;
- niemal 60 proc. badanych przyznało, że spotkało się z hejtem lub mową nienawiści online;
- 33 proc. młodych osób czuje się gorszymi, kiedy w mediach społecznościowych porównują się do innych;
- 75 proc. młodzieży deklaruje, że nikt z dorosłych nigdy z nimi nie rozmawiał o tym, jak poradzić sobie z hejtem w sieci.

Za tym liczbami kryją się prawdziwe i konkretne historie cierpienia, niezrozumienia i osamotnienia. One wszystkie, choć rozgrywają się w rzeczywistości cyfrowej, to jednak w swoich skutkach i objawach są na wskroś realne (np. przejawiają się obniżoną samooceną, lękiem społecznym, poczuciem wstydu i samotnością, a nawet myślami samobójczymi). W celu wspierania zdrowej i bezpiecznej obecności młodych ludzi w świecie cyfrowym należy podjąć niezbędne działania profilaktyczne

i psychoedukacyjne. Jednak dojrzała w swej mądrości profilaktyka jest czymś więcej niż zakazem. Wielu dorosłych, zarówno w rodzinach, jak i w szkołach reaguje na problemy cyfrowe poprzez zakazy, ograniczenia, dyscyplinę technologiczną. Tymczasem młodzież potrzebuje bezpiecznej przestrzeni rozmowy, zrozumienia i wsparcia emocjonalnego. Profilaktyka nie może opierać się na kontroli, bowiem swoją siłę powinna opierać się na zaufaniu i edukacji.

Dlatego współczesna psychoedukacja musi:

- łączyć świat realny i wirtualny jako integralne środowisko życia dziecka;
- uczyć rozpoznawania emocji i granic w relacjach cyfrowych;
- pomagać zrozumieć działającą istotę funkcjonowania mechanizmów porównań, lęku przed wykluczeniem, presji lajków;
- uczyć reagowania na hejt, ale też budować odporność na jego wpływ,
- pokazywać, że technologia może służyć do budowania relacji, a nie ich niszczenia.

Zdaniem dr Macieja Dębskiego zatracenie się młodych ludzi w świecie wirtualnym wynika z braku alternatywy w świecie rzeczywistym. Badacz zwraca uwagę na istotną rolę rodziców. Problematyczne jest jednak to, że oni sami zazwyczaj nie potrafią zarządzać własną higieną cyfrową. Natomiast środowisko szkolne ma potencjał, aby być stać się miejscem przestrzenią mądrej i empatycznej profilaktyki.

Jest to możliwe, gdy:

- nauczyciele są przygotowani do prowadzenia rozmów o świecie cyfrowym bez oceniania;
- profilaktyka jest zintegrowana z codzienną praktyką wychowawczą;
- tematy dotyczące internetu, hejtu, samooceny cyfrowej są obecne na lekcjach wychowawczych;
- uczniowie są przeświadczeni, że bez wstydu mogą opowiadać o swoich doświadczeniach.

Psychoedukacja nie powinna być jednorazowym warsztatem o hejcie, ale ciągłym procesem wzmacniania kompetencji emocjonalnych i cyfrowych. Dlatego niezmiernie potrzebna jest edukacja, która nie tylko nauczy młodych ludzi, jak w środowisku cyfrowym mają się chronić, ale ponadto wskaże im, w jaki sposób być obecnym w sieci, a jednocześnie zachować w sobie czujność i odporność wobec zagrożeń.

W czasach obecnych jednym z najważniejszych zadań wychowawczych i cywilizacyjnych, jakie stoją przed edukacją, rodziną i społeczeństwem, jest świadome

uczenie młodych ludzi życia w dwóch światach (realnym i wirtualnym). I nie chodzi tu tylko o ochronę czy profilaktykę, ale o formowanie tożsamości, relacyjności, granic i wolności w świecie, który nie zna już podziału na online i offline. Dlaczego tak się stało? Te oba światy są prawdziwe.

Nie ma już powrotu do świata sprzed internetu. Dla młodych ludzi świat cyfrowy nie jest alternatywą dla rzeczywistości, jest jej częścią. Tam zawierają przyjaźnie, doświadczają odrzucenia, rozwijają tożsamość, szukają sensu i przynależności. Uczenie świadomego życia w tych dwóch przestrzeniach wymaga uznania, że obie są realne emocjonalnie i społecznie. Świadomość cyfrowa to jednak nie techniczna biegłość. To umiejętność:

- rozpoznawania tego, co online człowieka wzmacnia, a co osłabia;
- stawiania granic i wybierania intencji w korzystaniu z mediów;
- krytycznego myślenia wobec treści i ról otrzymywanych w sieci;
- zachowania ciągłości tożsamości w obu światach, aby nie kreować siebie na kogoś innego w każdej z przestrzeni.

W czasach obecnych wiele uwagi poświęca się edukowaniu dzieci i młodzieży w zakresie reagowania na tzw. zły dotyk, niezdrowe relacje czy przemoc w realnym świecie. Warto się jednak zastanowić, czy młodzi ludzie umieją być tak asertywni w świecie wirtualnym. Świadome życie obejmuje także:

- umiejętność wychodzenia z internetu;
- dbanie o przestrzeń wolną od ekranów;
- przerwy cyfrowe jako rytuały regeneracji;
- akceptacja, że nie muszą być ciągle dostępni.

Dojrzałość cyfrowa to nie tylko samoświadomość, ale też świadomość wpływu na innych. Przejawem dojrzałego funkcjonowania zarówno w przestrzeni realnej, jak i wirtualnej jest uczenie dzieci oraz młodzieży odpowiedzialności za słowa zamieszczane w komentarzach, treści graficzne oraz relacje. To uczenie się obecności, troski, empatii także w komunikacji cyfrowej). W takim podejściu ujawnia się jeszcze jedna istotna kwestia. Rodzice i nauczyciele mają obowiązek prowadzić dziecko w taki sposób, aby ono – gdy jest poza siecią (offline), nie miało poczucia, że wirtualny świat stanowi dla niego jedyną alternatywę.

Dorośli często sami żyją niespójnie, prosząc, aby młody człowiek odłożył telefon, a sami nie potrafią się oderwać od aparatu nawet na chwilę. Dlatego świadome uczenie życia

w dwóch światach wymaga odwagi od samych dorosłych, aby siebie wychowywać na nowo. Holistyczne podejście do kwestii cyfryzacji pokazuje, że nie jest temat, który można zrealizować przez jedną jednostkę lekcyjną jako godzina wychowawcza. To sposób bycia z młodymi w ich rzeczywistości, z otwartością, zaciekawieniem i gotowością do towarzyszenia.

Podsumowanie

Świat cyfrowy nie jest zagrożeniem sam w sobie. Problem pojawia się wtedy, gdy – znając złożoność internetu, jego dynamikę, presję i złożoność – pozostawiamy dzieci i młodzież samym sobie. Mądra profilaktyka i psychoedukacja mogą być pomostem między światem ucznia a światem dorosłych, między rzeczywistością online a offline, między problemem a wspólnotą wsparcia. Jeśli ten mostu nie zostanie zbudowany, to młodzi ludzie zatracą się nim samotnie.

9. Związek między kompetencjami osób zarządzających w oświacie a kształtowaniem postaw u dzieci oraz młodzieży.

Właściwie prowadzona profilaktyka i psychoedukacja – szczególnie w dzisiejszych czasach życia na styku świata realnego i cyfrowego – ma zadanie o wiele głębsze niż tylko zapobieganie zagrożeniom. Jej sens sięga formowania człowieka świadomego siebie, swoich emocji, granic i relacji, zarówno offline, jak i online.

Zadania profilaktyki i psychoedukacji są następujące:

Nie tylko chronić, ale uzdrawiać.

Nie wystarczy uczyć, jak unikać zagrożeń. Mądra profilaktyka ma dotyczyć źródeł cierpienia, braku więzi, samotności, lęku. Ma być przestrzenią wzmacniania odporności psychicznej i odzyskiwania poczucia sensu.

Nie tylko edukować, ale prowadzić do refleksji.

Psychoedukacja nie jest przekazywaniem wiedzy. Jest budowaniem świadomości siebie i świata, pozwalając młodym ludziom nazywać to, co czują, czego doświadczają, czego potrzebują. A nade wszystko czuć, że nie są w tym sami.

Nie tylko ostrzegać, ale dawać alternatywę.

Jeżeli kategoriycznie występuje się przeciw hejtowi, uzależnieniu, przemocy, to trzeba umieć wskazać, jakie są wartości pozytywne (np. relacja, zaufanie, odpoczynek, wspólnota). Według założeń mądrej profilaktyki życie nie musi być ekstremalne, aby było wartościowe.

Nie tylko działać wobec uczniów, ale z nimi.

To nie jest jednostronny przekaz dorosłych, ale tworzenie przestrzeni wspólnego poznawania, dzielenia się, dialogu, w którym młodzi są nie odbiorcami, ale uczestnikami. Ich doświadczenia zaś stają się źródłem wiedzy.

Nie tylko mówić o świecie realnym, ale i o cyfrowym – jako jednym świecie.

Mądra profilaktyka nie udaje, że internet to tylko niegroźny dodatek. Ona włącza uwzględnia doświadczenia online ze sferą życia psychicznego i społecznego młodego człowieka. Takie działanie jest doskonałą lekcją funkcjonowania w obu przestrzeniach (online i offline).

Nie tylko interweniować, ale modelować.

Każda relacja dorosłego z młodym człowiekiem, każda rozmowa czy gest mogą mieć charakter profilaktyczny. Przebywanie rodziców czy nauczycieli z dziećmi i młodzieżą uczy ich funkcjonowania w grupie i poznania samych siebie.

Kurs Wartościowej Profilaktyki i Psychoedukacji© nie jest jedynie zbiorem narzędzi, ale przestrzenią kształtowania uważności, dojrzałości i etycznego towarzyszenia młodym ludziom.



Rysunek 4. Logotyp Kursu Wartościowej Profilaktyki i Psychoedukacji® obrazujący przesłanie idei kursu.

„Wartościowa Profilaktyka i Psychoedukacja®” to kurs kompetencyjny dedykowany wychowawcom klas, pedagogom, psychologom szkolnym oraz innym specjalistom, którzy na co dzień wspierają dzieci i młodzież w ich rozwoju emocjonalnym, społecznym i relacyjnym. Kurs powstał także z myślą o tych, którzy chcą prowadzić działania wychowawcze i profilaktyczne w sposób świadomy, oparty na wartościach i realnych potrzebach zespołów uczniowskich.

Celem kursu jest:

- wzmacnianie roli wychowawczej i wspierającej specjalistów szkolnych;
- rozwijanie kompetencji wychowawczych w kontekście dobrostanu i zdrowia psychicznego dzieci i młodzieży;
- budowanie wartościowych zespołów klasowych jako środowisk relacyjnych, bezpiecznych i wspólnotowych;
- zwiększenie skuteczności oddziaływań psychoedukacyjnych i profilaktycznych poprzez lepsze zrozumienie dynamiki grupy.

Jednym z najważniejszych elementów kursu jest praca z narzędziem EduPre© – autorską metodą profilowania zespołów uczniowskich, która pozwala:

- przeprowadzić diagnozę klimatu klasy i jej potrzeb psychospołecznych;
- analizować uzyskane wyniki w sposób pogłębiony i zrozumiały;
- zaprojektować adekwatną i wartościową ścieżkę wsparcia (miarę odpowiadającą potrzebom konkretnego zespołu).

Jaki jest założony efekt kursu?

Specjalista kończący ten kurs nie tylko lepiej rozumie młodych ludzi, z którymi pracuje, ale także potrafi działać w sposób zintegrowany, uważny i skuteczny, wzmacniając zarówno jednostki, jak i społeczności klasowe. To profilaktyka z poziomu sensu, relacji i odpowiedzialności, a nie tylko procedur i kampanii. Jest tak dlatego, że szkolenie „Wartościowa profilaktyka i psychoedukacja®” jest sztuką towarzyszenia z uważnością.

Wychowanie nie zaczyna się od metod. Zaczyna się od obecności.

Nie od razu widać, że w klasie, która wydaje się trudna do prowadzenia, kryje się niewypowiedziane napięcie. Bardzo często jest tak, że za nadmierną pewnością jednego ucznia stoi strach przed byciem niezauważonym. Często cisza niektórych to nie przejaw obojętności, tylko zmęczenie pozą ciągłego byciem silnym. Wartościowa profilaktyka i psychoedukacja nie szukają szybkich rozwiązań. One najpierw słuchają, pytają, zatrzymują się, zauważają drugą osobę. W ten sposób tworzy się przestrzeń wspólnoty. Działania profilaktyczne nie są doraźne, ale stanowią proces towarzyszenia uczniom w ich dojrzewaniu psychicznym, społecznym i emocjonalnym — z uważnością obserwując, co młodzi ludzie przeżywają, w co wierzą, co ich buduje, a co rani. To postawa, która wzmacnia zamiast ostrzegać. Przez bardzo długi czas profilaktykę postrzegano w kategoriach zakazu, prewencji, ochrony przed zagrożeniem. Tymczasem właściwie rozumiane podejście działa wówczas, gdy dziecko czuje się widziane i ważne (zanim jeszcze wydarzy się kryzys). Dlatego komunikację z uczniami warto zacząć nie od zakazów, ale podkreślenia wyjątkowości dziecka.

Wartościowa profilaktyka uznaje, że uczniowie nie potrzebują ochrony przed światem – oczekują wsparcia w odnalezieniu w nim swojego miejsca i siły. Psychoedukacja w kursie jest prezentowana jako droga a nie instrukcja. W tym rozumieniu nie jest wykładem o emocjach, ale wspólnym ich nazywaniem. Profilaktyka zatem to proces, który uczy:

- jak przeżywać frustrację bez niszczenia siebie i innych;
- jak mówić o tym, co trudne, w sposób, który nie oddala;
- jak współistnieć w klasie, gdzie każdy wnosi inną wrażliwość i granice.

Kurs „Wartościowa Profilaktyka i Psychoedukacja®” nie jest lekcją o hejcie, to proces, w którym młodzi przez cały czas doświadczają obecności dorosłego (przewodnika a nie kontrolera). Program ten nie oferuje gotowych odpowiedzi, ale uczy stawiania mądrych pytań, nowatorskich narzędzi i jest sposobem na bycie z drugim człowiekiem.

Kurs rozwija się w odniesieniu do dwóch kluczowych wymiarów funkcjonowania uczniów: **relacyjności i sprawczości**. To właśnie w tych obszarach najczęściej dochodzi do wyzwań, napięć, niezrozumienia.

- Czy uczniowie czują, że mogą być sobą w relacjach?
- Czy potrafią budować więzi bez lęku przed oceną?
- Czy wierzą, że mają wpływ na otaczający świat?
- Czy postrzegają siebie jako ludzi skutecznych czy jako wycofanych?

Autorskie narzędzie EduPre© nie ocenia, ono pokazuje właściwy sposób postępowania dla nauczyciela. Uczy go, aby odbierać klasę jako żywy organizm, który można wspierać z czułością, ale i z profesjonalizmem.

„Wartościowa Profilaktyka i Psychoedukacja®” to zaproszenie, aby w uczniu najpierw zobaczyć człowieka, a potem dostrzec go też w nauczycielu, pedagogu, wychowawcy. Program kursu przypomina drogę, w której specjalista sam wzrasta i dzięki temu może towarzyszyć innym. Nie tylko wie, co robi, ale przede wszystkim ma odwagę być z młodymi ludźmi (także wtedy, gdy sami jeszcze nie wiedzą, czego potrzebują). I to właśnie ta obecność (uważna, pokorna, mądra) staje się największą profilaktyką, jakiej można dziś udzielić młodym ludziom.

10. Wybrane metody i narzędzia wspierające proces cyfryzacji.

Transformacja cyfrowa w oświacie nie może być skuteczna bez odpowiedniego zarządzania procesem zmiany i bez świadomego kształtowania kultury organizacyjnej, zarówno w JST, jak i w szkołach.

Modele zarządzania zmianą mogą pomóc uporządkować i ustrukturyzować proces transformacji cyfrowej.

Przy tej okazji warto też zaznaczyć, że dla ORE⁸⁴, napisano bardzo wiele publikacji na temat zarządzania zmianą. Poniżej więc zamieszczono najbardziej popularne – zdaniem autorki niniejszego materiału – publikacje o tej tematyce:

- **Model Kurta Lewina** (Rozmrożenie – Zmiana – Zamrożenie) – zmiana wymaga zakwestionowania dotychczasowych sposobów działania, wprowadzenia nowych praktyk i ich utrwalenia.
- **Model Johna Kottera** (8 kroków do zmiany) – akcentuje znaczenie budowania poczucia pilności, tworzenia koalicji na rzecz zmiany, komunikacji wizji oraz celebrowania małych sukcesów.
- **Model Awareness, Desire, Knowledge, Ability, Reinforcement (dalej ADKAR)** – koncentruje się na indywidualnym przechodzeniu przez zmianę poprzez budowanie świadomości, chęci, wiedzy, umiejętności i utrwalania nowego sposobu działania.

W dalszej części tego rozdziału rozważania skoncentrują się na obrazowaniu drogi zmiany na poziomie etapów zarządzania. Nie wystarczy jednak wiedzieć, dokąd zmierza się, trzeba też wiedzieć, jak tam dojść. Skuteczna cyfryzacja wymaga zatem metodycznego podejścia i odpowiedniego wsparcia na każdym etapie. Proces transformacji cyfrowej w oświacie, aby był skuteczny i trwały, wymaga zastosowania odpowiednich metod i narzędzi wsparcia dostosowanych do każdego etapu zmiany.

Poniżej zamieszczono wybrane metody i narzędzia, które mogą wspierać szkoły i samorządy w skutecznej realizacji transformacji.

Etap 1: Diagnoza potrzeb i analiza gotowości

Pierwszym krokiem jest rzetelne rozpoznanie miejsca początkowego.

Metody i narzędzia:

- **Audyt cyfrowy szkoły** – analiza infrastruktury technologicznej, poziomu kompetencji cyfrowych kadry oraz aktualnych praktyk edukacyjnych.
- **Ankiety i wywiady z nauczycielami, uczniami i rodzicami** – badanie ich oczekiwań, potrzeb i obaw związanych z cyfryzacją.

⁸⁴ Domaradzka-Grochowalska Z., (2021), „Moduł zarządzania kryzysowego. Zarządzanie kryzysowe. Pakiet szkoleniowy dla dyrektorów szkół”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=31536> [dostęp, online dn. 2.09.2025]. W tej publikacji autorka obszernie scharakteryzowała zagadnienie zarządzania zmianą; Domaradzka-Grochowalska Z., (2021), „Moduł zarządzania kryzysowego. Zarządzanie kryzysowe. Pakiet szkoleniowy dla kadry JTS”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=34654> [dostęp, online dn. 2.09.2025].

- **Mapa gotowości cyfrowej** – narzędzie pomagające określić etap zaawansowania cyfrowego placówka.

Etap 2: Planowanie zmiany

Na podstawie diagnozy przygotowuje się strategię działania.

Metody i narzędzia:

- **Warsztaty strategiczne** – wspólne wypracowanie wizji cyfrowej szkoły oraz priorytetów działań.
- **Model SMART** (cele Specyficzne, Mierzalne, Osiągalne, Realistyczne, Terminowe) – do formułowania celów projektu transformacji.
- **Plany szkoleń** – systematyczne programy rozwoju kompetencji cyfrowych nauczycieli i kadry zarządzającej.

Etap 3: Wdrażanie działań

Faza praktycznej realizacji planu, która wymaga zarówno determinacji, jak i elastyczności.

Metody i narzędzia:

- **Pilotażowe wdrożenia** – rozpoczęcie zmian od wybranych klas, nauczycieli lub obszarów tematycznych, aby na tej podstawie wyciągać wnioski przed szerszą implementacją.
- **Mentoring i coaching** – wsparcie indywidualne dla nauczycieli w adaptacji nowych technologii i metod pracy.
- **Platformy współpracy online** (np. Teams, Google Workspace) – jako narzędzia do komunikacji, planowania i realizacji projektów edukacyjnych.

Etap 4: Monitorowanie i ewaluacja

Stałe badanie, jak przebiega proces zmiany i w jaki sposób można go udoskonalić.

Metody i narzędzia:

- **Krótkie ankiety cykliczne** – zbieranie informacji zwrotnych od uczniów i nauczycieli na temat wykorzystania technologii w codziennej pracy.
- **Spotkania refleksyjne** – przestrzeń do dzielenia się doświadczeniami, sukcesami i trudnościami.

- **Analiza danych edukacyjnych** – np. poprzez wykorzystanie danych o aktywności uczniów na platformach cyfrowych do optymalizacji procesu nauczania.

Etap 5: Utrwalanie zmiany i rozwój

Transformacja cyfrowa nie kończy się wdrożeniem technologii, wymaga ciągłego doskonalenia.

Metody i narzędzia:

- **Programy ambasadorów cyfrowych** – wyłanianie nauczycieli-liderów, którzy wspierają kolegów w dalszym rozwoju kompetencji.
- **Przykłady dobrych praktyk** – regularne dzielenie się sukcesami i inspirującymi rozwiązaniami w ramach rady pedagogicznej lub sieci szkół.
- **Aktualizacja strategii cyfrowej** – dostosowywanie planów rozwoju do zmieniających się technologii i potrzeb społeczności szkolnej.

Poniżej, mając na względzie fakt, że publikacja tego materiału ma być wsparciem dla uczestników projektu „Cyfrowy rozwój oświaty w JST – szkolenia i doradztwo dla kadry JST” (realizowanego przez ORE), zamieszczono opracowanie badania poziomu gotowości organizacji na zmiany. Taka analiza pozwoli osobom uczestniczącym w projekcie zweryfikować etap gotowości na wdrożenia zaplanowanych w HDR aktywności. Rzetelna i uczciwa weryfikacja poszczególnych stwierdzeń zawartych w kwestionariuszu pozwoli albo podjąć adekwatne kroki zaradcze, albo świadomie przejść do planowanych wdrożeń.

Badanie poziomu gotowości organizacji na zmiany inspirowane⁸⁵ kwestionariuszem według Kena Blancharda

Objaśnienia:

Osoba wypełniająca kwestionariusz powinna się skoncentrować na bieżących zmianach w organizacji, na które może mieć wpływ. Do podanych poniżej wypowiedzi należy ustosunkować się przy użyciu skali od 1 do 5. Punktem skali odpowiadają następujące stwierdzenia:

- 1 – zdecydowanie się nie zgadzam;**
- 2 – nie zgadzam się;**
- 3 – ani się zgadzam, ani się nie zgadzam;**

⁸⁵ Domaradzka-Grochowalska Z., Tomaszewicz D. – dostosowanie pojęć do obszaru zarządzania cyfryzacją w oświacie.

4 – zgadzam się;

5 – zdecydowanie się zgadzam.

Stwierdzenia	Liczba pkt
Ludzie zarządzający wprowadzaniem zmiany w obszarze cyfryzacji oświaty rozpatrzyli wiele opcji, przygotowując HDR.	
Do HDR wybrano najlepsze z możliwych opcji.	
Wdrożenie HDR jest niezbędne do wprowadzenia zmian w obszarze cyfryzacji oświaty.	
Istnieją motywujące powody dla wprowadzenia planowanych działań w HDR.	
Kadra zarządzająca w JST mocno wspiera wdrażanie HDR.	
Mam zaufanie do osób zarządzających odpowiedzialnych za wprowadzanie HDR.	
Komunikacja w zakresie planowanych wdrożeń wynikających z HDR – bez względu na nadawcę informacji – jest czytelna i wystarczająca.	
Mam świadomość efektów wynikających z planowanego wdrożenia HDR.	
Mam pozytywne nastawienie do planowanych wdrożeń wynikających z HDR.	
Z zadowoleniem patrzę w przyszłość mojej jednostki po wdrożeniu zaplanowanych działań.	
Rozumiem ważność planowanych działań w stosunku do innych projektów w danej jednostce.	
Dana jednostka jest gotowa wdrożyć planowane działania zgodnie z przyjętym harmonogramem.	
Napotykanie trudności będą traktowane jako okazja do nauki, a nie jako porażka wymagająca ukarania winnych.	
Pozyskam niezbędne zasoby do planowanych wdrożeń (np. ludzi, czas, narzędzia, szkolenia, informację zwrotną).	
Zostanę odpowiednio przeszkolony(a) w zakresie umiejętności niezbędnych do wdrażania zaplanowanych działań.	
Mam wiedzę, w jakich miejscach i u jakich podmiotów mogę szukać wsparcia i pomocy w razie pojawienia się jakiegokolwiek pytań, obaw czy nowych wyzwań związanych z planowanymi wdrożeniami.	

Stwierdzenia	Liczba pkt
Ludzie zarządzający zmianą w obszarze cyfryzacji oświaty – poprzez własną postawę – określają oczekiwania wobec innych.	
Jestem współodpowiedzialny(a) za przyczynienie się do powodzenia wprowadzanej zmiany wynikającej z wdrażania HDR.	
Jestem gotowy(a) wziąć współodpowiedzialność za powodzenie planowanych wdrożeń.	
Każde planowane działanie przewiduje monitorowanie założonych wskaźników realizacji.	
Jestem przekonany(a), że po wdrożeniu HDR moja jednostka dysponuje odpowiednimi możliwościami pozwalającymi na utrwalanie efektów wprowadzanych zmian.	
Zespół projektowy wraz z zespołem decyzyjnym postuluje konieczność włączenia w proces planowanej zmiany tych osób, których ona dotyczy.	
Wierzę, że zdecydowana większość osób, których dotyczą planowane działania, poprze zmianę, zamiast ją krytykować.	
Mam możliwość podzielenia się swoimi obawami dotyczącymi planowanych wdrożeń.	
Mam możliwość współdecydowania o zakresie i sposobie planowanych wdrożeń.	
SUMA	

Interpretacja wyników:

110–125 punktów: Wprowadzenie zmiany zostało odpowiednio przygotowane. Poradzono sobie z najbardziej typowymi przyczynami niepowodzenia zmiany, co zwiększa prawdopodobieństwo osiągnięcia sukcesu.

86–109 punktów: Wprowadzenie zmiany zostało odpowiednio przygotowane w niektórych obszarach, ale w innych wymaga dalszej pracy, żeby zwiększyć prawdopodobieństwo osiągnięcia sukcesu.

85 lub mniej punktów: Wprowadzenie zmiany nie jest przygotowane. Wymaga jeszcze dużych nakładów pracy w wielu obszarach, żeby zwiększyć prawdopodobieństwo osiągnięcia sukcesu.

Ważne!

Każde pytanie z trzema lub mniej punktami należy zaznaczyć. Obszary, których dotyczyło pytanie, stanowią potencjalne zagrożenie dla powodzenia procesu wprowadzania zmiany.

Zalecenia

Trzeba rozpocząć

Trzeba przestać

Trzeba kontynuować

Podsumowanie

Gromadzenie informacji stanowi pierwszy etap, gdyż okazuje się, że sama wiedza nie jest wystarczająca. Trzeba umieć i chcieć ją wykorzystać w praktyce. Zjawisko transformacji cyfrowej w oświacie jest procesem wieloaspektowym, który obejmuje nie tylko zmianę narzędzi, ale przede wszystkim jest wyrazem głębokiej przemiany w myśleniu o edukacji, roli uczniów, nauczycieli i liderów zmiany.

Wyzwania psychospołeczne, które towarzyszą tej transformacji, ukazują jak silnie są w nas zakorzenione schematy działania, a także jak wiele emocji budzi każda próba ich przełamania. Opór, lęk przed nieznanym, obawy o jakość relacji międzyludzkich w świecie cyfrowym są naturalnymi reakcjami, które jednak nie powinny blokować rozwoju, lecz stać się impulsem do świadomego kształtowania nowych kompetencji i postaw.

Cyfryzacja w oświacie to jest technologią dla technologii. To narzędzie, które – gdy zostanie wykorzystane w sposób przemyślany i odpowiedzialny – może wzbogacić proces kształcenia, otworzyć nowe możliwości dla uczniów i nauczycieli, Ponadto wpływa na przygotowanie młodych ludzi do życia w świecie dynamicznych zmian. Jednak, aby tak się stało, konieczne jest inwestowanie nie tylko w infrastrukturę i narzędzia, ale przede wszystkim w ludzi (ich kompetencje cyfrowe, emocjonalne i społeczne).

Równie kluczowe dla powodzenia transformacji cyfrowej jest zrozumienie, że jest to proces rozłożony w czasie, wymagający strategicznego zarządzania, wspierania kultury organizacyjnej szkoły oraz budowania sieci współpracy między wszystkimi uczestnikami życia oświatowego (samorządami, szkołami, nauczycielami, uczniami i rodzicami).

Świadome zarządzanie zmianą, inwestowanie w rozwój kompetencji, rozwijanie higieny cyfrowej i kształtowanie dojrzałości cyfrowej są nie tylko wyzwaniami, ale też stanowią ogromną szansę na budowanie bardziej otwartej, refleksyjnej i odpowiedzialnej edukacji. Warto sobie uzmysłowić, że technologia zmienia świat, ale to ludzie zmieniają przyszłość, mądrze korzystając z narzędzi cyfrowych. Poza tym nie można zapomnieć, że świat online, choć nie zastąpi świata wartości, to jednak może stać się przestrzenią ich świadomego rozwijania. Zatem wybierajmy mądrze.

11. Bibliografia.

Bauman Z., (2010), „44 listy ze świata płynnej nowoczesności”, Kraków: Wydawnictwo Literackie.

Benavides F., Dumont H., Istance D., (2013), „Istota uczenia się”, Warszawa: Wydawnictwo Wolters Kluwer Polska SA.

Carr N., (2013), „Płytki umysł. Jak internet wpływa na nasz mózg”, Gliwice: Helion.

Centrum Cyfrowe, (2020), „Edukacja w czasach pandemii – raport z badań. Edycja II”, zob. https://centrumcyfrowe.pl/wp-content/uploads/sites/16/2020/11/Raport_Edukacja-zdalna-w-czasie-pandemii-Edycja-II.pdf [dostęp, online dn. 2.09.2025].

Domaradzka-Grochowalska Z., (2021), „Moduł zarządzania kryzysowego. Zarządzanie kryzysowe. Pakiet szkoleniowy dla dyrektorów szkół”, Warszawa: Ośrodek Rozwoju Edukacji, zob. <https://ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=31536> [dostęp, online dn. 2.09.2025].

Domaradzka-Grochowalska Z., (2021), „Moduł zarządzania kryzysowego. Zarządzanie kryzysowe. Pakiet szkoleniowy dla kadry JTS”, Warszawa: Ośrodek Rozwoju Edukacji zob. <https://ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=34654> [dostęp, online dn. 2.09.2025].

- Dryden G., Vos J., (1999), „Rewolucja w uczeniu”, Poznań: Wydawnictwo Zysk i S-ka.
- EdTech Poland, (2022), „Raport: Wykorzystanie technologii edukacyjnych w polskich szkołach”, zob. <https://www.telix.pl/rynek/raporty-prezentacje/2023/01/w-wiekszosci-szkol-internet-jest-tylko-w-salach-informatycznych-i-pokojach-administracji> [dostęp, online dn. 2.09.2025].
- Fundacja Orange (2021), „Wykluczenie społeczno-cyfrowe w Polsce. Stan zjawiska, trendy i rekomendacje”, Warszawa: Fundacja Orange, zob. <https://fundacja.orange.pl/strefa-wiedzy/post/wykluczenie-spoecznie-cyfrowe-w-polsce-2021> [dostęp, online dn. 2.09.2025].
- Fundacja Dajemy Dzieciom Siłę, (2022), „Zdrowie psychiczne dzieci i młodzieży. Raport o zagrożeniach bezpieczeństwa i rozwoju dzieci w Polsce”, zob. https://fdds.pl/_Resources/Persistent/4/b/2/8/4b284d3df9b1087f1d2d0c9724538c9c6f24bf6e/Dzieci%20si%C4%99%20licz%C4%85%202022%20-%20Zdrowie%20psychiczne%20dzieci%20i%20m%C5%82odzie%C5%BCy.pdf [dostęp, online dn. 2.09.2025].
- Fundacja UNAWEZA, (2023), „Młode Głowy. Otwarcie o zdrowiu psychicznym. Raport z badania zdrowia psychicznego, poczucia własnej wartości i sprawczości wśród młodych ludzi”, zob. <https://mlodeglowy.pl/raport> [dostęp, online dn.2.09.2025].
- Hansen A., (2021), „Wyloguj swój mózg”, Kraków: Wydawnictwo ZNAK.
- Hatańska N., (2021), „Wiek paradoksów. Czy technologia nas ocali?”, Kraków: Wydawnictwo ZNAK.
- Jarmuż S., (2023), „Czy mądrości się można nauczyć?”, Warszawa: Wydawnictwo Naukowe PWN.
- Kotter J., (2008), „Sedno zmian. Narzędzia i taktyki pozytywnej transformacji twojej firmy”, HELION, Gliwice.
- Mazurkiewicz G., (red.), (2015), „Ucząca się szkoła. Od rozwoju jednostek do rozwoju wspólnoty”, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
- Ministerstwo Edukacji Narodowej, „Strategia transformacji cyfrowej edukacji – dokumenty strategiczne związane z cyfryzacją oświaty w Polsce”, zob. <https://www.gov.pl/web/edukacja/polityka-cyfrowej-transformacji-edukacji---projekt-uchwaly-rady-ministrow-skierowany-do-konsultacji2> [dostęp, online dn. 2.09.2025].

Ministerstwo Cyfryzacji, (2024), „Strategia Cyfryzacji Polski do 2035 roku”, <https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku> [dostęp: 19.08.2025].

Morańska D., Morbitzer J., Musiał E., Wojciechowski J., (red. nauk.), (2017), „Człowiek – Media – Edukacja”, Dąbrowa Górnicza: Wydawnictwo Naukowe Wyższa Szkoła Biznesu.

NASK – Państwowy Instytut Badawczy, (2021), „Nastolatki 3.0: Edukacja w dobie cyfryzacji”, zob. <https://www.gov.pl/web/cyfryzacja/mlodziez-w-internecie---raport-nastolatki-30> [dostęp, online, dn. 2.09.2025].

Pilipczuk K., (red.), (2013), „Myślenie systemowe w coachingu”, Warszawa: Pracownia Satysfakcji.

Rosenberg M.B., (2016), „To, co powiesz może zmienić świat”, Warszawa: Wydawnictwo Czarna Owca.

Schleicher A., (2019), „Edukacja światowej klasy. Jak kształtować systemy szkolne na miarę XXI wieku”, Warszawa: Związek Nauczycielstwa Polskiego.

Szewczyk A., (2017), *Cyfrowa szkoła – skok w przyszłość dydaktyki*, <https://repozytorium.ur.edu.pl/items/ae9f0071-1892-4d97-8f89-f7f130639581> [dostęp, online dn. 02.09. 2025].

Walkiewicz J., (2014), „Pełna MOC możliwości”, Gliwice: Wydawnictwo Onepress.

Walkiewicz J., (2017), „Pełna MOC życia. Jeśli o czymś w życiu marzysz – sięgnij po to”, Gliwice: Wydawnictwo Onepress.

Zielinski R., (2023), „Cyfrowa edukacja dziś: między szansą a wyzwaniem – studium porównawcze”, Warszawa: Instytut Badań Edukacyjnych, zob. <https://www.ibe.edu.pl/images/EBiS/Numery/2023-2/EBiS-2023-2-12-Cyfrowa-edukacja-dzis.pdf> [dostęp: 2.09.2025].

Związek Cyfrowa Polska, (2024), „Raport Cyfrowa Szkoła 4.0”, zob. https://cyfrowapolska.org/wp-content/uploads/2024/03/Raport_Cyfrowa_Szkola_4.pdf [dostęp, online dn. 2.09.2025].

ARKUSZE DIAGNOSTYCZNE DO BADANIA STANU CYFRYZACJI OŚWIATY W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO



Michał Cupiał, Zofia Domaradzka-Grochowalska, Dorota Jastrzębska, Anna Pawełas,
Dorota Pintal, Dorota Tomaszewicz

1. Arkusz do diagnozy wstępnej. Część 1.

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
1. Wdrożenie narzędzi cyfrowych umożliwiających zdalne nauczanie z wykorzystaniem technologii cyfrowych na poziomie JST, szkół, przedszkoli i placówek oświatowych.	1.1. Wdrożenie platformy umożliwiającej zdalne nauczanie, komunikację i współpracę.		
	1.2. Wdrożenie ZPE.		
	1.3. Inne:		
2. Wdrożenie narzędzi informatycznych wspomagających zarządzanie oświatą.	2.1. Wprowadzenie elektronicznych arkuszy organizacji z modułem finansowym usprawniających procedurę ich zatwierdzania i pozwalających oszacować koszty funkcjonowania szkół, przedszkoli i placówek na etapie zatwierdzania organizacji (np. program i Arkusz – Wolters Kluwer SA, SIGMA Firmy Vulcan, arkusz Firmy Astar 05).		
	2.2. Stosowanie zintegrowanego systemu informatycznego wspomagającego zarządzanie oświatą jako kompleksowe, systemowe rozwiązanie wspierające zarówno zadania realizowane przez wydziały edukacji, jak i codzienną pracę szkół i placówek oświatowych.		
	2.3. Inne:		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
3. Inwentaryzacja posiadanych zasobów cyfrowych (obejmujących software i hardware) w szkołach, przedszkolach i placówkach oświatowych.	3.1. Stosowanie specjalistycznego oprogramowania do inwentaryzacji zasobów teleinformatycznych.		
	3.2. Prowadzenie ewidencji w dedykowanym oprogramowaniu przez pracowników odpowiedzialnych za zasoby IT w szkole, przedszkolu, placówce oświatowej.		
	3.3. Prowadzenie ewidencji w arkuszach kalkulacyjnych przez pracowników odpowiedzialnych za zasoby IT w szkole, przedszkolu, placówce oświatowej.		
	3.4. Prowadzenie ewidencji z wykorzystaniem narzędzi księgowych w oparciu o przyjęte w szkole, przedszkolu i placówce oświatowej zasady rachunkowości.		
	3.5. Zinwentaryzowanie jednostek komputerowych oraz ich stopniowa wymiana. Zastosowanie jednolitego (na poziomie jednostek oświatowych lub całego JST) oprogramowania systemowego oraz narzędziowego wykorzystywanego w procesie nauczania).		
	3.6. Inne:		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
4. Weryfikacja posiadanych zasobów pod kątem wykorzystania technologii cyfrowych przez szkoły, przedszkola i placówki oświatowe.	4.1. Badanie wykorzystania sprzętu i oprogramowania (m. in. analiza logów systemowych i statystyk użytkowania, rejestry korzystania z oprogramowania edukacyjnego).		
	4.2. Analiza finansów i budżetu JST (przegląd sprawozdań budżetowych szkół, benchmarking między placówkami – porównanie nakładów finansowych w stosunku do liczby uczniów / nauczycieli).		
	4.3. Inne:		
5. Finansowanie doskonalenia nauczycieli w zakresie cyfrowej transformacji szkoły, przedszkola i placówki oświatowej.	5.1. Wyodrębnienie w budżecie środków finansowych na szkolenia dla nauczycieli w zakresie wykorzystania technologii cyfrowych.		
	5.2. Analiza wydatków na doskonalenie nauczycieli i kadry zarządzającej w zakresie podnoszenia kompetencji cyfrowych.		
	5.3. Inne:		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

2. Arkusz do diagnozy wstępnej. Część 2.

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
6. Planowanie i budowa infrastruktury IT. Wymóg wynikający z par. 20 ust. 2 pkt. 7, 8, 12 lit. f, KRI. Wymóg wynikający z art. 24 ust. 1 i 32 ust. 1 lit. b i c RODO.	6.1. Opracowano architekturę sieci zapewniającą optymalne wykorzystanie zasobów i zwiększenie jej przepustowości, w celu płynnego działania narzędzi edukacyjnych i aplikacji administracyjnych.		
	6.2. Zbudowano zaplanowaną według dobrych praktyk topografię sieci uwzględniającą strefy zdemilitaryzowane oraz uwzględniono możliwość dalszego planowania zabezpieczeń oraz prawidłowego umieszczania zabezpieczeń takich jak urządzenia UTM, firewall, sondy IPS / IDS oraz elementy monitorujące ruch sieciowy.		
	6.3. Zastosowano nowoczesne i odpowiednio zabezpieczone urządzenia sieciowe, takie jak routery, przełączniki oraz punkty dostępowe, zapewniające stabilność i bezpieczeństwo infrastruktury IT.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
6. Planowanie i budowa infrastruktury IT. Wymóg wynikający z par. 20 ust. 2 pkt. 7, 8, 12 lit. f, KRI. Wymóg wynikający z art. 24 ust. 1 i 32 ust. 1 lit. b i c RODO.	6.4. Przeprowadzono testy wydajności i bezpieczeństwa sieci, w celu identyfikacji i eliminacji potencjalnych problemów.		
	6.5. Zapewniono monitorowanie i regularne aktualizacje elementów infrastruktury IT zapewniając utrzymanie jej stabilności, bezpieczeństwa i wydajności, wspierając proces nauczania i zarządzania.		
	6.6. Inne:		
7. Analiza ryzyka dla zasobów IT. Wymóg wynikający z par.20 ust. 2 pkt. 3 KRI. Wymóg wynikający z art. 24 ust. 1 i 32 ust. 1 RODO.	7.1. Opracowano i wdrożono proces zarządzania bezpieczeństwem informacji, który obejmuje analizę ryzyka dla zasobów IT, umożliwiającą identyfikację potencjalnych zagrożeń wpływających na urządzenia, systemy informatyczne oraz przetwarzane dane.		
	7.2. Przeprowadzana jest regularnie, nie rzadziej niż raz na rok, identyfikacja potencjalnych zagrożeń lub ryzyk, które mogą wpływać na zasoby IT w jednostkach oświatowych i JST.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
7. Analiza ryzyka dla zasobów IT. Wymóg wynikający z par.20 ust. 2 pkt. 3 KRI. Wymóg wynikający z art. 24 ust. 1 i 32 ust. 1 RODO.	7.3. Proces analizy ryzyka uwzględnia identyfikację podatności systemów zarządzania zasobami IT, które mogą być wykorzystane przez cyberprzestępców lub spowodować awarie uniemożliwiające realizację zadań.		
	7.4. Ustalono potencjalny wpływ materializacji zagrożeń na jednostkę oświatową lub JST, dzięki czemu identyfikowane są konsekwencje wystąpienia poszczególnych zagrożeń oraz jakie zasoby będą niezbędne do ich usunięcia.		
	7.5. Zapewniono monitorowanie zidentyfikowanych ryzyk, co pozwala na bieżące dostosowywanie strategii zarządzania bezpieczeństwem informacji do zmieniających się warunków i nowych zagrożeń, utrzymując wysoki poziom bezpieczeństwa informacji w organizacji.		
	7.6. Inne:		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
8. Dobór zabezpieczeń. Wymóg wynikający z par. 20 ust. 2 pkt. 4–13, par. 21 KRI.	8.1. Opracowano i wdrożono adekwatne zabezpieczenia transferu danych, obejmujące wdrożenie technologii szyfrowania danych przesyłanych w sieci oraz identyfikację podmiotów uczestniczących w procesie transferu danych.		
	8.2. Zastosowano zabezpieczenia styku zasobów IT z siecią internet, w tym aktywne urządzenia brzegowe (UTM, bramy sieciowe trzeciej generacji itp.) oraz aktualne polityki bezpieczeństwa dla tych urządzeń poprzez odpowiednie licencje lub wykwalifikowany personel zarządzający tymi urządzeniami.		
	8.3. Regularnie aktualizowany jest firmware elementów infrastruktury IT (urządzenia sieciowe, urządzenia końcowe, serwery itd).		
	8.4. Wdrożono narzędzia do monitorowania stanu i wydajności urządzeń podłączonych do sieci jednostki, w celu śledzenia ich funkcjonowania i szybkiego reagowania na nieprawidłowości.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
8. Dobór zabezpieczeń. Wymóg wynikający z par. 20 ust. 2 pkt. 4–13, par. 21 KRI.	8.5. Zaimplementowano systemy wykrywania i zapobiegania intruzjom (np. IDS / IPS, SIEM, AV i Firewall 3gen), które monitorują sieć i reagują na podejrzany ruch lub zdarzenia.		
	8.6. Wdrożono rozwiązania zapobiegające wyciekom danych (DLP).		
	8.7. Zapewniono mechanizmy monitorowania ruchu sieciowego, zapewniono zapis i analizę logów sieciowych, w celu umożliwienia identyfikacji i reakcji na incydenty bezpieczeństwa.		
	8.8. Wdrożono politykę zarządzania uprawnieniami, która obejmuje mechanizmy kontroli dostępu do systemów i urządzeń na podstawie ról i uprawnień oraz systemu zastępstw, co zapobiega nieuprawnionej eskalacji nadawanych uprawnień.		
	8.9. Zabezpieczono urządzenia końcowe poprzez instalację oprogramowania antywirusowego i firewall, zapewnienie aktualnych wersji oprogramowania i systemów operacyjnych, a także wdrożenie pełnego szyfrowania dysków.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
8. Dobór zabezpieczeń. Wymóg wynikający z par. 20 ust. 2 pkt. 4–13, par. 21 KRI.	8.10. Wprowadzono monitorowanie i zdalne zarządzanie urządzeniami końcowymi za pomocą nowoczesnych systemów monitorujących, audytowych lub antywirusowych.		
	8.11. Wykorzystywane są systemy Data Loss Protection (dalej DLP) zapobiegające wyciekom danych.		
	8.12. Wdrożono oprogramowanie monitorujące wykorzystanie urządzeń IT, które umożliwia śledzenie zdarzeń związanych z bezpieczeństwem i zapewnienie ciągłości działania.		
	8.13. Zatrudniono wykwalifikowany personel IT odpowiedzialny za ciągłość działania i bezpieczeństwo zasobów IT oraz zgodność ich funkcjonowania z aktualnymi wymogami prawnymi i standardami.		
	8.14. Zapewniono zewnętrzny wykwalifikowany personel IT odpowiedzialny za ciągłość działania i bezpieczeństwo zasobów informatycznych, a także oraz zgodność ich funkcjonowania z aktualnymi wymogami prawnymi i standardami.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
8. Dobór zabezpieczeń. Wymóg wynikający z par. 20 ust. 2 pkt. 4–13, par. 21 KRI.	8.15. Wdrażając mechanizmy bezpieczeństwa informacji, kierowano się wymogami prawa, dobrymi praktykami i standardami (np. ISO 27001, NIST).		
	8.16. Wyznaczono pracowników odpowiedzialnych za wdrożone elementy zabezpieczeń.		
	8.17. Inne:		
9. Planowanie i wdrażanie SZBI. Wymóg wynikający z par. 20 ust. 1, ust. 2 pkt. 1, ust. 2 pkt. 1 KRI. Wdrożenie polityk mających na celu prawidłowe przetwarzanie i ochronę danych osobowych wynika z art. 24 ust. 2 RODO.	9.1. Opracowano i wdrożono SZBI nieuwzględniający planów ciągłości działania i procedur przywracania funkcjonalności systemów po katastrofie.		
	9.2. Opracowano i wdrożono SZBI uwzględniający plany ciągłości działania i procedury przywracania funkcjonalności systemów po katastrofie.		
	9.3. Przeprowadzono identyfikację krytycznych zasobów sprzętowych, informacyjnych i funkcji biznesowych.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
9. Planowanie i wdrażanie SZBI. Wymóg wynikający z par. 20 ust. 1, ust. 2 pkt. 1, ust. 2 pkt. 1 KRI. Wdrożenie polityk mających na celu prawidłowe przetwarzanie i ochronę danych osobowych wynika z art. 24 ust. 2 RODO.	9.4. Przeprowadzane są testy i symulacje ataków i awarii w celu weryfikacji skuteczności zaplanowanych scenariuszy awaryjnych i zapewnienia ich gotowości do użycia.		
	9.5. Prowadzona jest regularna ewaluacja i aktualizacja procedur na podstawie zmieniających się warunków operacyjnych i technologicznych, w celu utrzymania ich aktualności i skuteczności.		
	9.6. Regularnie przeprowadzane są szkolenia dla pracowników z zakresu obowiązujących procedur, bezpieczeństwa informacji, zasad reagowania na awarie i mechanizmów zapewnienia ciągłości działania.		
	9.7. Zapewniono zarządzanie zdarzeniami bezpieczeństwa informacji, obejmujące opracowanie i wdrożenie procedur postępowania z incydentami IT.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
9. Planowanie i wdrażanie SZBI. Wymóg wynikający z par. 20 ust. 1, ust. 2 pkt. 1, ust. 2 pkt. 1 KRI. Wdrożenie polityk mających na celu prawidłowe przetwarzanie i ochronę danych osobowych wynika z art. 24 ust. 2 RODO.	9.8. Zapewniono zarządzanie zdarzeniami bezpieczeństwa informacji, obejmujące opracowanie i wdrożenie procedur postępowania z incydentami IT zgodnie z wymogami prawnymi krajowego systemu cyberbezpieczeństwa i ogólnego rozporządzenia o ochronie danych.		
	9.9. Inne:		
10. Realizacja audytów bezpieczeństwa informacji. Wymóg wynikający z par. 20 ust. 2 pkt. 14 KRI. Wymóg wynikający z 32 ust. 1 lit. d RODO.	10.1. Opracowano i wdrożono procedury realizacji audytów bezpieczeństwa informacji w szkołach, przedszkolach i placówkach oświatowych oraz JST, w celu zapewnienia zgodności z przepisami prawa i przyjętymi normami oraz weryfikacji faktycznego poziom bezpieczeństwa danych i zasobów IT.		
	10.2. Realizowane są audyty bezpieczeństwa informacji umożliwiające dokładne zidentyfikowanie słabych punktów i potencjalnych zagrożeń, co pozwala na wczesne podjęcie działań korygujących i zapobiegawczych.		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

Zadanie	Narzędzia i rozwiązania zarządcze	Wdrożone w danej JST TAK / NIE	Jeśli TAK, proszę ocenić stopień efektywności w skali 1–4*
10. Realizacja audytów bezpieczeństwa informacji. Wymóg wynikający z par. 20 ust. 2 pkt. 14 KRI. Wymóg wynikający z 32 ust. 1 lit. d RODO.	10.3. Audyty przeprowadzane są nie rzadziej niż raz na rok, przez podmioty zewnętrzne posiadające uprawnienia, o których mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 roku w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dziennik Ustaw z 2018 roku pozycja 1999).		
	10.4. Jednostki oświatowe lub JST wskazały osoby odpowiedzialne za monitorowanie wykonania zaleceń poaudytowych.		
	10.5. Podczas audytów wykonywane są testy penetracyjne lub testy podatności posiadanych zasobów teleinformatycznych.		
	10.6. Inne:		

1 – bardzo niski, 2 – niski, 3 – wysoki, 4 – bardzo wysoki

3. Arkusz do diagnozy wstępnej. Część 3.

Narzędzia i rozwiązania wspierające personalny rozwój organizacji	Wdrożone w danej JST TAK	Wdrożone w danej JST NIE
1) Włączenie różnych interesariuszy, w tym dyrektorów szkół, przedszkoli i placówek oświatowych, w proces planowania rozwoju oświaty dotyczy cyfryzacji poprzez wspólne prowadzenie diagnozy, wspólne planowanie zmiany, wdrażanie i monitorowanie działań.		
2) Wypracowanie zasad współpracy i komunikacji na linii organ prowadzący i dyrektorzy szkół, przedszkoli i placówek oświatowych z wykorzystaniem wybranych narzędzi cyfrowych.		
3) Opracowanie ram i zasad współpracy pomiędzy szkołami i instytucjami zewnętrznymi (firmami, NGO, instytucjami kulturalnymi, uczelniami) na rzecz rozwoju kompetencji cyfrowych.		
4) Analizowanie potrzeb i oczekiwań społeczności lokalnej w zakresie organizacji i funkcjonowania jednostek oświatowych dotyczących cyfrowego rozwoju oświaty w JST, np. analizy SWOT z perspektywy samorządowca, rodzica, dyrektorów, nauczycieli, uczniów, pracodawców, itp.		
5) Przeprowadzenie badania wykorzystywania cyfrowego potencjału szkoły z wykorzystaniem narzędzia SELFIE w ostatnich dwóch latach.		
6) Przeprowadzenie ankiety wśród nauczycieli w zakresie wykorzystania zasobów szkoły, przedszkola i placówki oświatowej.		
7) Przeprowadzenie ankiety wśród nauczycieli w zakresie wykorzystania bezpłatnych, edukacyjnych zasobów internetowych, w tym Zintegrowanej Platformy Edukacyjnej.		

Narzędzia i rozwiązania wspierające personalny rozwój organizacji	Wdrożone w danej JST TAK	Wdrożone w danej JST NIE
8) Przeprowadzenie ankiety wśród uczniów w zakresie wykorzystywania zasobów cyfrowych przez nauczycieli.		
9) Przeprowadzenie badania umiejętności cyfrowych nauczycieli, dyrektorów, pracowników JST w odniesieniu do DigComp 2.2 – jako narzędzia wspierającego planowanie rozwoju (opis kompetencji na poszczególnych poziomach według Ramy Europejskiej).		
10) Prowadzenie badań ankietowych dotyczących poziomu kompetencji cyfrowych nauczycieli, dyrektorów, pracowników JST.		
11) Prowadzenie badań ankietowych (np. dotyczących porównania poziomu satysfakcji uczniów, nauczycieli, rodziców z jakości usług edukacyjnych) w zakresie kształcenia kompetencji cyfrowych.		
12) Prowadzenie badań potrzeb społecznych w zakresie cyfryzacji oświaty.		
13) Organizowanie debat o stanie cyfryzacji w oświacie z udziałem lokalnych interesariuszy.		
14) Planowanie doskonalenia zawodowego nauczycieli ukierunkowanego na rozwój kompetencji cyfrowych w formie procesowego wspomaganie.		
15) Podnoszenie kompetencji nauczycieli w zakresie stosowania narzędzi cyfrowych w pracy z uczniami o zróżnicowanych potrzebach edukacyjnych.		
16) Organizacja sieci współpracy i samokształcenia w zakresie cyfryzacji oświaty.		
17) Doskonalenie uwzględniającego model zarządzania szkołą z wykorzystaniem narzędzi cyfrowych.		
18) Organizacja wizyt studyjnych dyrektorów szkół i liderów samorządowej oświaty.		

Narzędzia i rozwiązania wspierające personalny rozwój organizacji	Wdrożone w danej JST TAK	Wdrożone w danej JST NIE
19) Wsparcie kompetencyjne dyrektorów ukierunkowane na budowanie nowoczesnego środowiska nauki i pracy w zmieniającej się rzeczywistości (kompetencje kluczowe ze szczególnym uwzględnieniem kompetencji cyfrowych, systemowy rozwój organizacji, szkoła jako organizacja ucząca się, inteligencja emocjonalna dyrektora i nauczyciela, budowanie dobrostanu psychicznego).		
20) Wsparcie coachingowe dla kadry zarządzającej (przedstawicieli JST i dyrektorów szkół).		
21) Wypracowanie z dyrektorami wdrożenia systemowych rozwiązań związanych z kształceniem na odległość i wykorzystywanie tych rozwiązań w codziennej pracy.		
22) Poszerzanie oferty szkół oraz instytucji kulturalno-oświatowych w zakresie rozwijania kompetencji cyfrowych dzieci i młodzieży o różnicowanych potrzebach edukacyjnych.		
23) Uspołecznianie procesu planowania finansowego w szkołach lub gminach (np. poprzez organizację grantów lokalnych na rzecz rozwijania kompetencji cyfrowych, projektów STEAM itp.).		
24) Uspołecznianie procesu planowania finansowego w szkole/gminie m.in. poprzez ustalenie kanonu informacji na temat możliwości pozyskiwania środków zewnętrznych oraz udrożnienie kanałów informacyjnych na linii JST – dyrektorzy.		
25) Pozyskiwanie środków zewnętrznych na finansowanie projektów i grantów ze szczególnym uwzględnieniem możliwości rozwoju cyfryzacji.		

4. Wzór Harmonogramu Działań Rozwojowych (dalej HDR)

Nazwa JST:

Cel.....

Obszar: Rola i zadania JST w zakresie cyfryzacji oświaty.

Zadania:

- 1)
- 2)

Narzędzia i rozwiązania zarządcze:

- 1)
- 2)

Polecane narzędzia i rozwiązania wspierające personalny rozwój organizacji:

- 1)
- 2)
.....

Czas realizacji HDR:

Krótką charakterystyka JST:

Przebieg diagnozy (narzędzia, metody):

Wnioski z diagnozy i rekomendacje:

Zadanie nr 1:

Lp.	Działanie	Sposób realizacji i uwagi	Terminy	Zasoby (np. ludzie, miejsce, czas)	Osoba odpowiedzialna
1.1					
1.2					
...					

Zadanie nr 2:
.....

Lp.	Działanie	Sposób realizacji i uwagi	Terminy	Zasoby (np. ludzie, miejsce, czas)	Osoba odpowiedzialna
2.1					
2.2					
...					

Sposoby monitorowania HDR

Monitorowanie			
Numer działania	Miernik	Wskaźnik	Sposoby dokumentowania
1.1			
1.2			
...			
2.1			
2.2			
...			

Prezentacja rozwiązań przyjętych w HDR (do wyboru)⁸⁶:

1. Opis dobrej praktyki.
2. Minireportaż z wywiadem.
3. Studium refleksji w oparciu o etapy dyskusji zogniskowanej.

⁸⁶ Formatki do opisu dobrych praktyk znajdują się w opracowaniu „Model doradztwa dla jednostek samorządu terytorialnego”, zob. <https://ore.edu.pl/2019/05/materiały-do-pobrania-2/> [dostęp, online dn.2.09.2025].

SŁOWNIK POJĘĆ



Poniższy słownik ma na celu pomoc w zrozumieniu pojęć stosowanych w arkuszach diagnostycznych.

Brama sieciowa – urządzenie lub oprogramowanie, które kontroluje ruch sieciowy przepływający między różnymi sieciami komputerowymi. Dobrze skonfigurowana brama sieciowa działa jako bariera ochronna, pozwalając na przepływ tylko autoryzowanego ruchu, blokując jednocześnie nieautoryzowane połączenia i chroniąc sieć przed zagrożeniami zewnętrznymi.

Data Loss Prevention (DLP) – systemy zapobiegania wyciekom danych, które monitorują, wykrywają i blokują nieautoryzowane przesyłanie poufnych danych na zewnątrz organizacji. DLP zapewnia, że ważne informacje (np. dane osobowe, finansowe czy inne ważne informacje) są chronione przed utratą i nieuprawnionym dostępem.

Firewall – urządzenie lub program komputerowy, które monitoruje i kontroluje ruch przychodzący i wychodzący w sieci na podstawie określonych reguł bezpieczeństwa. Firewall działa jako pierwsza linia obrony, blokując potencjalne zagrożenia takie jak ataki hakerskie czy wirusy.

Hardware – fizyczne komponenty komputera i innych urządzeń elektronicznych. Do hardware zaliczamy procesory, pamięci Random Access Memor (RAM), dyski twarde, karty graficzne, monitory, klawiatury, myszki, drukarki i inne urządzenia peryferyjne.

Infrastruktura technologii informatycznej (IT) – całość zasobów technicznych (fizycznych) i programowych używanych do zarządzania i obsługi informacji w organizacji. Infrastruktura IT jest różnorodna (np. obejmuje okablowanie, serwery, sieci, urządzenia sieciowe, bazy danych, systemy operacyjne, oprogramowanie aplikacyjne i inne zasoby technologiczne).

Intruzja – nieautoryzowane wejście do systemu komputerowego lub sieci. Intruzja może prowadzić do kradzieży danych, uszkodzenia systemu lub zakłócenia jego działania. Atakujący mogą używać różnych technik (np. phishingu, złośliwego oprogramowania czy brute force), aby uzyskać dostęp do systemów informatycznych.

International Organization for Standardization 27001 (ISO) – międzynarodowa norma dotycząca SZBI. Norma ISO 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI, mając na celu ochronę informacji przed zagrożeniami i zapewnienie poufności, integralności oraz dostępności danych. W Polsce norma ISO 27001 jest bardzo często wzorcem postępowania implementowanym do przepisów prawa określających zasady zarządzania bezpieczeństwem informacji.

Krajowy System Cyberbezpieczeństwa (KSC) – system regulacji i procedur mających na celu ochronę infrastruktury krytycznej i usług kluczowych przed zagrożeniami cybernetycznymi na poziomie krajowym (aktualny stan prawny). KSC obejmuje środki zapobiegawcze, procedury reagowania na incydenty oraz współpracę między różnymi podmiotami w zakresie cyberbezpieczeństwa na poziomie kraju oraz zasady współpracy międzynarodowej w tym zakresie. KSC jest zdefiniowany w ustawie z dnia 5 lipca 2018 roku o KSC (Dziennik Ustaw z 2023 roku pozycja 913 ze zmianami).

Krajowe Ramy Interoperacyjności (KRI) – Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dziennik Ustaw z 2017 roku pozycja. 2247) stanowiące zbiór wytycznych i standardów, które mają na celu zapewnienie interoperacyjności systemów teleinformatycznych używanych przez administrację publiczną w Polsce. Jednym z elementów KRI jest nałożenie na podmioty realizujące zadania publiczne obowiązku wdrożenia SZBI (w szczególności par. 20 KRI).

Malware – złośliwe oprogramowanie, które może uszkodzić komputer, kraść dane lub powodować inne problemy. Przykładami malware są: wirusy, robaki, trojany, ransomware i spyware. Malware jest często wykorzystywane przez cyberprzestępców do kradzieży informacji, szantażu lub sabotażu.

Monitorowanie ruchu sieciowego – proces obserwacji i analizy danych przesyłanych przez sieć komputerową w celu wykrywania i reagowania na podejrzanе lub nieautoryzowane działania. Monitorowanie ruchu sieciowego pomaga w identyfikacji

zagrożeń, takich jak ataki Distributed Denial of Service (DDoS – atak, którego efektem jest „zablokowanie” realizowanej za pomocą zasobów IT usługi), próby włamań czy inne anomalie.

Network and Information Systems Directive 2 (NIS2) – dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE (Directive (EU) 2022/2555 of the European Parliament and of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). Dyrektywa Unii Europejskiej mająca na celu poprawę cyberbezpieczeństwa w państwach członkowskich. NIS2 wprowadza minimalne wymagania dotyczące bezpieczeństwa sieci i informacji oraz obowiązki raportowania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych. Przepis ten będzie implementowany w Polsce zmianą ustawy o krajowym systemie cyberbezpieczeństwa.

Narodowe Standardy Cyberbezpieczeństwa (NSC) – to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. NSC zostały opracowane na podstawie standardów amerykańskiego National Institute of Science and Technology (NIST) oraz przyporządkowane obowiązującym w polskim systemie prawnym normom stosowanym w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych. NSC to przewodniki metodyczne, które ułatwią budowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w administracji federalnej USA. NSC realizują interwencję 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (RP) na lata 2019–2024 w zakresie opracowania i wdrożenia NSC⁸⁷.

Program antywirusowy – oprogramowanie zaprojektowane do wykrywania, blokowania i usuwania złośliwego oprogramowania z komputerów i sieci. Programy antywirusowe skanują pliki i monitorują aktywność systemu w poszukiwaniu zagrożeń, takich jak wirusy, robaki, trojany czy ransomware.

⁸⁷ Narodowe Standardy Bezpieczeństwa (NSC), zob. <https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber> [dostęp, online 2.09.2025].

Punkt dostępowy – urządzenie, które umożliwia bezprzewodowym urządzeniom (np. laptopom, smartfonom) łączenie się z siecią komputerową poprzez sieć internetową (dalej Wi-Fi). Punkt dostępowy działa jako most między siecią bezprzewodową a przewodową, zapewniając dostęp do zasobów sieciowych.

Ransomware – rodzaj złośliwego oprogramowania, które szyfruje dane ofiary i żąda okupu za ich odszyfrowanie. Ransomware blokuje dostęp do systemu lub danych, dopóki ofiara nie zapłaci okupu, często w krypto walucie (np. Bitcoin).

Ogólne rozporządzenie o ochronie danych (RODO) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). RODO określa zasady przetwarzania i ochrony danych osobowych.

Router – urządzenie sieciowe, które kieruje pakiety danych między różnymi sieciami, zapewniając połączenie między nimi. Routery są używane do łączenia sieci lokalnych z Internetem oraz zarządzania ruchem danych w sieci.

Security Information and Event Management (SIEM) – system zbierający i analizujący dane z różnych źródeł w celu wykrywania, analizowania i reagowania na zagrożenia bezpieczeństwa. SIEM umożliwia centralne zarządzanie logami i zdarzeniami z różnych systemów bezpieczeństwa, takich jak firewalles, systemy Intrusion Detection System (dalej IDS) / Intrusion Prevention System (dalej IPS) i inne.

Software – oprogramowanie, czyli programy komputerowe i aplikacje działające na sprzęcie komputerowym lub urządzeniach IT.

Sonda IDS (Intrusion Detection System) – system wykrywający nieautoryzowane i podejrzane działania w sieci, ale nie podejmujący działań w celu ich zablokowania. IDS monitoruje ruch sieciowy i generuje alerty w przypadku wykrycia potencjalnych zagrożeń.

Sonda IPS (Intrusion Prevention System) – system wykrywający i zapobiegający nieautoryzowanym działaniom w sieci poprzez blokowanie podejrzanego ruchu. IPS działa podobnie jak IDS, ale dodatkowo podejmuje działania zapobiegawcze (np. blokowanie podejrzanych pakietów danych).

Strefa zdemilitaryzowana (DMZ) – część sieci komputerowej, która jest odseparowana od sieci wewnętrznej i zewnętrznej. DMZ jest używana do hostowania (utrzymywania i świadczenia) usług dostępnych publicznie, takich jak serwery WWW, co minimalizuje ryzyko bezpośredniego ataku na sieć wewnętrzną.

Systemy teleinformatyczne i informatyczne – zintegrowane systemy sprzętowe i programowe używane do zarządzania i przetwarzania informacji. Systemy informatyczne mogą obejmować bazy danych, serwery aplikacji, systemy Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) i inne. Zgodnie z ustawą z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dziennik Ustaw z 2019 roku pozycja 60 ze zmianami) systemy teleinformatyczne/informatyczne definiowane są jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.

Technologie cyfrowe – narzędzia i zasoby oparte na technologiach komputerowych, które umożliwiają przetwarzanie, przechowywanie i przesyłanie danych w formie cyfrowej. Przykładami technologii cyfrowych są: komputery, smartfony, internet, chmura obliczeniowa i inne.

Test penetracyjny – symulowany atak na zasoby IT w celu identyfikacji jego słabych punktów i oceny skuteczności zabezpieczeń. Celem testu penetracyjnego jest przełamanie zabezpieczeń, dlatego powinny być one przeprowadzane przez specjalistów ds. bezpieczeństwa w kontrolowanych warunkach.

Testy podatności – proces identyfikacji i oceny słabych punktów systemów informatycznych, które mogą być wykorzystane przez atakujących. Testy podatności obejmują skanowanie systemów w poszukiwaniu znanych luk bezpieczeństwa.

Urządzenie końcowe – komputer, tablet, smartfon lub inne urządzenie używane przez końcowego użytkownika do uzyskania dostępu do zasobów sieciowych. Urządzenia końcowe są często celem ataków cybernetycznych, dlatego muszą być odpowiednio zabezpieczone.

Unified Threat Management (UTM) – zintegrowany system zarządzania zagrożeniami, łączący różne funkcje bezpieczeństwa, takie jak firewall, antywirus, filtracja treści,

wykrywanie intruzji i inne. UTM zapewnia kompleksową ochronę przed różnymi typami zagrożeń.

Zasoby cyfrowe – pliki, dokumenty, oprogramowanie i inne dane przechowywane i przetwarzane w formie cyfrowej.

Zasoby internetowe – strony internetowe, aplikacje online, bazy danych i inne usługi dostępne przez internet.

Zasoby szkoły – wszystkie materiały, urządzenia, oprogramowanie i dane, które są wykorzystywane w szkole do celów edukacyjnych i administracyjnych. Zasoby szkoły obejmują urządzenia IT, komputery, podręczniki, oprogramowanie edukacyjne, bazy danych nauczycieli i inne.

Publikacja została przygotowana w ramach projektu „Cyfrowy rozwój oświaty w jednostkach samorządu terytorialnego – szkolenie i doradztwo dla kadry JST,” realizowanego w partnerstwie Ośrodka Rozwoju Edukacji ze Związkiem Miast Polskich, współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Plus w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027, Priorytet FERS 01.00, Działanie 01.04 Rozwój systemu edukacji.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



OŚRODEK
ROZWOJU
EDUKACJI