STYCZEŃ-LUTY 2026/NR 1(32)

PWN NAUKA

WSZYSTKO O NOWOCZESNYM SZKOLNICTWIE, NAUCE I WSPÓŁPRACY Z BIZNESEM

CYBERBEZPIECZEŃSTWO NIE MOŻE BYĆ PROJEKTEM NA PÓŹNIEJ

KRZYSZTOF GAWKOWSKI

wicepremier, minister cyfryzacji

ZARZĄDZANIE RYZYKIEM

CYBERBEZPIECZEŃSTWO – PROBLEM IT CZY RYZYKO STRATEGICZNE UCZELNI?

Dr Łukasz Olejnik

MARKETING UCZELNI

MARKA UCZELNI ZACZYNA SIĘ W DZIEKANACIE I W BEZPIECZEŃSTWIE DANYCH

dr inż. Jacek Kotarbiński

TEMAT NUMERU

CYFROWA UCZELNIA

Między technologią, odpowiedzialnością a kulturą organizacyjną

ISSN 2719-4299

PWN | NAUKA

MAGAZYN BEZPŁATNY

Drodzy Czytelnicy,

oddajemy w Państwa ręce numer, którego tematem wiodącym jest cyfrowa transformacja uczelni. Jak pokazują doświadczenia liderów szkół wyższych, ekspertów i praktyków, przestaje ona być jedynie konferencyjnym hasłem, a coraz wyraźniej staje się realnym doświadczeniem instytucji, ludzi i procesów.

W tym wydaniu przyglądamy się jej z różnych perspektyw – strategicznej, technologicznej, organizacyjnej i po prostu ludzkiej. Bo dziś już wiemy, że cyfryzacja szkolnictwa wyższego nie jest projektem informatycznym, lecz jednym z kluczowych obszarów zarządzania uczelnią i budowania jej przewagi konkurencyjnej.

Z rozmów z rektorami i ekspertami wybrzmiewa wyraźnie wniosek, że prawdziwe wyzwania nie zaczynają się w kodzie systemów, lecz w kulturze organizacyjnej. Zmiana narzędzi jest stosunkowo prosta, trudniejsza okazuje się zmiana nawyków, procedur i sposobów myślenia. To dlatego cyfryzacja coraz częściej opisywana jest jako proces kulturowy, a nie wyłącznie technologiczny.

W tym numerze pokazujemy także, jak dane stają się nową walutą zarządzania uczelnią. Nie chodzi tylko o raporty czy statystyki, ale o zdolność podejmowania decyzji opartych na rzetelnej analizie informacji, która wspiera strategię, rozwój i codzienne funkcjonowanie instytucji.

W tym numerze sporo miejsca poświęcamy też bezpieczeństwu cyfrowemu, które dziś nie jest już tylko zagadnieniem technicznym, lecz jednym z kluczowych elementów zarządzania ryzykiem i reputacją. Incydenty rzadko wynikają z jednego błędu systemu, częściej z tego, jak dane krążą między jednostkami, narzędziami i ludźmi. To dlatego zaufanie staje się dziś najcenniejszym kapitałem uczelni i coraz częściej realnym wskaźnikiem jej siły rynkowej.

Przyglądamy się również współpracy nauki i biznesu, rozprawiając się ze stereotypami, które przez lata utrudniały dialog między tymi środowiskami. Różnice rzadko tkwią w ludziach, częściej w systemach motywacyjnych i narracjach, które powtarzamy bez refleksji.

Ten numer jest zapisem momentu przejścia od cyfryzacji rozumianej jako modernizacja systemów do cyfryzacji jako strategii rozwoju uczelni. Łączy głosy decydentów, praktyków, badaczy i partnerów technologicznych, bo tylko taka wieloperspektywiczność pozwala zobaczyć prawdziwą skalę zmiany.

Dziękuję wszystkim autorom i rozmówcom za ich wiedzę, doświadczenie i chęć dzielenia się refleksją. Państwa zapraszam do lektury tego numeru, który, mam nadzieję, stanie się nie tylko źródłem inspiracji, ale także impulsem do rozmów o przyszłości uczelni.

Dorota Siudowska-Mieszkowska

redaktor naczelna

PWN | NAUKA

REDAKTOR NACZELNA
Dorota Siudowska-Mieszkowska

PROMOCJA
Katarzyna Piątkowska

KOREKTA
Anna Wasilewska

PROJEKT GRAFICZNY
I SKŁAD
Anna Piwońska

WYDAWCA
Wydawnictwo Naukowe PWN SA
ul. G. Daimlera 2,
02-460 Warszawa
www.pwn.pl

DOŚWIADCZENIA WDROŻENIOWE

MARKETING UCZELNI

BIZNES I NAUKA

Cyfrowa uczelnia – między technologią, odpowiedzialnością a kulturą organizacyjną

Cyfryzacja szkolnictwa wyższego przestała być projektem informatycznym. Dziś jest jednym z kluczowych obszarów zarządzania uczelnią, dotyka administracji, dydaktyki, finansów, komunikacji, bezpieczeństwa, a w coraz większym stopniu także strategii rozwoju i budowania przewagi konkurencyjnej. W 2026 roku nie pytamy już, czy cyfryzować, lecz jak robić to mądrze: tak, by procesy były szybsze, dane bezpieczne, a wspólnota akademicka rzeczywiście odczuwała poprawę jakości funkcjonowania.

W tym numerze oddajemy głos osobom, które kształtują ten kierunek zmian – ministrowi cyfryzacji oraz rektorom i przedstawicielom uczelni z różnych części Polski. To spojrzenie wieloperspektywiczne: od poziomu regulacyjnego i systemowego, przez zarządzanie uczelnią jako złożoną organizacją, po doświadczenie studenta i codzienną pracę administracji.

Wicepremier i minister cyfryzacji Krzysztof Gawkowski jasno stawia sprawę: cyberbezpieczeństwo nie może być „projektem na później", lecz musi stać się warunkiem stabilnego funkcjonowania uczelni. Nowe przepisy, minimalne standardy bezpieczeństwa, obowiązek raportowania poważnych incydentów i wsparcie sektorowego CSIRT pokazują, że państwo oczekuje od uczelni konkretnych działań, ale równocześnie deklaruje wsparcie systemowe.

Rektorzy uczelni wskazują, że cyfryzacja to proces głęboko transformacyjny. Uniwersytet Ekonomiczny w Poznaniu buduje przewagę na danych i rozwija analitykę wspierającą decyzje strategiczne. Na Uniwersytecie Ekonomicznym w Krakowie podkreśla się, że technologia sama w sobie nie jest największym wyzwaniem, kluczowy okazuje się wymiar kulturowy i zmiana przyzwyczajeń. Politechnika Koszalińska mówi o elastyczności i konsekwencji jako fundamentach długofalowego procesu, który trwa już od ponad dwóch dekad. W SGGW akcent pada na zdalność i sprawność, większość spraw powinna dać się załatwić szybciej, bez papieru i bez zbędnych barier. UMCS stawia na uporządkowanie i integrację procesów, podkreślając, że cyfryzacja ma porządkować, a nie wzmacniać poczucie kontroli. Z kolei Uniwersytet SWPS przypomina, że technologia nie może zastępować relacji, ma odciążać zespoły i pozwalać im pełnić rolę doradczą wobec studentów. UKSW zwraca uwagę na odpowiedzialność instytucjonalną i misję uczelni: rozwiązania cyfrowe mają służyć człowiekowi i wspólnocie, a nie być celem samym w sobie.

Wypowiedzi te pokazują wyraźnie, że wspólnym mianownikiem jest dziś integracja systemów (EOD, EZD, SAP, USOS, CRM), wdrażanie e-doręczeń, e-dyplomów, a także rozwój bezpiecznych e-usług. Jednak równie silnie wybrzmiewa inny wątek: cyfryzacja wymaga przeprojektowania procedur, jasnego określenia odpowiedzialności, budowania kompetencji cyfrowych i prowadzenia dialogu ze społecznością akademicką. To proces nie tylko technologiczny, ale zarządczy i kulturowy.

W centrum tej zmiany pozostaje człowiek – student, pracownik administracji, nauczyciel akademicki. Cyfrowa uczelnia ma być szybsza, bardziej transparentna, dostępna zdalnie, ale także bezpieczna i odporna na zagrożenia. Ma upraszczać, a nie komplikować. Ma integrować, a nie mnożyć narzędzia. Ma wzmacniać wspólnotę, a nie ją fragmentować.

Prezentowane w tym dziale wypowiedzi tworzą obraz polskich uczelni w momencie intensywnej transformacji. To nie jednorazowe wdrożenia, lecz proces strategiczny, który będzie definiował funkcjonowanie akademii w najbliższych latach.

Zapraszamy do refleksji: jak budować cyfrową uczelnię, która łączy sprawność operacyjną, bezpieczeństwo danych i wrażliwość na potrzeby ludzi?

Dorota Siudowska-Mieszkowska

Cyberbezpieczeństwo nie może być projektem na później

Krzysztof Gawkowski

wicepremier, minister cyfryzacji

Uczelnie wyższe wykonują ważne zadanie publiczne. Kształcą, prowadzą badania, napędzają rozwój kraju. Korzystają przy tym z wielu systemów informatycznych: do obsługi studiów, kadr czy finansów, przetwarzając ogromne zbiory danych osobowych studentów i pracowników. Dlatego cyberbezpieczeństwo to dziś nie „projekt na później", ale warunek normalnego, stabilnego funkcjonowania uczelni.

Kampus uniwersytecki nie może stawać w miejscu, bo ktoś kliknął w podejrzany link albo system nie wytrzymał obciążenia. Żeby działać cyfrowo, trzeba zadbać o bezpieczeństwo sieci i systemów – to wielka odpowiedzialność.

W nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa Sejm wprowadził uproszczone wymogi cyberbezpieczeństwa dla uczelni. To praktyczna „lista kontrolna" minimalnych działań, które każda uczelnia powinna wdrożyć: przeprowadzić inwentaryzację zasobów IT, weryfikować uprawnienia personelu, stosować oprogramowanie antywirusowe i dbać o cyberhigienę. Chodzi tu o solidne podstawy, które da się wdrożyć realnie i szybko. Zrezygnowano natomiast z podejścia opartego na analizie ryzyka, bo wymagałoby ono od uczelni posiadania wykwalifikowanych specjalistów, którzy potrafiliby przeprowadzić szacowanie ryzyka i na tej podstawie sami zaproponować odpowiednie zabezpieczenia.

Jednocześnie uczelnie nadal będą zgłaszać incydenty poważne do właściwego sektorowego zespołu CSIRT. Taki zespół reagowania na incydenty w sektorze badań naukowych będzie działał przy ministrze nauki i szkolnictwa wyższego. I tu ważne doprecyzowanie: nie trzeba raportować w ten sposób każdego problemu, ale wyłącznie te zdarzenia, które istotnie zakłócają pracę uczelni. Progi incydentu poważnego określimy w przygotowywanym rozporządzeniu – tak żeby było jasne, kiedy należy zgłaszać incydenty cyberbezpieczeństwa. CSIRT sektorowy będzie wspierał uczelnie w reagowaniu na takie zdarzenia i pomagał jak najszybciej przywrócić działanie usług. Bo w cyberbezpieczeństwie czas reakcji ma kluczowe znaczenie.

Na koniec rzecz bardzo praktyczna: każda uczelnia powinna jasno określić i przetestować wewnętrzną ścieżkę zgłaszania incydentów – do komórki odpowiedzialnej za cyberbezpieczeństwo albo do zewnętrznego dostawcy, jeśli uczelnia korzysta z takich usług. Równie ważne jest to, żeby jasno przypisać odpowiedzialność. Cyberbezpieczeństwo nie zadzieje się „samo". To proces, który wymaga szybkich decyzji, jasnych procedur i konsekwencji. Cel jest prosty: żeby student miał dostęp do usług, dane były chronione, a uczelnia mogła uczyć i prowadzić badania naukowe bez cyfrowych przestojów.

Elastyczność i konsekwencja to fundament cyfryzacji uczelni

Dr hab. Danuta Zawadzka, prof. PK

Rektor Politechniki Koszalińskiej

Do priorytetów w obszarze cyfryzacji zaliczamy dalszą digitalizację obiegu dokumentów, wdrażanie kolejnych e-usług i dostosowywanie eksploatowanych systemów do przepisów prawa. Rok na pewno zostanie zapamiętany przez pryzmat e-doręczeń i uruchomienia KSeF. Nie można pominąć równie istotnych e-dyplomów czy testowania mikropoświadczeń.

Studenci zyskają zdalny dostęp do katalogu e-usług od składania wniosków, poprzez odbiór decyzji, zaświadczeń aż po pobieranie e-dyplomów. Uprości to formalności, zwiększy dostępność i transparentność, a studenci będą mogli sprawdzać status procedowania sprawy.

Z perspektywy pracownika dzięki ucyfrowieniu i automatyzacji procesów obiegu dokumentów zoptymalizuje (zmniejszy) się koszyk czynności powtarzalnych. Każde działanie związane z ucyfrowieniem procesu wpływa na uporządkowanie i dostosowanie wewnętrznych procedur organizacyjnych. Podkreślić trzeba także kontekst cyberbezpieczeństwa – poprawę bezpieczeństwa i rozliczalności działań dzięki elektronicznym śladom audytowym.

W procesie cyfryzacji najtrudniejsze to realizacja planu. W każdej organizacji wygląda to trochę inaczej. Dużo zależy od tego, na jakim poziomie cyfryzacji jest już dana organizacja. Z jakich systemów informatycznych korzysta? Czy jest przygotowana od strony formalno-organizacyjnej na zmiany? No i chyba najważniejszy w tym wszystkim jest każdy, niepowtarzalny i wyjątkowy użytkownik ze swoim bagażem doświadczeń i uprzedzeń, ale również zaskakujących pomysłów. Czy można to wszystko ze sobą połączyć? Czy uda się znaleźć choć jedno rozwiązanie dla tej układanki zależności, które pozwoli w perspektywie określonego czasu (np. roku) wdrożyć kolejną e-usługę?

Muszę powiedzieć, że cyfryzacja u nas rozpoczęła się prawie 25 lat temu, kiedy to w roku 2002 uruchomiliśmy nasz własny system informatyczny WirKa do obsługi kilku podstawowych procesów zarządczych w uczelni, tj. składanie zapotrzebowań na dostawy/usługi, delegacji czy umów zleceń. To i kolejne wdrożenia systemów informatycznych nauczyły nas, że w praktyce sprawdza się tylko elastyczne podejście i konsekwentne zarządzanie zmianą, a zdefiniowany plan działania i jego słuszne (w teorii) założenia w praktyce nie zawsze działają. Z naszej perspektywy coraz trudniejsze staje się utrzymanie porządku w architekturze integracji systemów informatycznych. Problem dostawców, standardów wymiany danych, czasu wykonania zmian, ale też jakości i oczywiście ponoszenia dodatkowych kosztów w coraz większym stopniu

wpływa na obciążenie wewnętrznych zespołów IT, jak również na uruchamianie nowych funkcjonalności w eksploatowanych systemach. Na drugim miejscu znajduje się oczywiście zmiana przyzwyczajeń i procedur. Dobrze znany jest wszystkim wzrost wolumenu wydruków papierowych po wdrożeniu elektronicznych obiegów dokumentów. Podsumowując, najważniejsi są ludzie, zarówno ci, którzy analizują, planują i wdrażają kolejne e-usługi, jak i użytkownicy korzystający z tych e-usług, a rolą zarządczą jest ciągłe balansowanie, elastyczne podejście do zmian, ale przede wszystkim konsekwentne dążenie do realizacji celu. Na koniec tylko wspomnę o coraz większym wpływie i wykorzystywaniu AI.

Relacje powinny być w centrum, technologia w tle

Marta Komor

Dyrektorka Działu Komunikacji i Obsługi
Uniwersytet SWPS

Z perspektywy obsługi i komunikacji mamy dwa najważniejsze cele strategiczne. Pierwszy z nich to dbanie o doświadczenie osób uczących się, personalizując obsługę i rozwijając wsparcie w toku edukacji, a drugi to zapewnienie naszej społeczności akademickiej efektywnego i przyjaznego systemu komunikacji wewnętrznej, opartego na narzędziach cyfrowych.

Masowość szkolnictwa wyższego i nadmiar biurokracji utrudniają budowanie relacji z osobami studiującymi i zapewnienie osobistego kontaktu. Projektując rozwiązania cyfrowe, chcemy zadbać o to, aby technologia odciążała zespoły i pozwoliła im pełnić rolę doradczą wobec studentów. Systemy mają rzeczywiście wspierać administrację akademicką, wydziały i osoby uczące się w pomyślnym funkcjonowaniu na uczelni, a nie stanowić jedynie kolejny format dla dotychczasowych rozwiązań manualnych czy papierowych.

W zgodzie z tymi celami od dawna wprowadzamy i udoskonalamy kolejne cyfrowe rozwiązania. Większość procesów i usług na uczelni prowadzimy w obiegu cyfrowym: od obiegu dokumentów i podpisów po obsługę spraw. Od 5 lat pracujemy przy wykorzystaniu CRM, który umożliwia automatyzację komunikacji i obiegu wszystkich spraw w toku studiów. Każde zapytanie natychmiast trafia do właściwej osoby w zespole obsługi, a gdy przychodzi do nas osoba studiująca z problemem, nie musimy się przeklikać przez pliki i repozytoria informacji studenckiej. Mając widok 360 historii studiowania każdej osoby, możemy od razu skupić się na udzieleniu pomocy. Sukcesywnie rozbudowujemy naszą zintegrowaną platformę edukacyjną o kolejne funkcjonalności wspierające obsługę wybranych procesów od multiwyszukiwarki informacji stanowiącej bazę wiedzy dla wszystkich osób studiujących i pracujących na uczelni, przez postępowania w trybie KPA, praktyki, wymianę międzynarodową, po dostosowania dla osób ze szczególnymi potrzebami i marketing automation. Obecnie

wprowadzamy rozwiązania AI w procesie obsługi, aby pomóc każdemu doradcy w każdym kampusie udzielać szybciej odpowiedzi na pytania studentów i studentek we wszystkich kategoriach w czasie rzeczywistym, automatycznie przeszukiwać przepastne regulaminy, zasady i statusy w toku studiów, aby zminimalizować przekierowanie spraw i skrócić czas reakcji.

Rosnąca liczba osób uczących się i pracujących ze specjalnymi potrzebami, zarówno osób z orzeczeniem o niepełnosprawności, jak i bez niego, ujawniła potrzebę dalszej modernizacji dostępności obsługi. Od początku tego roku wdrażamy zdigitalizowany system adaptacji w procesie studiowania, umożliwiający zgłoszenie, opracowanie i akceptację dostosowań na uczelni dla osób ze specjalnymi potrzebami. Każdy student i studentka może się zgłosić za pomocą formularza, który system kieruje do odpowiedniej osoby. Osoba studiująca szybciej otrzymuje odpowiedź, raport tłumaczący decyzję i wskazuje przysługujące udogodnienia. Wszyscy zyskują: studenci i studentki łatwo składają podanie, pracownicy mogą w krótszym czasie rozpatrzyć więcej zgłoszeń, a osoby prowadzące zajęcia wiedzą, jak dostosować proces kształcenia na swoich zajęciach do danych potrzeb.

Takie indywidualne podejście do każdej osoby jest dla nas niezwykle istotne i jest jednym z najważniejszych celów, o czym wspominałam wcześniej. Mamy sześć kampusów, łącznie blisko 16,4 tys. osób studiujących na studiach wyższych, 4,5 tys. na studiach podyplomowych, 69 doktorantów i doktorantek, dlatego spersonalizowane podejście do każdego, kto potrzebuje szybkiej pomocy w swojej sprawie, wymaga maksymalnego zautomatyzowania procesów. Chcemy, by nasi studenci i studentki mogli w pełni skupić się na nauce, a nie martwić się administracyjnymi sprawami. Dlatego dbamy o ich komfort zdobywania wiedzy na uczelni. Analizujemy ścieżki studiowania, dzięki czemu potrafimy zidentyfikować główne punkty zapalne i być gotowi na te wyzwania.

Na zmiany ustawowe i rozporządzenia zmierzające do transformacji cyfrowej jesteśmy gotowi w każdej chwili i często ich wyczekujemy. Przykładowo mLegitymacje na Uniwersytecie SWPS pojawiły się natychmiast, gdy tylko było to możliwe, to znaczy kiedy tylko powstały odpowiednie regulacje i mieliśmy pewność, że są bezpieczne. Podobnie czekaliśmy na rozporządzenie ws. e-dyplomów. Uczestniczyliśmy w zeszłym roku w Okrągłym Stole e-dyplomowym m.in. razem z przedstawicielami Ministerstwa Cyfryzacji, NASK-u i innych uczelni. To są właściwe kierunki rozwoju zgodne z unijną ideą Digital Campus, w którym wszystkie procesy – od rekrutacji po dyplom – odbywają się cyfrowo i w sposób zintegrowany.

Relacje powinny być w centrum, technologia w tle

Przy okazji warto zastanowić się nad końcowym celem cyfryzacji. Obecnie przepisy wymagają wprowadzenia wielu elektronicznych usług dla samej innowacji. Dublujemy rozwiązania, podczas gdy powinniśmy zastanawiać się, jak zdigitalizowane narzędzia mogą zastąpić swoje papierowe odpowiedniki, co ułatwi życie wszystkim osobom mającym do czynienia z uczelnianą administracją.

mLegitymacje są dobrym wzorem, bo są wydawane z automatu, a o plastikową kartę należy wnioskować. Często odgórnie proponowane regulacje i rozwiązania nie zastępują papieru czy pracy manualnej i stanowią kolejny format tego samego procesu obsługiwanego tradycyjnie. W niektórych przypadkach przepisy promują podejście digital first i to kierunek, w którym powinniśmy zmierzać. Jeśli jednak formaty analogowe: papier czy plastik będą dalej dopuszczane, to jak długo i na podstawie jakich kryteriów?

W procesie cyfryzacji na uczelniach są trzy największe wyzwania: procedury, czas i finanse.

Kiedy chcemy zdigitalizować czynność, która nie ma jednego, ustandaryzowanego procesu, to musimy go wspólnie wypracować, często metodą kompromisu. Wymaga to od nas wszystkich zmiany przyzwyczajeń, ale przy dobrze działającym nowym systemie widzimy więcej korzyści niż trudności.

Niekiedy to nie jest dobry moment na wprowadzenie danej zmiany, np. początek roku akademickiego to czas wzmożonej pracy, studenci i studentki chcą załatwić wiele spraw. Dlatego wtedy staramy się unikać wszelkich ingerencji w systemy i procesy.

Wreszcie finanse, najbardziej oczywiste wyzwanie. Zawsze analizujemy, jak cyfryzacja danego procesu wpisuje się w naszą strategię. Dopiero potem ustalamy priorytety wśród planowanych zmian.

Cyfryzacja ma porządkować, a nie kontrolować

Prof. dr hab. Radosław Dobrowolski

Rektor Uniwersytetu Marii Curie-Skłodowskiej w Lublinie

W Uniwersytecie Marii Curie-Skłodowskiej w Lublinie konsekwentnie łączymy akademicką tradycję z nowoczesnym podejściem do zarządzania i organizacji pracy. Jednym z filarów tej strategii jest rozbudowana, nowoczesna i stale rozwijana infrastruktura informatyczna, wspierająca kluczowe procesy administracyjne, dydaktyczne oraz badawcze. Systemy IT stanowią dziś integralny element obsługi Uczelni, zapewniając ciągłość działania w wielu obszarach i realnie wpływając na komfort pracy oraz studiowania.

Podczas planowania dalszego rozwoju w obszarze cyfryzacji administracji i obiegu dokumentów w 2026 roku jednym z naszych priorytetów będzie optymalizowanie procesów funkcjonujących na Uniwersytecie oraz ich integracja w ramach posiadanych już rozwiązań informatycznych.

Szczególne znaczenie ma produkcyjne uruchomienie systemu elektronicznego zarządzania dokumentacją (EZD RP), który umożliwi realizowanie blisko połowy spraw w pełni elektronicznie. Starannie zaplanowaliśmy i rozłożyliśmy w czasie jego wdrożenie, tak by stopniowo przygotować organizację i pracowników do trwałej zmiany sposobu pracy.

Jestem przekonany, że wprowadzenie EZD to jeden z najważniejszych kroków w modernizacji pracy administracyjnej – pomoże nam uporządkować obieg dokumentów, skróci czas realizacji spraw oraz zwiększy ich transparentność. Co istotne, system wybrany przez UMCS został opracowany i jest stale rozwijany przez NASK – Państwowy Instytut Badawczy, co dodatkowo wzmacnia zaufanie do tego rozwiązania.

Ważnym elementem cyfryzacji naszej Uczelni jest także rozwój wykorzystywanych systemów informatycznych, w szczególności platformy SAP. Aktualnie działania te koncentrują się na zapewnieniu pełnej obsługi Krajowego Systemu e-Faktur oraz dostosowaniu procesów finansowo-księgowych do zmieniających się wymogów prawnych. Dzięki funkcjonującym już na Uczelni rozwiązaniom w zakresie elektronicznych faktur oraz rozliczeń realizowanych w systemie SAP, wdrożenie KSeF nie będzie stanowiło tak dużego wyzwania, jak w podmiotach rozpoczynających ten proces od podstaw. Integracja SAP z KSeF będzie stanowiła raczej naturalne dopełnienie dotychczasowego modelu obsługi finansowo-księgowej. Nie mam wątpliwości, że podjęte działania bezpośrednio przełożą się na sprawność funkcjonowania administracji uczelnianej.

Równolegle rozwijamy system USOS, w którym coraz większy nacisk kładziemy na obsługę formalnej komunikacji elektronicznej pomiędzy Uczelnią a studentami oraz nauczycielami akademickimi. Dotyczy to w szczególności wdrażania rozwiązań związanych z elektronicznymi

doręczeniami (tzw. e-doręczeniami), umożliwiającymi przekazywanie pism i informacji w sposób bezpieczny i zgodny z obowiązującymi przepisami. Widzimy, że usprawniają one komunikację, zwiększają dostępność usług oraz ograniczają konieczność osobistych wizyt w jednostkach administracyjnych.

Z perspektywy studentów i pracowników cyfryzacja oznacza przede wszystkim uproszczenie procedur, skrócenie czasu obsługi spraw oraz większą przewidywalność procesów administracyjnych. Uzupełnieniem tych działań będzie uruchomienie nowego portalu internetowego UMCS, integrującego funkcje internetowe i intranetowe. Portal ten uporządkuje dostęp do e-usług, dokumentów i informacji, a jednocześnie wzmocni komunikację wewnętrzną i zewnętrzną Uczelni, budując spójne cyfrowe środowisko dla całej społeczności akademickiej.

Stale pamiętamy również o bezpieczeństwie cyfrowym. Żyjemy bowiem w czasach, w których ataki w przestrzeni wirtualnej stały się realnym narzędziem destabilizacji instytucji publicznych, w tym uczelni wyższych. Dlatego nie czekamy biernie na ostateczny kształt nowelizacji krajowych przepisów i naszą strategię działania opieramy bezpośrednio na wymogach europejskiej dyrektywy NIS 2, do której wdrażania przystąpiliśmy z wyprzedzeniem. Aby nadać tym procesom odpowiednią rangę, powołaliśmy w strukturze UMCS Biuro Bezpieczeństwa, które łączy kompetencje z zakresu cyberbezpieczeństwa i ochrony danych osobowych, oraz pracujemy nad Systemem Zarządzania Bezpieczeństwem Informacji (SZBI).

Wyzwaniem pozostaje koordynacja działań w tym obszarze pomiędzy wszystkimi jednostkami Uniwersytetu, a także podnoszenie świadomości wśród społeczności akademickiej na temat możliwych zagrożeń i zasad bezpieczeństwa informacji. Wprowadziliśmy dlatego cykliczne szkolenia z zakresu bezpieczeństwa cyfrowego, skierowane zarówno do pracowników, jak i studentów, oraz planujemy kolejne działania.

Jednym z najtrudniejszych aspektów cyfryzacji Uniwersytetu pozostaje jej wymiar zarządczy i kulturowy. Cyfrowe narzędzia mogą budzić obawy związane z nadmierną kontrolą pracy, śledzeniem obiegu dokumentów czy automatycznym rozliczaniem terminów. Chcę jednak jasno podkreślić, że celem cyfryzacji nie jest zwiększenie kontroli nad pracownikami, lecz uporządkowanie i przyspieszenie procesów, poprawa przejrzystości działań oraz realne odciążenie użytkowników systemów IT od powtarzalnych, manualnych czynności.

Istotnym wyzwaniem jest również pokusa prostego odtwarzania procesów papierowych w formie elektronicznej, bez ich rzeczywistego przeprojektowania. Nasze doświadczenia pokazują, że taka praktyka nie przynosi oczekiwanych efektów. Skuteczna cyfryzacja wymaga spojrzenia na procesy administracyjne od nowa – ich uproszczenia, eliminacji zbędnych kroków oraz jasnego określenia ról i odpowiedzialności, zanim zostaną one wsparte narzędziami informatycznymi. Kluczowe znaczenie ma tutaj współpraca pomiędzy jednostkami UMCS oraz systematyczne rozwijanie kompetencji cyfrowych użytkowników. To właśnie one decydują o bezpiecznym i efektywnym korzystaniu z systemów IT, które na naszej Uczelni są dziś nieodłącznym elementem codziennej pracy.

W praktyce najlepiej sprawdza się podejście ewolucyjne, oparte na pilotażach, dialogu z użytkownikami i konsekwentnym wyjaśnianiu sensu wprowadzanych zmian. Tak rozumiana cyfryzacja staje się nie tylko wdrażaniem technologii, lecz także realną transformacją sposobu funkcjonowania Uniwersytetu – transformacją, która wzmacnia potencjał UMCS i służy studentom, pracownikom oraz całej wspólnocie akademickiej.

Rozwiązania cyfrowe mają służyć człowiekowi, nie być celem samym w sobie

Ks. prof. dr hab. Ryszard Czekalski

Rektor Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Cyfryzacja administracji uczelni wyższych nie jest dziś jedynie kwestią technologii, lecz elementem odpowiedzialnego zarządzania społecznością akademicką oraz zapewnienia jej bezpieczeństwa i sprawności funkcjonowania. To niewątpliwie wyzwanie, choćby ze względu na różnice wieku interesariuszy systemów uczelnianych. Z jednej strony mamy wprawionych studentów, którzy od dziecka żyją w świecie cyfrowym, z drugiej zaś nieco starszych profesorów, którzy ten świat w zasadzie dopiero odkrywają i niekoniecznie chcą się przekonać do większego zaangażowania w przestrzeni „cyber". Oczywiście nie jest to reguła.

W perspektywie roku 2026 priorytety Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie w tym obszarze koncentrują się na dalszej integracji systemów informatycznych, rozwoju bezpiecznych usług elektronicznych oraz pełnej cyfryzacji obiegu dokumentów administracyjnych i studenckich.

Jednym z kluczowych kierunków działań jest konsekwentne wdrażanie elektronicznych procedur administracyjnych – od spraw studenckich, przez obsługę procesów kadrowych i finansowych, po zarządzanie dokumentacją uczelnianą.

Dzięki rozwiązaniom, które otrzymujemy także z administracji centralnej i rządowej, możliwe jest nie tylko skrócenie czasu realizacji spraw, ale również zwiększenie ich transparentności, dostępności i bezpieczeństwa. Z perspektywy studentów cyfryzacja oznacza przede wszystkim uproszczenie kontaktu z administracją uczelni, ograniczenie konieczności osobistych wizyt oraz możliwość załatwiania większości spraw w sposób zdalny, niezależnie od miejsca i czasu. Dla pracowników – zarówno akademickich, jak i administracyjnych – to większa spójność procesów, redukcja obciążeń biurokratycznych oraz lepsze narzędzia do pracy w środowisku rozproszonym. Nie bez znaczenia pozostaje także aspekt cyberbezpieczeństwa: nowoczesne systemy pozwalają skuteczniej chronić dane osobowe oraz inne wrażliwe informacje, co jest jednym z fundamentalnych obowiązków uczelni publicznej.

Doświadczenie UKSW pokazuje, że największym wyzwaniem w procesie cyfryzacji nie jest sama technologia, lecz aspekt zarządczy i organizacyjny. Zmiana utrwalonych przyzwyczajeń, procedur oraz sposobu myślenia o pracy administracyjnej bywa trudniejsza niż wdrożenie kolejnego systemu informa-

tycznego. Cyfryzacja wymaga ścisłej współpracy pomiędzy jednostkami organizacyjnymi, jasnego określenia odpowiedzialności oraz konsekwentnego przywództwa instytucjonalnego.

W praktyce najlepiej sprawdza się podejście ewolucyjne, oparte na dialogu, szkoleniach oraz stopniowym angażowaniu interesariuszy – od władz uczelni, przez kadrę kierowniczą, po pracowników i studentów. Kluczowe znaczenie ma także integracja systemów, tak aby użytkownik końcowy nie musiał poruszać się pomiędzy wieloma rozproszonymi narzędziami, lecz korzystał z jednego, spójnego środowiska cyfrowego. Cyfryzacja nie powinna bowiem komplikować funkcjonowania uczelni, lecz je porządkować i wzmacniać.

Uniwersytet Kardynała Stefana Wyszyńskiego traktuje cyfryzację jako proces długofalowy, wpisany w misję nowoczesnej, odpowiedzialnej i bezpiecznej uczelni, która łączy tradycję akademicką z wyzwaniami współczesnego świata. W tym sensie rozwiązania cyfrowe są narzędziem służącym człowiekowi i wspólnocie akademickiej, a nie celem samym w sobie.

Większość spraw powinna dać się załatwić zdalnie

Prof. dr hab. Michał Zasada

Rektor Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie

W 2026 roku priorytetem SGGW jest kompleksowa cyfryzacja administracji i obiegu dokumentów: powszechne wykorzystanie e-podpisu i e-pieczęci, wprowadzenie cyfrowych dyplomów oraz rozwój zintegrowanych e-usług dla studentów i pracowników.

Dążymy do tego, aby większość spraw można było załatwić zdalnie, szybciej i bez papieru, przy jednoczesnym wzmocnieniu cyberbezpieczeństwa oraz ochrony danych. Oznacza to krótsze procedury, większą przejrzystość i łatwiejszy dostęp do informacji. To kierunek działań, który konsekwentnie realizujemy w ramach przyjętej strategii rozwoju uczelni, z myślą o jej dalszym, stabilnym i odpowiedzialnym funkcjonowaniu.

Najtrudniejsze pozostają zmiana przyzwyczajeń i integracja systemów między jednostkami, dlatego stawiamy na dialog, szkolenia i etapowe wdrożenia. Ewolucyjny charakter tych działań nie oznacza jednak powolności – skala zagrożeń i tempo rozwoju technologii wymagają od uczelni zdecydowanych, szybkich decyzji i ciągłego nadążania za bezprecedensową dynamiką zmian.

Rozwiązania cyfrowe mają służyć człowiekowi, nie być celem samym w sobie

Dziś przewagę uczelni buduje dostęp do danych

Rozmowa z prof. Barbarą Jankowską, Rektor Uniwersytetu Ekonomicznego w Poznaniu

Cyfryzacja administracji na uczelniach coraz rzadziej jest dziś pojedynczym projektem, a coraz częściej długofalowym procesem zmian. Jakie są najważniejsze priorytety Uniwersytetu Ekonomicznego w Poznaniu w 2026 roku w obszarze cyfryzacji administracji i obiegu dokumentów, i co z perspektywy studentów oraz pracowników ma się dzięki nim realnie zmienić?

Cyfryzacja, która wpisuje się w unowocześnienie procesów badawczych i dydaktycznych, w sposób świadomy jest przez nas także wykorzystywana do usprawnienia działań administracyjnych w naszej Uczelni. W 2026 roku będziemy kontynuować już wcześniej podjęte działania związane z cyfryzacją i nakierowane na dalsze podniesienie sprawności działania naszego Uniwersytetu w wymiarze organizacyjno-administracyjnym.

Nasz Dział Technologii Informacyjnych realizuje prace programistyczne dotyczące przygotowywania nowych procesów w systemie Elektronicznego Obiegu Dokumentów (EOD). Jednocześnie, mając na uwadze zmiany w przepisach prawa, na bieżąco dostosowujemy funkcjonujące w Uczelni systemy informatyczne.

W systemie EOD mamy wdrożone ponad 100 obiegów, które są odbiciem analogicznych procesów wcześniej procedowanych w formie papierowej. Nasze statystyki pokazują, że mamy już wprowadzone ponad 250 000 dokumentów. Zestawiając ten wskaźnik dla 2025 roku i dla 2022 roku, okaże się, że liczba takich dokumentów wzrosła czterokrotnie. System uruchomiliśmy w 2021 roku.

Konsekwentnie dążymy do tego, aby cyfrowa transformacja wspierała także zieloną transformację. Zwiększające się wykorzystanie elektronicznego obiegu dokumentów w Uczelni wpłynęło na istotne ograniczenie liczby dokumentów powstających w wersji papierowej, co wpłynęło także na spadek liczby zamawianych ryz papieru.

Cyfryzacja pozwala nam nie tylko na usprawnienie obiegu dokumentów, ale także na skrócenie czasu realizacji wielu procesów. Tym, co obserwujemy w naszym Uniwersytecie, jest także poprawa efektywności pracy naszych pracowników i jednocześnie komfortu ich pracy. Warto także dodać, że posługując się EOD, zyskaliśmy też szansę lepszego monitoringu dokumentów.

W debacie o zarządzaniu uczelniami coraz częściej pojawia się teza, że realna przewaga konkurencyjna budowana jest dziś na danych. Jaką rolę odgrywają obecnie dane i analityka w funkcjonowaniu Uniwersytetu Ekonomicznego w Poznaniu?

Będąc Uczelnią, nie tylko w procesach ewaluacji, ale również akredytacji międzynarodowych rozwijamy i udoskonalmy systemy gromadzenia danych i raportowania. Mamy świadomość, jak ważne jest podejmowanie decyzji w oparciu o rzetelnie zbierane i przetwarzane dane, dlatego też w 2025 roku powołaliśmy Centrum Analityczne. To jednostka organizacyjna, która wspiera decyzje zarządcze w naszym Uniwersytecie.

Prowadzenie pogłębionych, wielowymiarowych analiz jest możliwe m.in. dlatego, że posługujemy się oprogramowaniem Microsoft PowerBI. Jak dotąd, przygotowanych zostało kilkanaście rozbudowanych raportów w kluczowych obszarach funkcjonowania Uczelni. Pozwalają one na szybkie przedstawienie niezbędnych informacji bez konieczności angażowania pracowników i żmudnej analizy danych.

Jako rektor Uniwersytetu Ekonomicznego w Poznaniu towarzyszy mi przekonanie, że w dzisiejszym świecie źródłem przewagi konkurencyjnej są dane i dostęp do danych pozwala najpierw projektować, a potem wdrażać adekwatne strategie.

Wiele uczelni deklaruje dziś, że cyfryzacja ma realnie poprawiać doświadczenie studentów i wykładowców, a nie tylko porządkować zaplecze administracyjne. Jak w praktyce wygląda to na Uniwersytecie Ekonomicznym w Poznaniu?

Cyfryzacja w obszarach bezpośrednio dotyczących naszych studentów to chociażby system USOS i platforma e-learningowa Moodle. System USOS ułatwia studentom codzienne funkcjonowanie, zapewniając dostęp do kluczowych informacji.

Platforma Moodle wspiera natomiast prowadzenie zajęć w formie zdalnej i hybrydowej. Umożliwia wykładowcom publikowanie materiałów dydaktycznych, tworzenie kursów, testów i zadań, a studentom zapewnia dostęp do zasobów edukacyjnych w jednym miejscu.

Traktując podnoszenie sprawności naszej Uczelni w obszarze administracji jako priorytet, konsekwentnie dążymy do wykorzystywania cyfryzacji w celu ułatwienia funkcjonowania Uniwersytetu tak dla studentów, jak pracowników. Intensywnie pracujemy nad rozwiązaniem, które wykorzystując sztuczną inteligencję, byłoby wsparciem w zakresie odnajdywania potrzebnych informacji w regulacjach wewnętrznych i zewnętrznych. Jednym z kluczowych zadań będzie także przygotowanie Uczelni do wydawania e-dyplomów.

Cyberbezpieczeństwo stało się jednym z kluczowych wyzwań uczelni – nie tylko technologicznych, ale także organizacyjnych i kulturowych. Czym dziś, w Pani ocenie, jest „bezpieczna uczelnia" w świecie cyfrowym i jak Uniwersytet Ekonomiczny w Poznaniu definiuje to pojęcie?

„Bezpieczna uczelnia" w świecie cyfrowym to uczelnia, którą charakteryzuje wysoki poziom cyberbezpieczeństwa i ochrony danych. Zatem ważna jest w tym momencie bezpieczna infrastruktura informatyczna, która zapewnia ciągłość kształcenia, ochronę własności intelektualnej, buduje zaufanie społeczności akademickiej i partnerów zewnętrznych.

W dobie transformacji cyfrowej, w której uczestniczymy i dalej chcemy uczestniczyć, jak też ogromnych wyzwań związanych z cyberatakami, podejście do bezpieczeństwa musi być kompleksowe. Wspomniana kompleksowość oznacza, że bezpieczeństwo stanowi zakorzeniony w Uczelni element funkcjonowania. Wspomniane zakorzenienie musi przejawiać się zarówno w wymiarze technologicznym, jak i organizacyjnym.

Bezpieczeństwo w świecie cyfrowym nabiera szczególnego znaczenia, gdy przetwarzamy dane osobowe czy dane wrażliwe, a takie procesy są udziałem uniwersytetów. Budowanie bezpiecznej uczelni w świecie cyfrowym to nie tylko działania kierownictwa uczelni i odpowiednich, dedykowanych tym zagadnieniom komórek organizacyjnych, ale także konsekwentne kształtowanie świadomości cyfrowej. To wiąże się chociażby z faktem odpowiedzialnego korzystania z technologii przez studentów i pracowników.

Dlatego też staramy się zapewniać dostęp do wiedzy na temat zagrożeń i bezpiecznego funkcjonowania w środowisku informatycznym. W Uczelni organizowane są szkolenia z tematyki cyberbezpieczeństwa, a także dot. świadomego korzystania z narzędzi sztucznej inteligencji. To jest bardzo duże wyzwanie, gdyż chodzi o bezpieczne, umiejętne i etyczne posługiwanie się tymi narzędziami. Przed takim wyzwaniem stają wszystkie uniwersytety. Uczestnicząc chociażby w konferencjach organizowanych przez międzynarodowe instytucje akredytujące i rozmawiając z rektorami praktycznie ze wszystkich stron świata, nie trudno dostrzec, że cyberbezpieczeństwo powiązane z wykorzystywaniem narzędzi sztucznej inteligencji stanowi wyzwanie dla wszystkich, stawiamy sobie podobne pytania i stajemy wobec podobnych dylematów. W naszej Uczelni zostały opracowane rekomendacje dla nauczycieli akademickich i studentów w odniesieniu do korzystania ze sztucznej inteligencji w procesie dydaktycznym, w tym w procesach pisania prac zaliczeniowych, licencjackich i magisterskich.

W miarę możliwości finansowych sukcesywnie też unowocześniamy infrastrukturę serwerową i sieciową, rozbudowujemy system kopii zapasowych wraz z tzw. środowiskiem odtworzeniowym, a także wdrażamy rozwiązania podnoszące poziom bezpieczeństwa na urządzeniach końcowych, w tym m.in. wdrożyliśmy usługę pozwalającą na kompleksowe zarządzanie komputerami firmowymi z poziomu centralnej konsoli administracyjnej oraz wieloskładnikowe uwierzytelnianie. Centralne zarządzanie komputerami umożliwia zdalne instalowanie aplikacji i ich aktualizację, konfigurowanie zabezpieczeń oraz zapewnienie spójnych ustawień na wszystkich urządzeniach.

Planując prace, Uczelnia korzysta także z wyników przeprowadzanych audytów bezpieczeństwa. Raporty i zalecenia poaudytowe - w tym np. dot. audytu zgodności UEP z wymogami unijnej dyrektywy NIS2 - stanowią ważne wytyczne do dalszych działań w obszarze poodnoszenia poziomu bezpieczeństwa UEP.

W wielu rozmowach z kadrą zarządzającą uczelniami pojawia się wątek, że największym wyzwaniem cyfryzacji nie jest technologia, lecz zmiana sposobu myślenia i przyzwyczajeń. Co z perspektywy zarządczej okazuje się dziś najtrudniejsze w procesie cyfryzacji uczelni?

Z perspektywy rektor Uczelni, która za najcenniejszy kapitał Uniwersytetu uznaje kapitał ludzki, chciałabym podkreślić, że zawsze zależy mi na tym, aby ostateczny kształt zmian wprowadzanych w Uczelni wyłaniał się z konstruktywnych dyskusji z pracownikami. Jeśli jednak chodzi o bezpieczeństwo Uczelni, w tym bezpieczeństwo cyfrowe, są obszary, w których dyskusja musi zostać zastąpiona dyrektywą. To trudne z perspektywy zarządczej. Dyrektywy wiążą się nierzadko ze zmianą przyzwyczajeń i nakłonieniem pracowników do nowych rozwiązań. Nie da się ukryć, że te, które dotyczą bezpieczeństwa cyfrowego, wymagają niekiedy większego zaangażowania pracowników, czasem rezygnacji z pewnego komfortu, podejmowania dodatkowych czynności. Ta zmiana przyzwyczajeń jest od strony zarządczej trudniejsza niż integracja w wymiarze technicznym.

Korzystając z dotychczasowych doświadczeń przykładamy dużą wagę do identyfikowania i przedstawiania korzyści wprowadzonych rozwiązań teleinformatycznych oraz prowadzenia transparentnej komunikacji. Ważne jest, aby pracownicy znali uzasadnienie dla wprowadzanych zmian. W obszarze związanym ze sztuczną inteligencją konieczne jest wypracowywanie rozwiązań zespołowo – zespół musi skupiać osoby aktywne zarówno w obszarze nauki, dydaktyki, jak i administracji, bo takie rozwiązania często dotykają przekrojowo różnych sfer w Uczelni. W przypadku wdrażania nowych usprawnień przygotowywane są szkolenia dla użytkowników, a także niezbędne instrukcje. Proces cyfryzacji Uczelni wymaga ciągłego doskonalenia, dlatego w zakresie rozwiązań teleinformatycznych dążymy do ciągłej optymalizacji.

Dziękuję za rozmowę.

Rozmawiała: Dorota Siudowska-Mieszkowska

Cyfryzacja uczelni to proces kulturowy, nie tylko technologiczny

Rozmowa z dr. hab. Bernardem Ziębickim, prof. UEK, Rektorem Uniwersytetu Ekonomicznego w Krakowie

Na wielu uczelniach cyfryzacja administracji przeszła już fazę pilotaży i pojedynczych wdrożeń. Coraz częściej mówimy dziś o dojrzałych systemach, które obejmują całe funkcjonowanie instytucji. Na jakim etapie znajduje się Uniwersytet Ekonomiczny w Krakowie i jakie priorytety stawia sobie na 2026 rok w obszarze cyfryzacji administracji i obiegu dokumentów w kontekście dalszego rozwoju całej uczelni?

W 2026 roku priorytety Uniwersytetu Ekonomicznego w Krakowie w tym obszarze wynikają z naturalnej ewolucji funkcjonującego już na naszej uczelni systemu Elektronicznego Obiegu Dokumentów (EOD), którego pierwsze moduły uruchomiliśmy ponad trzy lata temu. Przez ten czas system systematycznie ewoluował, obejmując kolejne obszary: od administracji i finansów, poprzez zarządzanie nauką, aż po dydaktykę. Dziś nasz EOD to już dojrzałe narzędzie, obsłu-

gujące złożone procesy, takie jak obieg faktur, korespondencja wewnętrzna i zewnętrzna czy elektroniczny obieg praktyk studenckich, który połączył studentów, uczelnię i pracowników w jednym, cyfrowym środowisku.

W 2026 roku naszym priorytetem będzie maksymalne upowszechnienie Elektronicznego Obiegu Dokumentów we wszystkich obszarach funkcjonowania uczelni. Chcemy, aby EOD stał się standardem codziennej pracy, co pozwoli nam w możliwie największym stopniu odejść od dokumentacji papierowej. Bardzo ważnym elementem tej strategii jest również konieczność pełnej integracji z systemami państwowymi: e-Doręczeniami czy KSeF (Krajowym Systemem e-Faktur).

W debacie o cyfryzacji administracji często pojawia się argument, że prawdziwą zmianę odczuwają dopiero użytkownicy końcowi – studenci i pracownicy. Jakie konkretne korzyści przynosi im dziś elektroniczny obieg dokumentów?

Liczę, że działania w tym zakresie przyniosą szereg korzyści naszej społeczności akademickiej. Jedną z nich z pewnością będzie odejście od ręcznego zbierania podpisów, czyli – kolokwialnie mówiąc – koniec z koniecznością „biegania z papierami". Dokumenty (faktury, podania, wnioski, umowy) przekazywane będą w zaprojektowanych obiegach, w których elektroniczne podpisy mogą być składane szybko i niezależnie od miejsca pobytu sygnatariusza.

Automatyzacja obiegów decyzyjnych istotnie wpływa na skrócenie czasu rozpatrywania spraw. System automatycznie przekazuje dokumenty pomiędzy kolejnymi etapami procesu oraz informuje użytkowników o przypisanych im zadaniach, co pozwala ograniczyć przestoje i eliminować tzw. wąskie gardła.

Dodatkowym efektem jest pełna transparentność procesu – użytkownicy mają stały wgląd w aktualny status swoich spraw, co sprzyja budowaniu zaufania do instytucji oraz wzmacnia poczucie sprawczości. Dla pracowników oznacza to ograniczenie obciążeń biurokratycznych na rzecz koncentracji na pracy merytorycznej, natomiast dla studentów – dostęp do nowoczesnego standardu obsługi, odpowiadającego realiom cyfrowego świata roku 2026.

Pojęcie „bezpiecznej uczelni" w świecie cyfrowym coraz częściej pojawia się w dyskusjach akademickich, ale bywa różnie rozumiane. Jak Uniwersytet Ekonomiczny w Krakowie definiuje dziś bezpieczeństwo w środowisku cyfrowym?

Pojęcie bezpiecznej uczelni w środowisku cyfrowym należy dziś rozumieć jako zrównoważony system rozwiązań organizacyjnych, technologicznych i edukacyjnych, uwzględniających specyfikę funkcjonowania wspólnoty akademickiej. Bezpieczeństwo informacji w uczelni ma charakter wielowymiarowy, ponieważ dotyczy grup o odmiennych kompetencjach cyfrowych, potrzebach oraz postawach wobec technologii. Szczególnym wyzwaniem pozostaje zróżnicowanie pokoleniowe – z jednej strony kadra akademicka o wysokim dorobku naukowym, często preferująca tradycyjne modele pracy, z drugiej zaś studenci, swobodnie funkcjonujący w środowisku cyfrowym, lecz nie zawsze w pełni świadomi konsekwencji związanych z ochroną danych.

Istotnym kontekstem jest również akademicka kultura otwartości, oparta na swobodnym dostępie do wiedzy i danych oraz na wymianie myśli. Wprowadzanie mechanizmów bezpieczeństwa nie powinno tej otwartości ograniczać, lecz wspierać ją poprzez rozwiązania proporcjonalne, transparentne i adekwatne do rzeczywistych zagrożeń.

Wiele strategii cyberbezpieczeństwa koncentruje się na narzędziach i procedurach. Jaką rolę odgrywa w tym wszystkim edukacja i kształtowanie postaw użytkowników?

Budowanie kultury odpowiedzialnego korzystania z danych wśród pracowników i studentów wymaga działań edukacyjnych dostosowanych do poszczególnych grup odbiorców. W odniesieniu do pracowników szczególne znaczenie mają szkolenia z zakresu higieny cyfrowej oraz bieżące wsparcie w korzystaniu z nowych narzędzi i procedur. W przypadku studentów skuteczniejsze mogą być z kolei działania warsztatowe z obszaru cyberbezpieczeństwa, ukazujące praktyczne aspekty zagrożeń, w tym ryzyka związane z manipulacją danymi czy bezkrytycznym wykorzystaniem narzędzi opartych na sztucznej inteligencji.

Kluczowym elementem systemu bezpieczeństwa informacji pozostaje jednak człowiek, dlatego sądzę, że istotne jest także promowanie postaw odpowiedzialności i gotowości do zgłaszania incydentów, zamiast koncentrowania się wyłącznie na mechanizmach restrykcyjnych. Odpowiedzialność za bezpieczeństwo i integralność danych powinna być postrzegana jako integralna część etosu akademickiego – zarówno w działalności naukowej, jak i w procesie kształcenia.

W dyskusjach o cyfryzacji uczelni często pada stwierdzenie, że technologia nie jest dziś największym problemem.

Co z perspektywy zarządczej okazuje się najtrudniejsze w przeprowadzaniu takich zmian?

Z perspektywy wieloletniego doświadczenia w cyfryzacji naszej uczelni można stwierdzić, że technologia, choć pozornie skomplikowana, nie stanowi głównego wyzwania. Integracja systemów informatycznych, w tym EOD, jest w gruncie rzeczy zadaniem inżynierskim, sprowadzającym się do prawidłowego doboru protokołów i interfejsów. Prawdziwe trudności mają charakter zarządczy i kulturowy.

Największym wyzwaniem pozostaje zmiana utrwalonych przyzwyczajeń oraz „niepisanych zasad" funkcjonowania uczelni. Wspólnota akademicka przyzwyczajona do tradycyjnych rytuałów pracy wymaga nie tylko opanowania nowych narzędzi, lecz przede wszystkim zmiany mentalności. Szczególnie trudne jest przekonanie pracowników, że cyfrowy ślad w systemie jest bardziej wiarygodny i bezpieczny niż fizyczny podpis, który od lat stanowił podstawę procedur.

Na ile te wyzwania wynikają także z konieczności porządkowania i przebudowy samych procedur, a nie tylko zmiany narzędzi?

W procesie projektowania elektronicznych ścieżek obiegu regularnie zderzamy się z zapisami, które są nieprzejrzyste, niekonsekwentne lub po prostu nie uwzględniają wszystkich możliwych scenariuszy i sytuacji nadzwyczajnych. System informatyczny wymaga logiki i jednoznaczności, co w praktyce oznacza konieczność uporządkowania lub przebudowy procesów, co naturalnie może spotykać się z pewnym oporem naruszającym w pewien sposób dotychczasowe poczucie bezpieczeństwa pracowników.

Dodatkowe utrudnienia wynikają z braku stabilności procedur i zmian organizacyjnych, nierozerwalnie związanych z cyklicznymi wyborami władz rektorskich. Każda modyfikacja struktury lub koncepcji zarządzania wymaga rekonfiguracji obiegów w systemie EOD, co sprawia, że cyfryzacja jest procesem ciągłym i wymaga nieustannej adaptacji do nowej architektury uprawnień i odpowiedzialności.

Wyzwania dotyczą także współpracy między jednostkami, które w wyniku cyfryzacji muszą zmieniać zakres obowiązków – niektóre przejmują nowe zadania, inne tracą dotychczasowe.

Najlepsze efekty osiąga się poprzez partycypacyjne modelowanie procesów. Zamiast przenosić istniejące, wadliwe procedury do systemu, należy je – wspólnie z pracownikami różnych szczebli – analizować i optymalizować. Widoczna korzyść, jaką stanowi uproszczenie procedur, eliminacja ręcznego zbierania podpisów i zwiększenie przejrzystości odpowiedzialności, przekształca początkowy opór w zaangażowanie. Kluczowe znaczenie ma także wsparcie władz uczelni, które jasno sygnalizuje odejście od „niepisanych zasad" na rzecz przejrzystych, cyfrowych standardów.

Dziękuję za rozmowę.
Rozmawiała: Dorota Siudowska-Mieszkowska

Cyberbezpieczeństwo – problem IT czy ryzyko strategiczne uczelni?

Poważny incydent cyberbezpieczeństwa rzadko wynika z jednego błędu w jednym systemie. Najczęściej jest skutkiem tego, jak informacje krążą między jednostkami uczelni – przez technologię, procedury i praktyki doraźne. Odpowiedzią nie są kolejne korekty ad hoc, lecz zrozumienie ryzyk poprzez analizę zbiorów danych, kanałów obiegu, odpowiedzialności i uprawnień. Nie po to, by dokumentować, ale by świadomie zarządzać ryzykiem. W warunkach rosnących zagrożeń, szybkich zmian technologicznych (AI) i regulacyjnych mapa ryzyk staje się jednym z kluczowych narzędzi ograniczania chaosu decyzyjnego.

Mapy ryzyk

Mapa ryzyk działa wtedy, gdy opisuje mechanizmy, które powtarzają się w wielu procesach. Wiele z tych procesów ma podobną strukturę niezależnie od wydziału, na przykład obsługa danych studenckich i obsługa dokumentacji projektowej. W projektach finansowanych zewnętrznie przebieg dokumentacji jest w dużej mierze narzucony przez instytucję finansującą, więc różnice między jednostkami częściej biorą się z narzędzi i praktyk obiegu dokumentów niż z samego procesu.

> Bezpieczeństwo informacji wymaga spójnych reguł na poziomie uczelni, ponieważ dane przechodzą między jednostkami.

Bezpieczeństwo informacji wymaga spójnych reguł na poziomie uczelni, ponieważ dane przechodzą między jednostkami. Praktyki zdecentralizowane działają, ale bez wspólnych zasad mogą powstać niespójne uprawnienia i równoległe obiegi danych. Zamiast opisywać każdy przypadek osobno, mapa ryzyk porządkuje procesy i pokazuje, gdzie ryzyko wynika z obiegu danych, a gdzie z uprawnień i wyjątków.

Weźmy na przykład taki mechanizm jak niekontrolowane kopie danych. Powstają wtedy, gdy informacja opuszcza repozytorium główne (np. bazę danych), w którym obowiązują zasady dostępu i okresy przechowywania, i zaczyna żyć jako plik na lokalnych dyskach twardych, czy jako załącznik w różnych skrzynkach e-mailowych, być może w różnych formatach plików, a może nawet jako wydruki w różnych biurach. W takiej sytuacji zanika właściciel kopii i znika reguła usuwania. Kopie pozostają dostępne dłużej niż zakładano i szerzej niż repozytorium źródłowe.

Drugi mechanizm to uprawnienia doraźne w przypadku prac różnych komisji, zastępstw, zadań okresowych. Czyli sytuacji, gdy dostęp do wrażliwych danych może być nadawany na krótkie okresy. Gdy zabraknie jasnej reguły wygaszania takich dostępów, uprawnienia w praktyce pozostają trwale jako ślad po dawnej roli, być może na pewnym etapie dawno zapomniane. To zwiększa liczbę osób, które mają wgląd do spraw, do których służbowo już nie wrócą. Jeżeli dostęp nie jest potrzebny do bieżącego zadania, powinien wygasać wraz z zakończeniem pracy.

> Dane mogą nie wyglądać na wrażliwe w tabeli, arkuszu kalkulacyjnym ani na wydruku, ale stają się takie przez treść sprawy.

Trzeci mechanizm to wrażliwość kontekstowa. Dane mogą nie wyglądać na wrażliwe w tabeli, arkuszu kalkulacyjnym ani na wydruku, ale stają się takie przez treść sprawy. Przykładem jest wniosek dotyczący zdrowia, dokumentacja konfliktu zawodowego, opis sytuacji rodzinnej albo materiał badawczy z udziałem ludzi, w tym dane medyczne. W takich sprawach

szkoda wynika z ujawnienia treści i okoliczności. Sam identyfikator (PESEL, imię i nazwisko) ma mniejsze znaczenie niż opis sytuacji.

Czwarty mechanizm to skupienie danych w jednym punkcie lub ich fuzja (konwergencja). Obrazowo taka sytuacja występuje, gdy informacje z różnych domen zbiegają się w jednym miejscu pracy, na przykład w jednej konkretnej sprawie, we wspólnym katalogu lub wątku mailowym. Błąd kontroli dostępu odsłania wtedy materiał z kilku procesów naraz, ponieważ granice między danymi dotyczącymi kadr, studentów i finansów przestają być rozdzielone. Jeden katalog, sprawa lub wątek mailowy gromadzi materiały z kilku procesów. Mapa ryzyk ma wskazać miejsca, w których sytuacja taka może pojawiać się regularnie i może być trudna do wyeliminowania. Ma też przypisać właściciela reguł dostępu oraz ustalić minimalne standardy pracy z dokumentami w tych miejscach, w tym sposób wycofywania dostępu po zakończeniu zadania. Środkiem łagodzącym tu może być budowa świadomości i edukacji, ale to już w konkretnych jednostkach i małych zespołach, a nie na poziomie centralnym uczelni.

Pierwszy z zarysowanych elementów opisuje zbiory danych i procesy, w których są używane. Drugi opisuje usługi i miejsca przechowywania, w tym narzędzia chmurowe i współpracę zewnętrzną. Trzeci opisuje role i uprawnienia, łącznie z kontami administracyjnymi oraz kontami serwisowymi używanymi przez systemy do automatycznej wymiany danych między aplikacjami, bez udziału człowieka. Czwarty opisuje wyjątki, czyli sytuacje, w których praca odbywa się poza standardowym obiegiem.

Mapa ryzyk ma sens wtedy, gdy jest aktualizowana przy zmianach procesów i narzędzi. W przeciwnym razie pozostaje arkuszem, który nie ma związku z praktyką i z rzeczywistością. Mapa nie jest jedynie kwestią czysto techniczną (bezpieczeństwo IT), to szerszy proces zarządzania ryzykiem. Mapa ryzyk to także przydatne narzędzie przy wdrożeniach, które zmieniają mechanizm zarządzania informacją, na przykład przy podpisie elektronicznym i cyfryzacji dokumentów studenckich.

Narzędzia AI wprowadzają dodatkowy kanał przetwarzania informacji wpisywanych przez pracowników i studentów. W mapie ryzyk trzeba przypisać, w których procesach dopuszcza się użycie takich narzędzi, jakie kategorie danych mogą do nich trafiać oraz gdzie obowiązuje zakaz wprowadzania danych ze względu na treść spraw.

Grupy danych i konteksty przetwarzania

- **Tożsamość cyfrowa i dostęp**

Tożsamość cyfrowa dotyczy konta, ról, grup uprawnień, także procesów takich jak zasady resetów haseł, rejestry logowań (kto, kiedy, skąd), informacje o urządzeniach używanych do logowania. Ryzyko w tym obszarze zależy od szerokości uprawnień i od tego, czy konto daje dostęp do zasobów wspólnych oraz danych przekrojowych. Przejęcie konta o szerokich uprawnieniach może nawet zatrzymać pracę procesu. Największe konsekwencje występują w następstwie przejęcia kont, które mają dostęp do repozytoriów dokumentów oraz do ustawień udostępnień w przestrzeniach współdzielonych.

- **Komunikacja i współdzielenie pracy**

Z punktu widzenia mapy ryzyk ważne jest, że korespondencja bywa miejscem, gdzie gromadzone są dokumenty z różnych procesów, a dostęp do nich bywa szerszy niż dostęp do repozytorium źródłowego (np. bazy danych), w którym dokument powstał. Błędy w obiegu poczty często mają postać nadmiarowego udostępnienia. Przykładem może być przekazanie wątku e-mailowego razem z załącznikiem zawierającym czyjś dokument tożsamości. Taki błąd jest trudny do cofnięcia, bo kopie trafiają do wielu skrzynek.

Z kolei w chmurze i narzędziach współpracy ryzyko zależy od sposobu udostępniania. Przestrzenie robocze tworzone na potrzeby zespołów projektowych są koniecznością. Lecz pojedyncze udostępnienie może przerodzić się w trwałą ekspozycję. Na przykład gdy link do dokumentu pozwala na jego otworzenie przez „każdego z linkiem", w dodatku został utworzony na czas prac, a pozostaje aktywny miesiące czy lata po ich zakończeniu… W cyfrowych narzędziach współpracy da się wymusić ograniczenia czasu udostępnienia i wymóg przeglądu dostępów. Z nieformalnymi wydrukami jest trudniej.

Mapa ryzyk to także przydatne narzędzie przy wdrożeniach, które zmieniają mechanizm zarządzania informacją, na przykład przy podpisie elektronicznym i cyfryzacji dokumentów studenckich.

- **Dokumenty i sprawy**

Repozytoria spraw i obieg dokumentów zbierają decyzje, protokoły, pełnomocnictwa, korespondencję urzędową i inne detale. I to w tym obszarze treść bywa wrażliwa kontekstowo, ponieważ dokumenty opisują sytuacje osobiste albo sporne.

Obieg dokumentów ma też konsekwencje formalne. Konta używane do podpisu elektronicznego i autoryzacji dokumentów mają inny profil ryzyka niż zwykłe konta użytkowników. Nadużycie może prowadzić do kwestionowania ważności dokumentów.

- **Cykl życia studenta**

> Konta używane do podpisu elektronicznego i autoryzacji dokumentów mają inny profil ryzyka niż zwykłe konta użytkowników.

Rekrutacja jest procesem masowym. Dawniej sprzyjało to tworzeniu zestawień roboczych i szybkiemu przekazywaniu dokumentów w komisjach lub między ludźmi, zwłaszcza gdy procedury były obciążone terminami i odwołaniami. Tok studiów i dokumentacja decyzji administracyjnych wymagają stabilnej integralności danych. W wielu uczelniach działają dojrzałe systemy obsługi toku studiów, co ogranicza ryzyko problemów i wprowadza standardy. Nie eliminuje to ryzyka wynikającego z lokalnych integracji i lokalnych dodatków, działań niestandardowych.

- **Kadry i finanse**

Kadry i płace obejmują wynagrodzenia, dane bankowe, dane podatkowe, umowy oraz dokumenty w załącznikach. Ryzyko tutaj obejmuje zarówno szkody osobiste po ujawnieniu, jak i możliwości wykorzystania informacji do oszustw. W mapie ryzyk liczą się punkty, w których dokumenty przechodzą przez obieg – do ich akceptacji.

- **Badania, granty i dane regulowane**

W obszarze badań i projektów ryzyko wynika głównie z obiegu dokumentacji między organizacjami. Dokumentacja projektowa zawiera budżety, harmonogramy, role w zespole, dane partnerów, korespondencję oraz materiały robocze. W mapie ryzyk należy opisać kanały współpracy zewnętrznej i to, jak wygląda dostęp w konsorcjach, ponieważ dokumenty krążą między organizacjami i bywają przechowywane równolegle w kilku miejscach.

Osobny profil ryzyka mają badania z udziałem ludzi. Zwłaszcza te o charakterze medycznym. Ujawnienie danych uczestników może prowadzić do wstrzymania pracy badawczej, sporów z komisjami etycznymi, a być może nawet roszczeń. Skutki mogą objąć też relacje z partnerami i instytucjami finansującymi. W takim badaniu zwykle istnieje warstwa danych analitycznych oraz warstwa danych identyfikujących uczestnika. Nawet jeśli w zbiorze analitycznym nie ma imienia i nazwiska (w użyciu jest pseudonimizacja), to powiązanie z konkretną osobą bywa możliwe, gdy ktoś niepowołany uzyska dostęp do materiałów rekrutacyjnych, dokumentacji zgód, harmonogramów wizyt, korespondencji z uczestnikiem albo do pliku, który odwzorowuje identyfikator badawczy na dane osobowe. W specjalistycznej mapie ryzyk trzeba więc opisać, jak przechowywane są takie tabele lub pliki wiążące identyfikator badawczy z osobą, kto ma do nich dostęp, jak wygląda nadawanie i wygaszanie uprawnień w zespole oraz jak dokumentowane jest pobieranie kopii do analiz.

> Mapa ryzyk nie powinna ograniczać się do tego, czy coś wolno, a bardziej opisywać mechanikę.

Kluczowe jest też wskazanie zasad udostępniania danych poza zespół, na przykład do podwykonawców analiz, partnerów naukowych albo jednostek klinicznych.

W tym miejscu mapa ryzyk nie powinna ograniczać się do tego, czy coś wolno, a bardziej opisywać mechanikę. Czyli jakim kanałem dane są przekazywane? Gdzie są przechowywane, kto może je dalej udostępniać i w jaki sposób kończy się dostęp po zakończeniu współpracy?

- **Zmiany regulacyjne**

W tle są zmiany w RODO, które przełożą się na to, jak uczelnia opisuje zbiory danych i jak rozdziela odpowiedzialność. W tym miejscu zamiast dodatkowych "szkoleń z RODO", lepszym rozwiązaniem byłoby porządkowanie praktyk, które i tak są potrzebne do zarządzania ryzykiem. Jeżeli nowe przepisy doprecyzują status i zastosowania pseudonimizacji, uczelnia skorzysta tylko wtedy, gdy ma opisane sposoby stosowania tego podejścia.

- **Dostępność usług i odtwarzanie**

Ryzyko dostępności polega na tym, czy procesy mogą wrócić do pracy po awarii lub incydencie. W mapie ryzyk trzeba powiązać usługi z procesami i opisać kolejność odtwarzania i zależność procesów od usług. Procesy wskazują kolejność przywracania i tolerancję na przestój, co pozwala przełożyć to na realia funkcjonowania uczelni. Samo przywracanie z kopii zapasowych powinno być testowane i realizowane przez dedykowane zespoły IT.

Jak mówić o ryzyku?

Opis ryzyka powinien opierać się na procesach, danych, odpowiedzialnościach i kanałach obiegu informacji. W takiej formie ryzyko jest porównywalne między jednostkami i da się ustawiać priorytety bez rozbudowy dokumentów.

Na końcu pozostaje też element komunikacji. Jak mówić o ryzyku bez szkodzenia sprawie, bez wzbudzania poczucia, że to kolejne środki biurokratyczne i szkolenia, które trzeba odhaczyć?

Dr Łukasz Olejnik

Niezależny badacz i konsultant. Visiting Senior Research Fellow Wydziału Studiów nad Wojną King's College London. Był doradcą cyberwojny w Międzynarodowym Komitecie Czerwonego Krzyża. Doktorat (w INRIA), LL.M. w Information Technology Law (Uniwersytet Edynburski). Przewodniczący Komitetu Sterującego programu badawczego NCBiR „CyberSecIdent – cyberbezpieczeństwo i tożsamość". Autor publikacji naukowych, raportów, książek „Filozofia cyberbezpieczeństwa" i „Propaganda". Autor cyklu „Cyberpolityka" w Dzienniku Gazecie Prawnej. Komentował w mediach krajowych (Dziennik Gazeta Prawna, Gazeta Wyborcza) i międzynarodowych (New York Times, Washington Post, Financial Times). Prowadzi wykłady z cyberbezpieczeństwa, technologii, operacji informacyjnych (dezinformacji) – zarówno na poziomie technicznym (informatyka, cyberbezpieczeństwo), jak i społecznym (bezpieczeństwo narodowe, stosunki międzynarodowe). Otwarty na współpracę dydaktyczną z polskimi uczelniami: me@lukaszolejnik.com.

Cyfryzacja uczelni w praktyce

Jak cyfryzacja wygląda w praktyce wdrożeniowej? Zapytaliśmy ekspertów firm technologicznych, które od lat realizują projekty cyfryzacyjne na uczelniach publicznych i niepublicznych. To partnerzy wdrożeniowi uczestniczący w całym cyklu zmian: od analizy procesów, przez projektowanie obiegu dokumentów, po integrację systemów, szkolenia użytkowników oraz rozwiązywanie problemów pojawiających się już po uruchomieniu systemów.

Ich wypowiedzi pokazują, że największe wyzwania cyfryzacji rzadko mają charakter stricte technologiczny. Znacznie częściej wynikają z niespójnych procedur, niejasnego podziału odpowiedzialności, równoległego funkcjonowania obiegów papierowych i elektronicznych i nieprecyzyjnego zarządzania uprawnieniami. W efekcie cyfryzacja okazuje się wyzwaniem organizacyjnym w większym stopniu niż technologicznym.

Prezentujemy te głosy nie jako uniwersalne recepty, lecz jako zapis doświadczeń z projektów realizowanych w różnych modelach organizacyjnych. Razem tworzą one obraz cyfryzacji „od kuchni", z jej ograniczeniami, kompromisami i dobrymi praktykami, które pozwalają uczelniom przejść od technologicznej zmiany do trwałej poprawy jakości zarządzania dokumentami i informacją.

Technologia nie zastąpi świadomości użytkowników

Marcin Dudek

kierownik CERT Polska

Instytucje edukacyjne są miejscem szczególnie ważnym w kontekście cyberbezpieczeństwa. Poufność, integralność i dostępność danych należących do uczelni, ich pracowników i studentów stanowi podstawę zaufania społecznego, którym placówki te zasłużenie się cieszą. Dlatego tak ważna jest ich obrona – inwestycje w narzędzia i specjalistów z dziedziny cyberbezpieczeństwa, rozwój kierunków studiów w tym zakresie, ale też codzienne działania.

Doświadczenie z obsługi incydentów uczy, jak ważne są wykonywane na czas aktualizacje, aktualne i odseparowane kopie zapasowe, odpowiednia segmentacja sieci, czy monitorowanie zdarzeń na urządzeniach w organizacji. Te wszystkie mechanizmy nie wyręczą jednak użytkownika w dbaniu o cyberbezpieczeństwo, mogą go tylko wspomóc. Niezbędna jest edukacja, świadomość ryzyka i potrzeby wdrażania rozwiązań takich jak dwuetapowe uwierzytelnianie.

Cyfrowy obieg dokumentów jest naturalnym etapem rozwoju instytucji. Podpisy i pieczęcie elektroniczne ułatwiają funkcjonowanie, a jednocześnie stanowią lepsze zabezpieczenie niż ich tradycyjne odpowiedniki, pod warunkiem, że są poprawnie użytkowane. Podczas analizy incydentu zazwyczaj znajdujemy błędy, za które odpowiedzialny jest tzw. czynnik ludzki – czy to bezpośrednio, poprzez udział w scenariuszu phishingowym, czy pośrednio, na przykład poprzez zaniedbanie aktualizacji systemu lub zostawienie niezabezpieczonego wektora wejścia dla atakujących. Tego czynnika nie da się w zupełności wyeliminować technologią, a wręcz nie powinniśmy do tego dążyć, zamiast tego należy wyrabiać wśród użytkowników właściwe instynkty i rozwijać procedury wykrycia i reakcji na incydent.

CERT Polska udostępnia bezpłatne narzędzia, których wdrożenie może wesprzeć instytucje w zabezpieczaniu infrastruktury. Narzędzia te są dostępne w portalu moje.cert.pl dla wszystkich podmiotów, niezależnie od ich wielkości. Po dodaniu i zweryfikowaniu domeny oraz zakresów adresacji IP organizacja może m.in. korzystać z regularnego skanowania stron pod kątem podatności, otrzymywać informacje o infekcjach i wyciekach haseł, a także — od niedawna — analizować widok organizacji z perspektywy atakującego. W serwisie publikowane są również komunikaty bezpieczeństwa, ostrzegające przed aktualnie wykorzystywanymi scenariuszami oszustwo raz nowo ujawnianymi podatnościami. Upowszechnienie wykorzystania tych bezpłatnych narzędzi może stanowić istotny krok w kierunku poprawy cyberbezpieczeństwa środowiska akademickiego.

O sukcesie cyfryzacji decyduje rektor, a nie system

Łukasz Nowak

prezes zarządu PCG Academia,
partnera premium WEBCON

O sukcesie elektronicznego obiegu dokumentów nie decyduje samo wdrożenie systemu, lecz zestaw świadomych decyzji podejmowanych na poziomie rektora i kanclerza – wynika z doświadczeń PCG Academia, firmy od lat specjalizującej się w cyfryzacji uczelni wyższych, partnera premium WEBCON. To one przesądzają, czy cyfryzacja realnie upraszcza pracę administracji, zwiększa bezpieczeństwo informacji i wspiera rozwój uczelni, czy pozostaje jedynie technologiczną zmianą bez trwałego efektu organizacyjnego.

Nasze doświadczenia z kilkudziesięciu wdrożeń WEBCON na uczelniach publicznych i niepublicznych, a także w instytucjach sektora publicznego pokazują wyraźnie, że elektroniczny obieg dokumentów musi być traktowany jako **projekt zarządczy**, a nie wyłącznie informatyczny. Uczelnie, w których projekt ma silne wsparcie władz rektorskich i kanclerskich oraz jest osadzony w strategii rozwoju i bezpieczeństwa informacyjnego, osiągają zdecydowanie wyższy poziom dojrzałości cyfrowej.

> Elektroniczny obieg dokumentów musi być traktowany jako projekt zarządczy, a nie wyłącznie informatyczny ponieważ realnie zmienia sposób funkcjonowania całej instytucji.

Standaryzacja i odpowiedzialność jako fundament

Jedną z najważniejszych decyzji podejmowanych na poziomie centralnym uczelni jest **ustanowienie jednoznacznych standardów organizacyjnych**, które system obiegu dokumentów ma egzekwować. Dotyczy to w szczególności jasnego przypisania ról i odpowiedzialności. Każdy proces realizowany w WEBCON – od spraw studenckich, przez kadry, finanse, po decyzje strategiczne – powinien mieć formalnego właściciela odpowiedzialnego za jego przebieg, aktualność oraz zgodność z regulacjami wewnętrznymi i zewnętrznymi.

Z perspektywy bezpieczeństwa kluczowe znaczenie ma także **centralna polityka uprawnień**, oparta na zasadzie minimalnego dostępu. Konsekwentnie rekomendujemy uczelniom odejście od nieformalnych praktyk udostępniania dokumentów na rzecz precyzyjnie zdefiniowanych ról procesowych, wspieranych przez mechanizmy platformy WEBCON. Takie podejście

> Z perspektywy bezpieczeństwa kluczowe znaczenie ma centralna polityka uprawnień.

znacząco ogranicza ryzyko nieautoryzowanego dostępu do danych wrażliwych oraz ułatwia spełnienie wymogów audytowych.

Logowanie, audyt i integracje – decyzje, które robią różnicę

Nie mniej istotne są decyzje dotyczące standardów uwierzytelniania i logowania. Integracja systemu obiegu dokumentów z centralnymi mechanizmami tożsamości (SSO, Acti Każdy proces realizowany w WEBCON e Directory) powinna być traktowana jako element polityki cyberbezpieczeństwa uczelni, szczególnie w kontekście rosnącej roli e-podpisu, e-pieczęci oraz dokumentów cyfrowych, takich jak elektroniczne dyplomy.

WEBCON zapewnia pełną audytowalność procesów – każdy etap obiegu dokumentu jest rejestrowany, a ślad decyzyjny pozostaje jednoznaczny i niepodważalny. Warunkiem wykorzystania tej przewagi jest jednak decyzja władz uczelni o obligatoryjnym korzystaniu z systemu i rezygnacji z równoległego obiegu papierowego, który w praktyce osłabia zarówno efektywność, jak i bezpieczeństwo.

Równie ważnym elementem jest **integracja systemowa**. Elektroniczny obieg dokumentów powinien stanowić centralny komponent ekosystemu IT uczelni, współpracujący z systemami dziekanatowymi, kadrowo-płacowymi, finansowymi oraz narzędziami do podpisu elektronicznego.

Dojrzałość organizacyjna i wybór partnera

Cyberbezpieczeństwo w cyfrowym obiegu dokumentów nie jest wyłącznie efektem zastosowanych technologii, lecz konsekwencją dojrzałości organizacyjnej uczelni oraz głębokiego zrozumienia procesów akademickich, uwarunkowań prawnych i realiów funkcjonowania uczelni po stronie partnera wdrożeniowego. Dzięki temu cyfryzacja staje się narzędziem budowy nowoczesnej, bezpiecznej i efektywnej uczelni – a nie jedynie kolejnym projektem informatycznym.

> Elektroniczny obieg dokumentów powinien stanowić centralny komponent ekosystemu IT uczelni, współpracujący z systemami dziekanatowymi, kadrowo-płacowymi, finansowymi oraz narzędziami do podpisu elektronicznego.

„To fascynująca książka pokazująca, jak można dzisiaj myśleć o instytucjach szkolnictwa wyższego w nowym kontekście technologicznej rewolucji – radykalnie zmieniającej podstawy funkcjonowania”.

prof. dr hab. Marek Kwiek,
dyrektor Centrum Studiów Zaawansowanych w Naukach Społecznych i Humanistycznych UAM w Poznaniu

Cyfryzacja dokumentów na uczelni: bezpieczeństwo zaczyna się od procesów

Radosław Cichoń

ekspert ds. rozwiązań IT dla uczelni
OPTeam S.

Cyfryzacja obiegu dokumentów na uczelniach, obejmująca e-usługi, podpis elektroniczny oraz systemy EZD, jest dziś procesem nieuniknionym. Z naszych doświadczeń, zdobytych w trakcie wieloletniej współpracy z uczelniami publicznymi i niepublicznymi, wynika jednak jasno, że samo wdrożenie technologii nie przekłada się automatycznie na poprawę bezpieczeństwa danych i dokumentów. Kluczowe są konkretne, często stosunkowo proste działania organizacyjne i techniczne, które przynoszą najszybsze i realne efekty.

Bezpieczeństwo zaczyna się od tożsamości

Jednym z najważniejszych działań jest uporządkowanie i ujednolicenie zasad zarządzania tożsamością i uprawnieniami użytkowników. W praktyce oznacza to integrację systemów z centralnym mechanizmem uwierzytelniania, wdrożenie zasady minimalnych uprawnień oraz regularne przeglądy ról i dostępów.

Z doświadczeń wdrożeniowych na uczelniach wynika, że już samo odejście od kont współdzielonych i nadawania szerokich uprawnień znacząco ogranicza ryzyko nieautoryzowanego dostępu do dokumentów wrażliwych, takich jak akta osobowe, dokumentacja studencka czy dane finansowe.

> Samo odejście od kont współdzielonych i nadawania szerokich uprawnień znacząco ogranicza ryzyko nieautoryzowanego dostępu do dokumentów wrażliwych, budując kulturę odpowiedzialnego zarządzania dostępem do danych.

Proces przed technologią

Drugim obszarem, który najszybciej poprawia poziom bezpieczeństwa, jest standaryzacja procesów przed ich cyfryzacją. Uczelnie, które najpierw porządkują procedury administracyj-

ne, a dopiero potem odwzorowują je w systemach IT, znacznie rzadziej popełniają błędy skutkujące wyciekiem danych lub chaosem informacyjnym. Doświadczenia uczelni pokazują, że bezpieczeństwo danych zaczyna się na poziomie procesu, a nie samej technologii – jasno określone role, punkty decyzyjne i odpowiedzialności ograniczają ryzyko incydentów nawet przy bardzo rozbudowanym obiegu dokumentów. W tym kontekście ogromne znaczenie mają nowoczesne platformy low-code, takie jak nAxiom, które umożliwiają szybkie i bezpieczne modelowanie procesów uczelnianych bez konieczności tworzenia dedykowanego oprogramowania od podstaw.

> Bezpieczeństwo danych zaczyna się na poziomie procesu, a nie samej technologii.

Z naszych doświadczeń wynika, że zastosowanie low-code pozwala uczelniom na bieżąco dostosowywać obiegi dokumentów do zmieniających się przepisów, regulaminów czy nawet struktury organizacyjnej – bez konieczności „obchodzenia" systemów poza kontrolą IT. Standaryzacja procesów realizowana w jednym, centralnym narzędziu znacząco zmniejsza ryzyko błędów ludzkich oraz niekontrolowanego przetwarzania danych. Platformy, takie jak nAxiom, mają również istotny wpływ na bezpieczeństwo dzięki wbudowanym mechanizmom kontroli dostępu, audytowalności i wersjonowania procesów. Każda zmiana w obiegu dokumentów jest rejestrowana, a uprawnienia użytkowników mogą być precyzyjnie przypisane do ról i etapów procesu. To szczególnie ważne w środowisku akademickim, gdzie struktura organizacyjna jest bardzo często dość złożona.

Kolejnym istotnym elementem jest świadome i poprawne wykorzystanie podpisu elektronicznego oraz pieczęci elektronicznej. Wdrożenia realizowane przez OPTeam pokazują, że integracja e-podpisu z systemami EZD i platformami low-code eliminuje potrzebę przesyłania dokumentów poza systemem (np. e-mailem), co znacząco poprawia integralność i poufność danych. Automatyzacja podpisywania dokumentów w ramach procesu zmniejsza także ryzyko błędów proceduralnych i nieuprawnionych modyfikacji.

Cyfryzacja to nie tylko IT

Równie ważnym, a często niedocenianym czynnikiem, są regularne szkolenia użytkowników. Nawet najlepiej zaprojektowany system nie zapewni bezpieczeństwa, jeśli pracownicy nie rozumieją zasad bezpiecznej pracy z dokumentami elektronicznymi.

W praktyce to krótkie, praktyczne szkolenia połączone z intuicyjnymi narzędziami znacząco redukują liczbę incydentów bezpieczeństwa i zwiększają akceptację cyfrowych procesów przez pracowników. Najczęściej chyba popełnianym błędem jest traktowanie cyfryzacji wyłącznie jako projektu IT. Skutkuje to wdrożeniem systemów bez realnego zaangażowania administracji, archiwum, inspektora ochrony danych czy kadry zarządzającej.

> Najczęściej popełnianym błędem jest traktowanie cyfryzacji wyłącznie jako projektu IT.

Kolejnym błędem, jaki można przytoczyć, jest kopiowanie papierowych procedur do systemów informatycznych bez ich uproszczenia, co prowadzi do obchodzenia systemów i powstawania niekontrolowanych obiegów. Często brakuje także spójnej architektury procesowej oraz narzędzi, które pozwalałyby ją rozwijać w sposób bezpieczny, systemowy i kontrolowany.

Podsumowując, doświadczenia OPTeam pokazują, że najszybszą i najbardziej trwałą poprawę bezpieczeństwa danych na uczelniach przynoszą: uporządkowanie uprawnień, standaryzacja procesów, właściwe użycie e-podpisu, edukacja użytkowników oraz szerokie wykorzystanie platform Low-Code, takich jak nAxiom. To właśnie one stają się dziś fundamentem bezpiecznej, elastycznej i długofalowej cyfryzacji obiegu dokumentów w szkolnictwie wyższym.

E-podpis i e-pieczęć na uczelni: najczęstsze ryzyka i błędy

Agnieszka Bocian

Project and Business Development Manager
SIGNIUS SA

Wdrażanie e-podpisu i e-pieczęci na uczelni to nie tylko projekt technologiczny, ale przede wszystkim zmiana organizacyjna. Jeśli zostanie niewłaściwie zaprojektowana, może prowadzić do nadużyć, chaosu kompetencyjnego i utraty zaufania do cyfrowych procesów.

Z doświadczeń w cyfryzacji podpisywania dokumentacji akademickiej wynika, że najczęstsze ryzyka są powtarzalne i możliwe do wyeliminowania, o ile uczelnia już na starcie ustali jasne zasady jako standard.

Niejasne role i odpowiedzialności

Pierwszym i najczęstszym problemem są niejasne role i odpowiedzialności. Uczelnia musi jednoznacznie określić, kto jest uprawniony do składania podpisu elektronicznego (kwalifikowanego lub zaawansowanego), a kto do używania e-pieczęci instytucjonalnej. Te dwa narzędzia pełnią różne funkcje prawne – podpis zawsze identyfikuje osobę fizyczną, a pieczęć reprezentuje organizację. Brak tej granicy prowadzi do sytuacji, w której dokumenty są podpisywane np. przez niewłaściwe osoby.

> Uczelnia musi jednoznacznie określić, kto jest uprawniony do składania podpisu elektronicznego, a kto do używania e-pieczęci instytucjonalnej.

Nadmierne i nieuzasadnione uprawnienia

Drugim krytycznym obszarem są nadmierne i nieuzasadnione uprawnienia, w szczególności związane z fizycznymi nośnikami podpisu kwalifikowanego („penami"). W praktyce wciąż spotyka się sytuacje, w których tokeny pozostawiane są w sekretariatach, a dostęp do nich ma wiele osób. To realne ryzyko nadużyć i odpowiedzialności prawnej osoby, której podpis został użyty bez jej wiedzy. Uczelnia powinna przyjąć zasadę, że podpis elektroniczny jest narzędziem osobistym, nieprzekazywalnym, a jego użycie musi być technicznie i organizacyjnie zabezpieczone (np. poprzez rozwiązania chmurowe, czy silne uwierzytelnienie).

Równie istotne jest cyberbezpieczeństwo. E-podpis i e-pieczęć to produkty technologiczne, które muszą być chronione na poziomie systemowym i użytkowym. Przypinanie kodów PIN do penów czy współdzielenie haseł to niestety nadal spotykane praktyki, które całkowicie podważają sens cyfrowych zabezpieczeń. Standardem powinna być wdrożona polityka bezpieczeństwa czy zasada minimalnych uprawnień.

Brak spójnych zasad przypisywania podpisów do dokumentów

Kolejne źródło chaosu to niejasność w zakresie typów dokumentów i podpisów. Na uczelni powinien istnieć katalog dokumentów z przypisanym typem podpisu: które wymagają podpisu kwalifikowanego, które zaawansowanego, a które e-pieczęci. Mylenie tych zastosowań prowadzi do błędów formalnych i ryzyk prawnych. To obszar, który warto uregulować centralnie, a nie pozostawiać interpretacji poszczególnym jednostkom czy osobom.

> Na uczelni powinien istnieć katalog dokumentów z przypisanym typem podpisu: które wymagają podpisu kwalifikowanego, które zaawansowanego, a które e-pieczęci.

Nie można pominąć warsztatów, które powinny być obowiązkowe, krótkie i praktyczne – najlepiej gdy w trakcie użytkownik realnie podpisuje dokumenty. Tylko wtedy rośnie pewność, swoboda i bezpieczeństwo korzystania z narzędzi, a nowe rozwiązania nie blokują pracy administracji ani kadry akademickiej.

Fundamentem jest także zgodność technologii i usług z eIDAS i RODO. Uczelnia musi mieć pewność, że działania są prowadzone zgodnie z przepisami.

Nie da się zrealizować bezpiecznego wdrożenia bez kompetentnego i doświadczonego partnera technologicznego. Wybór dostawcy nie powinien opierać się na prezentacji handlowej, lecz na udokumentowanym doświadczeniu, znajomości realiów sektora publicznego i szkolnictwa wyższego oraz działających wdrożeniach. Partner powinien nie tylko dostarczyć narzędzie, ale też pomóc w zaprojektowaniu procesów i standardów.

Błędy ludzkie w procesach masowego podpisywania

Na szczególną uwagę zasługuje masowe podpisywanie dokumentów. Przy dużej skali łatwo o błędy ludzkie, np. podpisanie niewłaściwego pliku, błędna data na dokumencie czy pominięcie załącznika. Automatyzacja podpisywania znacząco redukuje te ryzyka i powinna być standardem tam, gdzie wolumen dokumentów jest wysoki.

> Nie można mówić o pełnej cyfryzacji uczelni, jeśli proces kończy się drukiem „do podpisu".

Na koniec warto podkreślić, że podpisy i pieczęcie są ostatnim ogniwem obiegu dokumentów. Nie można mówić o pełnej cyfryzacji uczelni, jeśli proces kończy się drukiem „do podpisu". Dopiero bezpieczne, uregulowane i świadome użycie e-podpisu i e-pieczęci domyka cyfrowy obieg dokumentów i nadaje mu realną wartość organizacyjną i prawną.

Marka uczelni zaczyna się w dziekanacie i w bezpieczeństwie danych

Najbardziej niedoceniany dział marketingu na uczelni mieści się zwykle między pokojem dziekanatu a okienkiem, w którym ktoś tłumaczy studentowi, że „system nie widzi" albo „u mnie działa". W tym samym miejscu rodzi się najcenniejszy kapitał reputacyjny, czyli zaufanie. Dziś to zaufanie coraz częściej działa jak KPI marketingu, bo wpływa na wybór uczelni, gotowość do płacenia za studia podyplomowe, chęć pozostania w relacji jako absolwent, a nawet na skłonność pracowników do obrony instytucji w kryzysie. Dlatego marka uczelni ma dwa fundamenty, o których broszury rekrutacyjne mówią niechętnie. To jakość doświadczenia administracyjnego oraz poczucie bezpieczeństwa danych.

W czasach, gdy cyberincydent potrafi w jeden weekend zamienić spokojną narrację o deklarowanej innowacyjności w serię pytań o to, kto miał dostęp do numerów PESEL, uczelnia jest oceniana mniej za obietnice, a bardziej za cyfrową odporność.

To nie jest abstrakcja. W brytyjskim badaniu rządowym dotyczącym naruszeń cyberbezpieczeństwa w instytucjach edukacyjnych aż 91 procent uczelni wyższych zadeklarowało, że w ostatnich 12 miesiącach zidentyfikowało incydent lub atak, a phishing był najczęściej wskazywaną kategorią zdarzeń[1]. To oznacza, że czy nas to spotka, przestało być banalnym pytaniem, a stało się wyzwaniem, jak szybko wykryjemy, jak mądrze zareagujemy i jak uczciwie to zakomunikujemy.

Zaufanie jako KPI, czyli co naprawdę kupuje kandydat i student?

W marketingu uczelni łatwo wpaść w pułapkę myślenia, że marka to głównie wizerunek, czyli kampania rekrutacyjna, sesja zdjęciowa, ranking, laboratoria, aktywność na platformach społecznościowych, wydarzenia, relacje z mediami.

Tyle że w rzeczywistości **marka jest doświadczeniem powtarzalnym.** Kandydat może zakochać się w filmie promocyjnym, ale decyzję o nauce podejmuje na podstawie swoistej codzienności. Czy potrafię załatwić sprawę bez zbędnej biurokracji, czy ktoś odpowiada na moje pytania, czy dane są bezpieczne, czy uczelnia panuje nad procesami?

Zaufanie jest też dobrem deficytowym na poziomie społecznym. Przykładowo badania opinii publicznej w Stanach Zjednoczonych pokazują, że oceny i nastroje wobec szkolnictwa wyższego są spolaryzowane, a duża część respondentów uważa, że system zmierza w złym kierunku[2]. Równolegle w innych pomiarach widać, że zaufanie do szkolnictwa wyższego potrafi się zmieniać, ale pozostaje kruche i wrażliwe na kryzysy reputacyjne[3]. W ujęciu globalnym widać z kolei rosnące napięcia wokół instytucji oraz wyraźną nierówność zaufania pomiędzy grupami społecznymi[4].

1 Department for Science, Innovation & Technology and Home Office (2025) *Cyber security breaches survey 2025: education institutions findings*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings (dostęp: 26 stycznia 2026).

2 Parker K. (2025), Growing share of Americans say the U.S. higher education system is headed in the wrong direction. Pew Research Center. https://www.pewresearch.org/short.

3 Jones J.M. (2025), U.S. Public Trust in Higher Ed Rises From Recent Low. Gallup. https://news.gallup.com/poll/692519/public-trust-higher-rises-recent-low.aspx (dostęp: 26 stycznia 2026).

4 Edelman Trust Institute (2025) 2025 Edelman Trust Barometer: Global Report. Edelman. https://www.edelman.com/sites/g/files/aatuss191/files/2025-01/2025%20Edelman%20Trust%20Barometer_Final.pdf (dostęp: 26 stycznia 2026).

W takim środowisku uczelnia nie wygrywa już samą deklaracją misji. **Wygrywa zdolnością do realnego zapewniania fundamentów.** Podstawą w XXI wieku jest także dojrzałość cyfrowa, w tym bezpieczeństwo i prywatność.

Jak administracja uczelni buduje reputację?

Wyobraźmy sobie historię, która wydarza się regularnie, tylko za każdym razem w innej uczelni. Studentka pierwszego roku składa wniosek o stypendium. Formularz jest dostępny jako plik, który trzeba wydrukować, podpisać i donieść. Potem przychodzi mail z prośbą o uzupełnienie, ale bez wskazania, czego brakuje. Telefon nie odpowiada. W dziekanacie kolejka. Ktoś mówi, że tak jest od lat. Studentka nie myśli wtedy o strategii marki. Myśli, że uczelnia nie panuje nad własnym procesem. Skoro nie panuje nad wnioskiem o stypendium, to czy panuje nad moimi danymi, wynikami, dokumentami, historią medyczną w przypadku praktyk, danymi z systemu bibliotecznego i platformy e-learningowej?

To jest moment, w którym marketing powinien przestać mówić wyłącznie językiem obietnic, a zacząć mówić językiem doświadczenia. Dla odbiorcy proces administracyjny jest dowodem kompetencji instytucji.

> Dla odbiorcy proces administracyjny jest dowodem kompetencji instytucji.

Twarde dane z badań studenckich, nawet jeśli pochodzą z raportów bazujących na ankietach rynkowych, konsekwentnie pokazują, że sprawność procesów i przejrzystość komunikacji mają realny wpływ na wybory i retencję.

W jednym z raportów opartych na badaniu doświadczeń studentów w obszarze pomocy finansowej wskazano na silną wrażliwość na czas obsługi i jakość narzędzi cyfrowych, a także na oczekiwanie jednego miejsca dostępu do usług studenckich[5].

Nawet jeśli uczelnia nie działa w identycznym modelu jak amerykański system finansowania, mechanizm jest uniwersalny, czyli im mniej zamieszania w procesach, tym większa skłonność do pozostania w relacji. Administracja jest więc „produktem codziennym" uczelni, a bezpieczeństwo danych jest gwarancją jakości tego produktu.

Cyberincydent jako test reputacji

W wielu instytucjach cyberbezpieczeństwo wciąż bywa traktowane jak temat stricte techniczny, który ma zabezpieczać IT. Tyle że cyberincydent uderza w markę dokładnie w tych punktach, które w edukacji są święte: wiarygodność, odpowiedzialność, etyka, opieka nad młodymi ludźmi, ochrona danych o szczególnym znaczeniu.

> Cyberincydent uderza w markę dokładnie w tych punktach, które w edukacji są święte: wiarygodność, odpowiedzialność, etyka, opieka nad młodymi ludźmi, ochrona danych o szczególnym znaczeniu.

Tymczasem skala i charakter zagrożeń rosną. Verizon w raporcie DBIR za 2025 rok opisuje wzrost znaczenia eksploatacji podatności jako wektora wejścia oraz wyraźny udział ransomware w naruszeniach[6]. Dla uczelni to kluczowe, bo system jest rozproszony na system dziekanatowy, platformy dydaktyczne, biblioteki, system płatności, system rekrutacyjny, narzędzia do ankiet, praktyk, badań i grantów, plus dziesiątki integracji.

Z perspektywy reputacji najgroźniejsze są incydenty, które łączą dwa elementy naraz, tj. zakłócenie działania i wyciek danych. Ransomware właśnie na tym polega. Badanie Sophos dotyczące sektora edukacji pokazuje, że w szkolnictwie wyższym znacząca część ataków kończyła się szyfrowaniem danych, a część przypadków obejmowała również eksfiltrację. Raport opisuje też, że część instytucji płaci okup, a koszty odtworzenia potrafią być znaczące, nawet jeśli sektor poprawia odporność[7].

5 Ellucian (2024) The Student Voice Report: How Financial Aid Impacts U.S. Higher Education Enrollment and Retention. Ellucian. https://lp.ellucian.com/rs/085-MHT-312/images/Student-Survey-White-Paper.pdf (dostęp: 26 stycznia 2026).

6 Verizon (2025) 2025 DBIR Executive Summary. Verizon Business. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf (dostęp: 26 stycznia 2026).

7 Sophos (2025) The State of Ransomware in Education 2025. Sophos. https://page.infinigate.com/hubfs/Sophos/sophos-state-of-ransomware-in-education-2025.pdf (dostęp: 26 stycznia 2026).

Do tego dochodzi wątek, który marketing uczelni zwykle omija, a który staje się coraz bardziej realny, czyli niekontrolowane użycie narzędzi AI przez pracowników i studentów, ryzyko „cichego wycieku" danych do zewnętrznych usług. W raporcie IBM o kosztach naruszeń danych pokazano, że incydenty związane z tak zwanym *shadow AI*[8] mogą podnosić średni koszt naruszenia, a wiele organizacji nie ma jeszcze polityk zarządzania tym obszarem[9].

> Uczelnie są atrakcyjnym celem, bo mają dużo wrażliwych danych i często muszą godzić otwartość akademicką z bezpieczeństwem.

W tle jest jeszcze jedna prawda. Uczelnie są atrakcyjnym celem, bo mają dużo wrażliwych danych i często muszą godzić otwartość akademicką z bezpieczeństwem. Microsoft w raporcie Digital Defense Report wskazuje, że wśród sektorów mocno dotkniętych atakami znajdują się także obszary badawcze i akademickie[10].

Historie z życia uczelni

W poniedziałek rano pracownica dziekanatu dostaje wiadomość, która wygląda jak mail od znanej firmy kurierskiej, z prośbą o *potwierdzenie danych do przesyłki z dokumentami*. Kliknięcie prowadzi do fałszywej strony logowania, hasło zostaje przechwycone, a atakujący loguje się do skrzynki, ustawia reguły przekierowań i po kilku dniach zaczyna wysyłać do studentów kolejne wiadomości, tym razem już z konta uczelni. Część studentów klika, część podaje dane, zaczynają się skargi, a ktoś wrzuca screeny do mediów społecznościowych. Technicznie to *phishing* i przejęcie konta, ale wizerunkowo to pytanie, jak to możliwe, że uczelnia nie wykryła incydentu przez kilka dni i dlaczego informacja dotarła do studentów najpierw przez plotkę?

Rozwiązanie, które naprawdę działa, nie jest jedną kampanią uświadamiającą. To zestaw praktyk. Po pierwsze, obowiązkowe uwierzytelnianie wieloskładnikowe dla kont o podwyższonych uprawnieniach oraz dla całej administracji. Po drugie, monitorowanie nietypowych logowań i reguł pocztowych, bo przekierowania są klasycznym sygnałem kompromitacji. Po trzecie, gotowy scenariusz komunikacji wewnętrznej uruchamiany w pierwszej godzinie, do dziekanatów, sekretariatów, biblioteki i rekrutacji, czyli tam, gdzie studenci pytają najpierw. I wreszcie, jasny komunikat zewnętrzny, co wiemy, czego nie wiemy, co robimy, jak student może się zabezpieczyć i gdzie zgłaszać podejrzane maile.

Taki scenariusz warto podpierać badaniami o skali problemu. W danych brytyjskich dla sektora edukacji phishing jest dominującym typem incydentu, szczególnie w instytucjach mocno cyfryzujących procesy, co oznacza, że prewencja i szybkość reakcji stają się elementem strategii marki[11]. To oznacza, że **prewencja i szybkość reakcji są elementem strategii marki**.

Inna historia. W środę w nocy pada część serwerów wydziału. Rano nie działa system do zapisów na zajęcia ćwiczeniowe. Potem przestaje działać dostęp do części zasobów badawczych. Pojawia się komunikat o okupie. Media pytają, czy doszło do wycieku danych grantowych i danych studentów. Pracownicy są wściekli, bo nie mają dostępu do wyników. Studenci panikują, bo trwa rekrutacja na praktyki. Tu już nie wystarczy informacja *pracujemy nad przywróceniem.*

Cyberincydent szybko przestaje być wyłącznie problemem technicznym i staje się testem reputacji w trzech wymiarach. **Sprawczości**, czyli tego, czy uczelnia ma plan i konsekwentnie go realizuje, czy jedynie improwizuje. **Transparentności**, czyli czy komunikuje fakty w rozsądnym rytmie, czy chowa się za ciszą, oraz **empatii**, czyli czy rozumie, co taki incydent oznacza dla studentów, kadry akademickiej, zespołów badawczych i partnerów. W tym kontekście raport Sophos dla sektora edukacji wskazuje, że w szkolnictwie wyższym nadal dochodzi do

> Cyberincydent szybko przestaje być wyłącznie problemem technicznym i staje się testem reputacji.

8 Shadow AI to nieautoryzowane używanie narzędzi sztucznej inteligencji w pracy, poza oficjalnie zatwierdzonymi rozwiązaniami firmy, często z wprowadzaniem do nich danych służbowych, co zwiększa ryzyko wycieku i naruszeń zgodności.

9 IBM Corporation (2025) Cost of a Data Breach Report 2025: The AI Oversight Gap. IBM. https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf (dostęp: 26 stycznia 2026).

10 Microsoft (2025) Microsoft Digital Defense Report 2025. Microsoft. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025 (dostęp: 26 stycznia 2026).

11 op.cit. Department for Science, Innovation & Technology and Home Office (2025)

szyfrowania danych, a część instytucji decyduje się na zapłatę okupu, choć jednocześnie rośnie ogólny poziom odporności[12]. Wniosek dla uczelni jest brutalnie prosty. **Reputacja zależy od przygotowania**, a nie od szczęścia.

Jak dbać o markę uczelni?

Pierwszy krok to zdefiniowanie zaufania jako KPI i przypisanie mu właściciela. Jeśli zaufanie ma być wskaźnikiem marketingu, musi mieć jasną definicję oraz rytm pomiaru. Uczelnia może mierzyć je w badaniach satysfakcji studentów i kandydatów (osobno dla obszarów administracyjnych i cyfrowych), a także poprzez NPS[13] lub prosty wskaźnik rekomendacji dla kluczowych punktów styku, takich jak dziekanat, rekrutacja, stypendia czy IT helpdesk. Warto równolegle śledzić liczbę incydentów i zgłoszeń bezpieczeństwa na tysiąc użytkowników, ale w połączeniu z czasem reakcji i zamknięcia sprawy, a także wskaźniki dojrzałości operacyjnej, m.in. poziom adopcji MFA[14], stan aktualizacji urządzeń oraz czas łatania krytycznych podatności. Do tego dochodzi „czas do prawdy" w komunikacji kryzysowej, czyli ile czasu mija od wykrycia problemu do pierwszego komunikatu wewnętrznego i zewnętrznego. W tle warto pamiętać, że koszty naruszeń obejmują nie tylko technologię, lecz także komunikację, obsługę kryzysu i zarządzanie reputacją.

> Najczęstszy błąd uczelni polega na tym, że nikt nie potrafi odpowiedzieć na proste pytania, jakie dane mamy, gdzie są, kto ma do nich dostęp i jak długo je trzymamy.

Najczęstszy błąd uczelni polega na tym, że nikt nie potrafi odpowiedzieć na proste pytania, jakie dane mamy, gdzie są, kto ma do nich dostęp i jak długo je trzymamy. Bez tego nie da się ani skutecznie chronić informacji, ani wiarygodnie komunikować w kryzysie. Minimum do wdrożenia obejmuje inwentaryzację systemów i przepływów danych, także tych nieoficjalnych, jak arkusze, dyski współdzielone czy narzędzia ankietowe. Następnie klasyfikację danych (osobno dla studentów, pracowników, kandydatów, badań i grantów), wdrożenie zasady minimalizacji dostępu, czyli przydzielanie uprawnień wyłącznie w zakresie niezbędnym dla danej roli wraz z regularnymi przeglądami, oraz jasne reguły retencji danych, czyli kasowania i archiwizacji.

Wiele incydentów zaczyna się poza uczelnią, bo coraz większą rolę w naruszeniach odgrywają podmioty trzecie, co pokazuje wspomniany raport DBIR. Dlatego uczelnia powinna wdrożyć prostą, ale twardą praktykę zarządzania dostawcami. Stosować standardowy zestaw pytań bezpieczeństwa przy zakupach i wdrożeniach, wymagać zgłaszania incydentów w jasno określonym czasie, narzucić minimalne standardy uwierzytelniania i szyfrowania oraz mieć plan awaryjny na wypadek niedostępności usługi, bo ciągłość działania jest też częścią doświadczenia studenta.

> Zbuduj kulturę, w której bezpieczeństwo nie jest strachem, tylko troską.

Dane z sektora edukacji pokazują, że instytucje coraz lepiej uczą się, a mimo to wciąż bywają często atakowane. To oznacza, że szkolenia muszą być krótkie, regularne i osadzone w realnych sytuacjach uczelni. Najlepiej działają lekcje dla administracji i kadry oparte na prawdziwych przykładach z uczelni, symulacje phishingu prowadzone bez zawstydzania (celem nie jest polowanie na winnych). Do tego jasny komunikat, że zgłoszenie podejrzanej sytuacji jest premiowane, a nie karane. Widać też jeden i prosty kanał zgłoszeń, by ani studenci, ani pracownicy nie musieli go szukać po zakładkach.

Warto łączyć cyberbezpieczeństwo z poprawą doświadczenia administracyjnego. Największą przewagą uczelni nie jest to, że ma politykę bezpieczeństwa, tylko że **potrafi zbudować procesy, które są jednocześnie bezpieczne i wygodne.** W praktyce pomagają w tym sprawdzone rozwiązania. Jeden portal usług studenckich i jeden standard komunikacji zamiast rozproszenia po dziesięciu systemach, kolejkowanie zgłoszeń oraz jasne czasy odpowiedzi w dziekanatach i helpdesku IT, automatyzacja powtarzalnych spraw (zaświadczenia, statusy wniosków, terminy), powiadomienia o statusie sprawy oraz jasne formularze napisane prostą polszczyzną. **Niezrozumiałe komunikaty rodzą błędy, a błędy rodzą ryzyko.** W raportach opartych na badaniach studenckich mocno wybrzmiewa oczekiwanie wygodnych, zintegrowanych narzędzi i szybkiej

12 cit. Sophos (2025) The State of Ransomware

13 NPS (Net Promoter Score) to wskaźnik lojalności/rekomendacji i mierzy, na ile ludzie są skłonni polecić Twoją organizację innym.

14 Odsetek kont/użytkowników, którzy mają włączone i faktycznie używają uwierzytelniania wieloskładnikowego przy logowaniu.

obsługi administracyjnej, a opóźnienia i niejasność przekładają się na decyzje i rezygnacje. Ten wątek warto czytać jako argument reputacyjny, nie tylko operacyjny.

Komunikacja marki uczelni

Komunikacja cyberbezpieczeństwa jest trudna, bo łatwo wpaść w dwa skrajne tony. Pierwszy to techniczny bełkot albo propagandowe hasła w stylu „jesteśmy w pełni bezpieczni", które w chwili incydentu obracają się przeciwko uczelni. Dobre komunikowanie opiera się na trzech zasadach. **To prostota, konkret i regularność.**

W komunikacji wewnętrznej warto jasno powiedzieć, po co to robimy, nie dla audytu, tylko dla ochrony ludzi oraz ciągłości studiowania i badań. Uczynić bezpieczeństwo częścią jakości pracy, traktując MFA i aktualizacje jako standard, a nie zło konieczne. Pomaga też rytm. Raz w miesiącu krótka informacja o najczęstszych zagrożeniach oraz o tym, co udało się poprawić, a także gotowe teksty odpowiedzi dla dziekanatów i sekretariatów, bo to one odbierają pierwszy kontakt. W komunikacji zewnętrznej najlepiej edukować bez moralizowania. Jak rozpoznać fałszywe maile, gdzie zgłosić podejrzenie i jak chronić konto? Także mówić o standardach (MFA, kopie zapasowe, testy, przeglądy dostawców) bez przechwałek.

Jeśli dochodzi do incydentu, komunikować warstwowo, tj. co się stało i jaki ma to wpływ na usługi, jakie dane mogły zostać dotknięte (jeśli to już wiadomo), co uczelnia robi teraz i co zrobi dalej oraz co może zrobić student lub pracownik? Kluczowe jest też utrzymanie jednego oficjalnego „punktu prawdy", aktualizowanego w stałym rytmie, bo brak informacji tworzy alternatywne narracje.

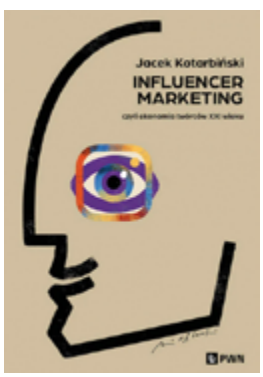
Warto pamiętać o kontekście sektorowym. Jeśli niemal wszystkie instytucje raportują incydenty, to transparentność i gotowość komunikacyjna stają się elementem normalnego zarządzania reputacją, a nie przyznaniem się do słabości.

Dlaczego uczelnie mogą wygrać?

W tych historiach jest dobra wiadomość. Uczelnie mają dwa atuty, których wielu organizacjom brakuje. Pierwszy to kompetencje. Solidne uczelnie to ludzie, którzy potrafią uczyć się szybciej niż przeciętny rynek i którzy rozumieją, że procedura jest narzędziem, a nie karą. Drugi to sens. W edukacji bezpieczeństwo danych nie jest tylko ochroną przed stratą finansową. Jest ochroną relacji z człowiekiem, który powierza instytucji kawałek swojej biografii.

Jeśli potraktować dziekanat jako serce marki, a cyberbezpieczeństwo jako język troski o studentów i pracowników, to uczelnia może budować zaufanie w sposób bardzo nowoczesny, bez wielkiego hałasu. Wystarczy robić dwie rzeczy konsekwentnie. **Upraszczać doświadczenie i wzmacniać odporność.** Reszta, w tym komunikacja na zewnątrz, staje się wtedy opowieścią opartą na faktach, a fakty są dziś najbardziej deficytową walutą reputacji.

dr inż. Jacek Kotarbiński



Ekonomista, marketer, rynkolog, inżynier. Uznany autorytet, strateg, międzynarodowy ekspert w zakresie marketingu, zarządzania marką, rozwoju innowacji i zarządzania sprzedażą. Od 1990 roku skutecznie wspiera przedsiębiorstwa w zakresie rozwoju konkurencyjności. Keynote konferencji branżowych, trener biznesu, doradca i mentor innowacyjnych firm. Laureat konkursu Blog Roku 2012 Onet.pl, w kategorii „Blogi profesjonalne i firmowe". Wykładowca uczelni wyższych na studiach MBA. Pomysłodawca i twórca fanpage „Bareizmy Wiecznie Żywe". Autor Bloga o Sztuce Marketingu kotarbinski.com.

Wszyscy kłamią. Dziewięć mitów o relacji nauki i biznesu

„Wszyscy kłamią" – mówił Gregory House, bohater jednego z najbardziej ikonicznych seriali pierwszej dekady XXI wieku. Nie dlatego, że ludzie są źli, lecz dlatego, że prawda jest niewygodna, niepełna albo źle opowiedziana. Dokładnie tak samo jest ze współpracą nauki i biznesu. Jakie kłamstwa krążą wokół tej relacji i dlaczego tak skutecznie blokują trafną diagnozę problemu?

Waga i interpretacja każdego przekazu zależą od okoliczności, w których się pojawia, oraz od tego, kto go formułuje. Z punktu widzenia czytelnika istotne jest więc, kto ten tekst pisze.

W 2010 roku rozpocząłem studia na Politechnice Warszawskiej. Najpierw ukończyłem lotnictwo i kosmonautykę, a następnie automatykę i robotykę. W 2015 roku otworzyłem swój pierwszy biznes technologiczny i tworzę kolejne po dziś dzień. W październiku 2024 roku rozpocząłem kształcenie w Szkole Doktorskiej Politechniki Warszawskiej w dyscyplinie nauki fizyczne. W międzyczasie współpracowałem – i nadal współpracuję – z Biurem Karier PW, Centrum Innowacji PW oraz kilkoma parkami technologicznymi w Polsce.

Piszę o tym nie po to, by budować autorytet, lecz by dać czytelnikowi pełen kontekst. Doświadczyłem bardzo konkretnych bodźców i mechanizmów, zarówno po stronie nauki, jak i biznesu. Sam jestem sceptykiem, dlatego uczciwie dostarczam argumentów także innym sceptykom.

Kłamstwo pierwsze: nauka i biznes to dwa przeciwne bieguny

Pierwszym kłamstwem jest przeciwstawianie nauki i biznesu jako dwóch odrębnych, wrogich biegunów – niczym para cząstka–antycząstka, które po zderzeniu ulegają anihilacji.

W zeszłym roku przeprowadziłem na Politechnice Warszawskiej bezpłatne szkolenie „Biznes na doktoracie". W jego trakcie zaproponowałem proste ćwiczenie: doktoranci mieli podzielić się na dwie grupy i wypisać cechy, jakie ich zdaniem charakteryzują naukowców oraz przedsiębiorców.

W pierwszym podejściu naukowcy byli opisywani jako dociekliwi, systematyczni, skupieni na jakości i prawdzie, ale też oderwani od realiów i niepraktyczni. Przedsiębiorcy jako dynamiczni, nastawieni na wynik, pragmatyczni, ale jednocześnie krótkowzroczni i gotowi na kompromisy etyczne.

Następnie poprosiłem o drugą listę: cechy dobrego naukowca i dobrego przedsiębiorcy. Ku zaskoczeniu uczestników okazało się, że te zestawy są niemal identyczne. Ciekawość, wytrwałość, umiejętność uczenia się na błędach, odporność na porażki, zdolność pracy zespołowej.

Różnica nie leży więc w ludziach, lecz w stereotypach, w środowisku, w którym funkcjonują, oraz w dostępnych zasobach i systemach motywacyjnych.

Warto dodać, że uczestnicy szkolenia mieli od około 25 do 50 lat i reprezentowali bardzo różne dziedziny – od fizyki, przez elektronikę i inżynierię mechaniczną, po architekturę i zarządzanie.

> Różnica nie leży w ludziach, lecz w stereotypach, w środowisku, w którym funkcjonują, oraz w dostępnych zasobach i systemach motywacyjnych.

Kłamstwo drugie: biznes jest brudny, a nauka nieskalana

Często można usłyszeć, że biznes z definicji postępuje nieetycznie. Przedsiębiorcy bywają przedstawiani jako złodzieje i kombinatorzy, którzy tylko czekają, by kraść pomysły na-

ukowcom. W domyśle oznacza to, że nauka jest przestrzenią czystą i moralnie nieskalaną.

Tymczasem zjawiska takie jak mobbing, kradzież wyników badań, pomijanie autorów w publikacjach, fałszowanie danych czy udział w tzw. papierniach są w nauce faktem – i nie są wcale marginalne.

Niejednokrotnie najgłośniej przed kradzieżą własności intelektualnej ostrzegają ci, którzy nigdy żadnej wartościowej własności intelektualnej nie wytworzyli, więc realnie i tak nie mogą nic stracić.

Ileż to razy słyszymy historie o genialnym pomyśle koleżanki lub kolegi z wydziału, który ktoś komuś opowiedział, a kilka lat później „jakaś firma zrobiła dokładnie to samo". Część z tych opowieści jest prawdziwa, część – nie. Problem w tym, że całe pokolenia studentów i młodych naukowców wychodziły z takich narracji z przekonaniem, że każdy przedsiębiorca zainteresowany współpracą jest potencjalnym złodziejem.

Cieszy mnie, że na uczelniach coraz częściej mówi się o ochronie własności intelektualnej. Wiedza o tym, czym jest własność intelektualna, kiedy i jak ją chronić, jest realną wartością. To zmiana widoczna w ostatnich latach i warta odnotowania.

Wielu z nas – w tym ja – chciałoby, aby procesy związane z własnością intelektualną wyglądały lepiej, ale nawet niedoskonałe procedury kształtują dobre nawyki. Uważam, że czasami rola własności intelektualnej jest przeceniana, kosztem działań biznesowych, ale to temat do osobnej dyskusji.

Kłamstwo trzecie: przedsiębiorczość to konieczność

Przedsiębiorczość jest cechą pozytywną i warto ją rozwijać. Nie widzę jednak uzasadnienia, by kogokolwiek do przedsiębiorczości zmuszać. Tak samo nie możemy nikogo zmusić do dbania o zdrowie – choć zarówno indywidualnie, jak i społecznie jest to wysoce pożądane.

W polskich jednostkach naukowych niewątpliwie są osoby utalentowane, z predyspozycjami do komercjalizacji wyników swojej pracy. To, czego często brakuje, to dobry wizerunek naukowców-przedsiębiorców oraz jasny sygnał, że taka ścieżka jest doceniana.

Jako absolwent, a dziś doktorant Politechniki Warszawskiej, widzę wyraźną poprawę w porównaniu z sytuacją sprzed 15 lat. Uczymy przedsiębiorczości – nie tylko studentów, ale i naukowców. Nie sposób tu nie wspomnieć o staraniach prof. Agnieszki Skali, która wraz z zespołem od lat prowadzi zajęcia z przedsiębiorczości technologicznej i startupowej na kolejnych wydziałach Politechniki.

Warto też pamiętać, że przedsiębiorczość nie ma wyłącznie wymiaru ekonomicznego. Można być przedsiębiorczym w zarządzaniu czasem, w organizacji zespołu, w tworzeniu dóbr niematerialnych. Pieniądz jest wygodną metryką, ale nie jesteśmy skazani na przeliczanie wszystkiego na złotówki.

Kłamstwo czwarte: naukowcy są oderwani od rzeczywistości

Z perspektywy biznesu naukowcy bywają postrzegani jako oderwani od rzeczywistości. I rzeczywiście – są oderwani od pewnej rzeczywistości, bo są głęboko w innej zanurzeni. Tak samo biznes bywa oderwany od rzeczywistości naukowej, ale jest za to ściśle przyklejony do ekonomii.

To nie wada, lecz konsekwencja specjalizacji. To, że ktoś jest zanurzony w jakimś otoczeniu i zna zasady jego funkcjonowania, jest zaletą. Naukowcom zależy na publikacjach i będą o ten obszar dbać. Biznesowi zależy na tworzeniu produktów i usług, więc będą o to zabiegać. Można zrealizować oba cele w jednym przedsięwzięciu, tylko trzeba szczerze o tym porozmawiać.

> Źródłem największych nieporozumień na linii nauka-biznes jest zazwyczaj stopień bezwładności i czasochłonności decyzji.

Źródłem największych nieporozumień na linii nauka-biznes jest zazwyczaj stopień bezwładności i czasochłonności decyzji. Zazwyczaj partnerzy naukowi są bardziej bezwładni niż ci biznesowi, szczególnie w przypadku małych i średnich przedsiębiorstw. Tak po prostu jest i trzeba uwzględnić to we wspólnych przedsięwzięciach. Instytucje naukowe powinny pracować nad tym, żeby te procesy przebiegały sprawniej. Nie ma co jednak oczekiwać, że będą działy się od ręki.

Będąc szczerym byłbym bardzo zmartwiony, gdyby tak było. To, że kilka osób coś – miejmy nadzieję – czyta i wydaje decyzje, wpisuje się w reguły należytej staranności. Należytej staranności nigdy za wiele. Mogę jedynie podpowiedzieć, że budowanie relacji sprzyja pokonywaniu barier biurokratycznych. To zwyczajnie kwestia zaufania i gotowości do kontaktu w spornych kwestiach, takich jak zapisy umowy.

To co należy poddać krytyce, to sytuacje gdy ktoś w procesie decyzyjnym partnera – naukowego lub biznesowego – wywraca wszystko do góry nogami w ostatniej chwili. Źródła takich zachowań są wszelakie. Czasami jest to źle przygotowany temat, czasami brak profesjonalizmu. Myślę, że wielu z nas czegoś takiego doświadczyło.

Kłamstwo piąte: biznes to pieniądze, nauka to publikacje

Gdyby moją jedyną funkcją celu były pieniądze, nie zajmowałbym się zaawansowanymi technologiami. Na nich można zarobić bardzo dużo, ale istnieją – przynajmniej krótkoterminowo – znacznie prostsze drogi. Zawsze mówię półżartem, że gdyby chodziło tylko o pieniądze, sprzedawałbym żelki.

Wielu przedsiębiorców robi to, co robi, ponieważ to lubi. Lubi tworzyć, dostarczać rozwiązania, które uważa za społecznie użyteczne. Dla niektórych pieniądze są efektem ubocznym, koniecznym zasobem do realizacji swoich pomysłów, a nie jedynym celem.

Podobnie nie wszyscy naukowcy są skupieni wyłącznie na publikacjach. Owszem, publikujemy, bo takie są reguły gry. Z drugiej strony zarzut, że naukowcom zależy tylko na nauce, jest sam w sobie karykaturalny. Na czym miałoby im zależeć jak nie na nauce?

Idąc dalej - jedni czerpią satysfakcję z kształcenia studentów, inni z rozwiązywania trudnych problemów, jeszcze inni z realnego wpływu na otoczenie. Znam wiele osób, które po prostu lubią środowisko akademickie. Ja też je lubię, dlatego do niego wróciłem.

> Chęć tworzenia jest często wspólnym mianownikiem nauki i biznesu.

Z doświadczenia mogę powiedzieć, że chęć tworzenia jest często wspólnym mianownikiem nauki i biznesu. Co więcej, każdy z tych obszarów używa nieco innych narzędzi, co jest siłą takiego połączenia. Nie da się postawić całego domu, używając tylko młotka albo tylko piły. Tak samo nie da się tworzyć rzeczy unikatowych nie łącząc różnych podejść, zasobów i możliwości. Dlatego współpraca nauki z biznesem ma tak duży potencjał.

Kłamstwo szóste: trzeba komercjalizować naukę

Dobrze, by badania naukowe miały jakiś sens i cel – może nim być poprawa bezpieczeństwa, dobrostanu lub produkt, który da się sprzedać. Nie każdy wynik badań da się jednak skomercjalizować w rozumieniu rachunku ekonomicznego i nie odbiera to tym badaniom wartości.

> Nie każdy wynik badań da się skomercjalizować w rozumieniu rachunku ekonomicznego i nie odbiera to tym badaniom wartości.

Co więcej, działalność naukowa bardzo często wynika tylko i wyłącznie z ciekawości. Historia pokazuje, że ciekawość prowadzi do bardzo praktycznych, wręcz spektakularnych efektów.

Efekt społeczny nauki jest szczególnie istotny w dobie dezinformacji i epoce postprawdy. Trudno jest sprzedać wyniki prac historyków czy etnografów, ale wyniki ich pracy zarówno na polu dydaktycznym, jak i naukowym mają charakter dobra publicznego w wymiarze pozaekonomicznym. Nadmienię, że tym bardziej w takich przypadkach musimy zwracać uwagę na jakość i zasadność takich badań, bo metryki, których w tym wypadku używamy, są trudniejsze do zdefiniowania i pomiaru.

W przestrzeni publicznej bardzo dużo mówimy o komercjalizacji technologii, a bardzo mało o komercjalizacji wiedzy - doradztwa, ekspertyz, kompetencji. To nisko wiszący owoc, którego notorycznie nie umiemy zerwać. Szkoda, bo to świetna okazja do budowy relacji nauki z biznesem i sprawdzenia obu stron w boju. Na poziomie instytucji badawczych trudno jest o realizację takich usług i jest w tym obszarze wiele do poprawy.

Badania naukowe są źródłem wiedzy i kompetencji, nie zawsze są źródłem wyników, które można skomercjalizować. Natomiast wiedza i kompetencje są zawsze podstawą do

tego, by chociażby opracowywać nowe technologie. Czynią nas one gotowymi do wykorzystywania okazji i… do trudnych czasów.

Kłamstwo siódme: musimy nauczyć naukowców biznesu

Gdy słyszę hasło „uczmy naukowców biznesu", odpowiadam: „uczmy handlowców mechaniki kwantowej". To oczywiście zgryźliwa riposta, ale kryje się za nią ważna myśl – nie tylko dlatego, że jako fizyk jestem zwolennikiem nauczania mechaniki kwantowej.

Nie można być dobrym we wszystkim - najczęściej nie dlatego, że coś jest zbyt trudne, lecz dlatego, że nie mamy na to czasu ani motywacji. W związku z tym kluczowe jest łączenie komplementarnych kompetencji.

To nie jest apel, by nie uczyć naukowców podstaw biznesu. Studia MBA czy kursy menedżerskie często poprawiają jakość komunikacji. Jest to zwyczajnie wyczuwalne w rozmowie. Ich celem nie jest jednak uczynienie z naukowca wybitnego przedsiębiorcy, lecz umożliwienie mu zrozumienia perspektywy drugiej strony.

Uczmy naukowców współpracy z tymi, którzy poprowadzą z nimi biznes – będziemy mieć z tego o wiele więcej pożytku.

Kłamstwo ósme: przedsiębiorcy nie mają pojęcia o nauce

Poziom wykształcenia części osób związanych z biznesem bywa barierą w dialogu, ale uogólnienia są tu równie krzywdzące jak w drugą stronę. Wielu przedsiębiorców ma bardzo dobry przegląd wiedzy naukowej. Często są to absolwenci wymagających studiów i cały czas przyswajają wiedzę z nowych obszarów. Nie raz tymi przedsiębiorcami są byli naukowcy. Ponadto firma firmie nierówna. Ktoś, kto zajmuje się projektami technologicznymi, zazwyczaj wie, co robi.

To, jaki stosunek do nauki mają ludzie biznesu, często zależy od nauczycieli akademickich i naukowców, jakich spotkali na swojej drodze. Akademia ma więc wymierny wpływ na wizerunek nauki.

Warta wysiłku jest ekspozycja środowiska biznesowego na tematykę naukową. Nie w formie pop nauki – tego jest już wystarczająco dużo – tylko w formie komunikatów naukowych. Nie tylko komunikowania podstaw naukowych, ale również obszarów zastosowań badań naukowych. Jeżeli nie zrobią tego naukowcy to zrobi to ktoś inny.

Uczmy przedsiębiorców współpracy z tymi, którzy budują przewagę konkurencyjną w oparciu o naukę, wiedzę i kompetencje – będziemy mieć z tego o wiele więcej pożytku… tak jak w poprzednim przypadku.

Kłamstwo dziewiąte: albo biznes, albo nauka

To fałszywa dychotomia. Owszem, istnieją środowiska wywierające presję na pełne poświęcenie się jednej ścieżce. Ale w dużej mierze to my sami wybieramy, w jakim otoczeniu funkcjonujemy. Nie ma tu złych i dobrych postaw. Ważne, żeby mieć świadomość, że każdy ma wybór, w którym miejscu spektrum nauka-biznes się znajduje. To miejsce może ewoluować w czasie.

Rozpoczynając doktorat, miałem pewne obawy z tym związane. Przypomnę, że mój doktorat nie dotyczy ekonomii czy zarządzania, tylko fizyki. Szybko okazało się, że moje doświadczenie biznesowe jest postrzegane jako zaleta, a nie wada. Wybrałem środowisko świadomie – i to miało bardzo duże znaczanie. Nie ukrywałem też, kim jestem. Nie raz ktoś zaczepia na korytarzach Politechniki, żeby skonsultować jakiś temat związany z przedsiębiorczością. Na pewno nie jestem pierwszym takim przypadkiem i jestem pewien, że nie ostatnim.

> Siłą każdej instytucji – niezależnie od obszaru, w którym działa – jest różnorodność.

Siłą każdej instytucji – niezależnie od obszaru, w którym działa – jest różnorodność. Nieważne, czy w firmie, czy na uczelni, to się zawsze sprawdza i warto to pielęgnować.

Czy w tym gąszczu kłamstw możemy coś zrobić razem?

Możemy. Jak? Najprostszą odpowiedzią jest: spróbować. Najlepiej zacząć od pilotażu – inicjatywy, która nie jest krytyczna dla żadnej ze stron. To pozwala poznać procedury, realne czasy trwania procesów i bariery biurokratyczne, które - choć uciążliwe – nie są nie do przejścia.

Jeżeli nie możesz zrobić wielkiego skoku – zrób mały krok. Może to być wspólne seminarium, praktyki studenckie, konsultacje, list intencyjny, udostępnienie infrastruktury – fizycznej lub chmurowej. Możliwości jest bardzo dużo i nie sposób ich wymienić. Często używamy tych samych słów, nadając im zupełnie różne znaczenia. Dopiero działanie pozwala zweryfikować, czy rzeczywiście mówimy o tym samym.

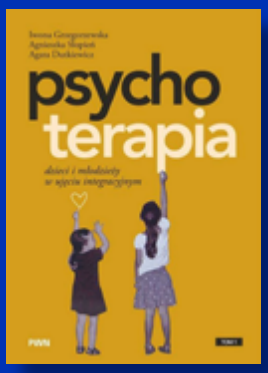
W biznesie obowiązuje prosta zasada: ryzykuj tylko tyle, ile możesz stracić. Podejrzewam, że nie dotyczy ona wyłącznie biznesu. Pytanie brzmi więc: czy stać nas na ryzyko dalszej wiary w kłamstwa o współpracy nauki z biznesem i rezygnację z potencjalnych rezultatów tej współpracy?

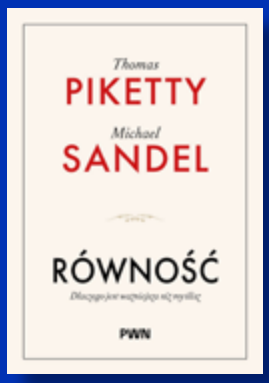
Błażej Roch Żyliński

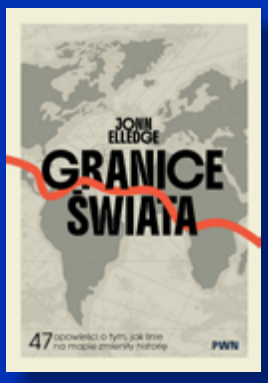
Najemny wynalazca, seryjny przedsiębiorca. Tworzy i komercjalizuje głębokie technologie. Kierownik projektów badawczo-rozwojowych.

Pracował w Laboratorium Mechatroniki i Robotyki Satelitarnej Centrum Badań Kosmicznych PAN. Twórca mTap Smart City dostarczającego inteligentne systemy sterowania oświetleniem miejskim i drogowym. Współpracownik Polskiego Funduszu Rozwoju. Mentor w konsorcjum ENHANCE+ i programie Uczelnie Przyszłości. Doktorant na Wydziale Fizyki Politechniki Warszawskiej. Naukowo zajmuje się sensorami kwantowymi we współpracy z CERN i Uniwersytetem w Zurychu. Obecnie rozwija rozwiązania z zakresu bezpieczeństwa infrastruktury krytycznej (QKZ) i białego wywiadu technologicznego (Deep Tech Space).

NOWOŚCI PWN, KTÓRYCH NIE MOŻNA PRZEGAPIĆ!







SZUKAJ NA KSIEGARNIA.PWN.PL