Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 219–232

https://doi.org/10.4467/20801335PBW.25.010.22176

VARIA

Bezpieczeństwo to wspólna sprawa!

W styczniu 2025 r. Polski Instytut Kontroli Wewnętrznej zorganizował konferencję pt. „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej". O wnioskach płynących z tego spotkania, roli kontroli wewnętrznej i zewnętrznej w zarządzaniu organizacją, dobrych praktykach i wyzwaniach w tym obszarze, jak również o potrzebie podnoszenia świadomości zagrożeń wśród pracowników zatrudnionych w podmiotach objętych statusem infrastruktury krytycznej, z **Ireneuszem Jabłońskim** i **Piotrem Grzybowskim**, członkami zarządu PIKW, rozmawia Daria Olender.

Ireneusz Jabłoński (z lewej) i Piotr Grzybowski

Daria Olender: Co zainspirowało Polski Instytut Kontroli Wewnętrznej do zorganizowania konferencji poświęconej zarządzaniu kryzysowemu i ochronie infrastruktury krytycznej?

Ireneusz Jabłoński: Przede wszystkim dynamicznie zmieniająca się sytuacja geopolityczna na świecie. Mieliśmy do czynienia z pandemią COVID-19, mamy wojnę w bliskim sąsiedztwie i inne konflikty, np. eskalację na linii Izrael–Palestyna. Jako kraj europejski zaczynamy zdawać sobie sprawę z dużego ryzyka zaistnienia zagrożeń i pozamilitarnych, i militarnych, które dotychczas postrzegaliśmy jedynie w kategorii potencjalnych. Pożar mostu Łazienkowskiego w Warszawie w 2015 r. spowodował, że zapaliła się czerwona lampka, zwłaszcza że jako przyczynę ekspertyzy wskazały podpalenie. Minęło kilka lat i doświadczyliśmy niemal symultanicznych pożarów – spłonęły Centrum Handlowe Marywilska 44 i składowiska odpadów, ogień wybuchł w pobliżu dużych fabryk i portów. To pokazało, jak ważne jest kompleksowe zadbanie o to, by nie dochodziło do takich zdarzeń. W PIKW, który zajmuje się problematyką zarządzania organizacją, uznaliśmy, że kwestie ważne dla bezpieczeństwa należy przedyskutować na szerszym forum.

Jesteśmy w przededniu wprowadzenia nowelizacji ustawy o zarządzaniu kryzysowym. Temat idealnie się wpisuje w te komponenty, o których traktuje model COSO opisany w publikacji *Kontrola wewnętrzna – zintegrowana struktura ramowa*[1]. W ramach tego modelu musimy zarządzać ryzykiem, identyfikować je, szacować i oceniać oraz właściwie na nie reagować. Nie można mówić o właściwym zarządzaniu organizacją, jeśli nie weźmie się pod uwagę sytuacji zewnętrznej. Jestem zdania, że jeśli dziś nie zajmiemy się zarządzaniem kryzysowym, to z czasem możemy nie mieć czego audytować i kontrolować. Kiedyś uważałem, że zarządzanie kryzysowe to problem innych, że powinien się o to martwić wojewoda czy inny samorządowiec. Dziś wiem, że to dotyczy każdego z nas. W PIKW doszliśmy do wniosku, że jeżeli w dobie tylu wyzwań i zagrożeń nie zaczniemy się tym tematem bardziej interesować, nie uwzględnimy go w programach naszych szkoleń, to zmniejszy się grono osób, które będą miały właściwe wyobrażenie o roli zarządzania kryzysowego.

[1] *Kontrola wewnętrzna – zintegrowana struktura ramowa*, Warszawa 2008, Polski Instytut Kontroli Wewnętrznej. COSO to akronim od angielskiej nazwy Internal Control – Integrated Framework. Wszystkie przypisy w tekście pochodzą od redakcji.

Podczas konferencji omówiliśmy najważniejsze zagadnienia związane z tym zarządzaniem, prześledziliśmy, jak ewoluuje prawo, by sprostać wyzwaniom dynamicznie zmieniającej się rzeczywistości. Dyskutowaliśmy m.in. o zmianach w polskim prawie, które są podyktowane unijnymi regulacjami – dyrektywą o odporności podmiotów krytycznych, tzw. dyrektywą CER, oraz dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, tzw. dyrektywą NIS 2, a także unijnym rozporządzeniem o cyfrowej odporności operacyjnej, tzw. rozporządzeniem DORA. Mówiliśmy również o ustawie o krajowym systemie cyberbezpieczeństwa, będącej odpowiedzią na dyrektywę NIS 2, a także o cyberbezpieczeństwie, rozwoju nowych technologii i ich wykorzystaniu w ochronie infrastruktury krytycznej. Skorzystam z okazji i podziękuję naszym prelegentom za inspirujące wystąpienia, praktyczne wskazówki i podzielenie się swoim doświadczeniem.

Piotr Grzybowski: Nowelizacja ustawy o zarządzaniu kryzysowym wprowadza wiele istotnych zmian, w tym rozszerzenie listy podmiotów o statusie infrastruktury krytycznej, co pozwoli skuteczniej chronić zasoby i systemy kluczowe dla funkcjonowania państwa. W dobie dynamicznych zmian w sytuacji geopolitycznej, ewoluujących zagrożeń oraz licznych, stale rosnących wyzwań związanych z bezpieczeństwem narodowym, konieczność adaptacji przepisów prawa do nowych realiów wydaje się priorytetem. Istotnym elementem nowelizacji jest ustanowienie funkcji koordynatora bezpieczeństwa infrastruktury krytycznej. Jego rolą będzie nie tylko nadzorowanie działań związanych z ochroną kluczowych zasobów, lecz także zapewnienie spójności i skuteczności podejmowanych działań na poziomie strategicznym. Rozwiązanie to ma na celu wzmocnienie współpracy między podmiotami odpowiedzialnymi za bezpieczeństwo, w tym – sektorem publicznym a prywatnym, co ma się przełożyć na podniesienie poziomu ochrony. To dowodzi rozumienia tego, że ochrona infrastruktury krytycznej jest zadaniem wymagającym zaangażowania wielu interesariuszy i kooperacji na wielu poziomach.

W kontekście organizacji konferencji dodam, że PIKW, którego początki sięgają lat 90., wywodzi się z edukacji. Jednym z naszych kluczowych zadań jest podnoszenie świadomości i szkolenie. Otwieramy oczy na problemy dostępności produktów, funkcjonalności usług, na bezpieczeństwo dnia codziennego, które, mam wrażenie, przez dekady wydawało się dane na zawsze. Woda w kranie, gaz w kuchence, prąd w gniazdku

nie podlegały wątpliwości. A teraz wojna i coraz liczniejsze akty sabotażu czy dywersji uświadomiły nam, że to może zostać zakłócone.

Świadomość konieczności ochrony infrastruktury krytycznej powinna dotyczyć każdego szczebla organizacji, od szeregowego pracownika po kadrę kierowniczą?

P. G.: Tak. Każdy powinien dbać o bezpieczeństwo i wiedzieć, że gramy do jednej bramki. Wydaje mi się, że wiele osób funkcjonuje jakby w uśpieniu – jest jak jest, ale koło toczy się dalej. Uważam, że wielu pracowników podmiotów posiadających infrastrukturę krytyczną nie jest w wystarczającym stopniu uświadamianych, jak ważna jest ich rola, jak istotne znaczenie dla społeczeństwa i państwa ma miejsce ich pracy. W PIKW chodzi nam o to, by osoby, które szkolimy, audytorzy, pełnili później funkcję „przekaźników" – by informowali kadrę kierowniczą danego podmiotu, co jest ważne w jego strukturze. Kierownictwo powinno z kolei przekazywać tę wiedzę podwładnym. Pracownik mający taką świadomość będzie czuł się bardziej odpowiedzialny za to, by dostrzec zaniechania czy niedociągnięcia i je zgłosić. Polityka kadrowa w takich miejscach powinna polegać na tym, by doceniać osoby na najniższych szczeblach.

I. J.: Kiedyś ktoś pokazał audytora w ten sposób, że umieścił w ramach piramidy poszczególne grupy pracowników – od szczebla niższego, przez średni i kierowniczy po prezesa, który znajduje się na samej górze i nie widzi wszystkiego, co się dzieje poniżej. Audytor natomiast stoi z boku i krytycznie przygląda się całości.

P. G.: Jest on osobą, która ma wskazywać luki, czynniki ryzyka. Ma pokazywać, co należy bądź można udoskonalić, a także zwracać uwagę na rolę procesu zarządzania kryzysowego i ochrony infrastruktury, zwłaszcza infrastruktury krytycznej. Ważne jest, by kadra zarządzająca w podmiocie poddanym audytowi ufała jego ocenie. Oczywiście, to od kierownika jednostki zależy, czy wdroży wnioski z audytu, czy zleci dodatkową analizę.

Według jakich kryteriów ocenia się dobre zarządzanie organizacją?

I. J.: Wiedza na ten temat jest zawarta w wytycznych COSO *Kontrola wewnętrzna – zintegrowana struktura ramowa*. Model zarządzania organizacją wynikający z tych wytycznych stanowi fundament działalności PIKW. Na jego kanwie skodyfikowano w ustawie o finansach publicznych[2] pojęcie kontroli zarządczej oraz określono standardy kontroli zarządczej dla sektora finansów publicznych. Wytyczne COSO, opublikowane w 1992 r., zrewidowane i zaktualizowane w 2013 r., pokazują organizację w praktycznym wymiarze oraz odpowiadają na pytanie, jak należy nią skutecznie zarządzać. Wszystkie działania, które obejmuje kontrola wewnętrzna, są realizowane przez człowieka bądź pod jego kontrolą, dlatego zawsze trzeba mieć na uwadze możliwość popełnienia błędów, zmowę pracowników czy niewłaściwe działanie pod presją kierownictwa lub czasu. Kompleksowy model zarządzania, jaki proponuje COSO, składa się z pięciu elementów, tj. środowiska kontroli, oceny ryzyka, działań kontrolnych, informacji i komunikacji, monitoringu. W organizacji powinny one działać w sposób zintegrowany i stwarzać ramy umożliwiające opis i analizę funkcjonującej w organizacji kontroli wewnętrznej, która zapewnia skuteczną realizację celów biznesowych. Polski Instytut Kontroli Wewnętrznej przetłumaczył wytyczne COSO, a następnie stosował i wdrażał rekomendowane rozwiązania w biznesie, jak również w sektorze finansów publicznych w celu zbudowania efektywnie działającego systemu kontroli wewnętrznej.

[2] *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych* (DzU z 2009 r. nr 157 poz. 1240). Zob. także: *Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych* (Dz. Urz. MF z 2009 r. nr 15 poz. 84).

Koncepcja ram COSO

Ramy COSO obejmują kilka ważnych stwierdzeń:

- Kontrola wewnętrzna jest procesem. Jest środkiem prowadzącym do celu, a nie celem samym w sobie.
- Kontrola wewnętrzna zależy od ludzi. To nie tylko polityka, podręczniki i formy, lecz także ludzie na każdym szczeblu organizacji.
- Rola kontroli wewnętrznej polega na dostarczaniu zarządzającym wyłącznie racjonalnego, a nie absolutnego zapewnienia, że cele będą osiągane.
- Kontrola wewnętrzna jest ukierunkowana na osiągnięcie celów organizacji w jednej bądź kilku odrębnych, lecz wzajemnie powiązanych kategoriach.

Pięć elementów ramowych kontroli wewnętrznej

1. Środowisko kontroli – baza dla pozostałych elementów kontroli wewnętrznej, nadaje ton organizacji, wpływając na świadomość. Czynniki środowiska kontroli obejmują uczciwość, wartości etyczne, styl kierownictwa operacyjnego, delegację systemów władzy, a także procesy zarządzania i rozwoju ludzi w organizacji.
2. Ocena ryzyka – bezwzględnie wymaga ustalenia celów organizacji, gdyż każdy podmiot, próbując wykorzystać rynkowe szanse, napotyka zagrożenia (zewnętrzne i wewnętrzne), które muszą zostać poddane ocenie. Identyfikacja i analiza ryzyka stanowią warunek ustalenia, w jaki sposób powinno się nim zarządzać.
3. Kontrola funkcjonowania – obejmuje kontrolę zgodności wielu różnorodnych działań (typu zgody, zezwolenia, weryfikacje, uzgodnienia, przeglądy działalności operacyjnej, podziały obowiązków) z obowiązującymi zasadami, procedurami i zarządzeniami. Działania kontrolne mają wymiar holistyczny – są prowadzone w całej organizacji, na wszystkich szczeblach i we wszystkich funkcjach.
4. Informacja i komunikacja – wymagają precyzji i transparentności. Systemy informacyjne odgrywają wiodącą rolę w systemach kontroli wewnętrznej, gdyż to one tworzą raporty zawierające informacje operacyjne, finansowe oraz te dotyczące zgodności. W szerszym znaczeniu skuteczna komunikacja musi zapewnić przepływ informacji z i do organizacji oraz w organizacji.
5. Monitoring – niezbędny nie tylko do oceny, lecz także do doskonalenia systemu kontroli wewnętrznej. Monitorowane procesy umożliwiają dokonanie oceny wydajności systemu w czasie, a wykrywane niespójności czy niedoskonałości można weryfikować i poprawiać i w ten sposób zapewniać ustawiczne korygowanie systemu.

Rozmawiamy o kontroli wewnętrznej, kontroli zarządczej, audycie. Wyjaśnijmy może, czym się różnią te pojęcia?

I. J.: Kontrola wewnętrzna jako pojęcie odnosi się do biznesu, w administracji natomiast mamy do czynienia z kontrolą zarządczą. Kontrola wewnętrzna to pewnego rodzaju dynamiczny system złożony z wielu mechanizmów i czynności, opisanych w procedurach, zarządzeniach, wymaganiach itd., występujący immanentnie w organizacjach, przedsiębiorstwach oraz jednostkach administracji rządowej i samorządowej. Ma on prowadzić do realizacji celów.

P. G.: Audyt ma charakter uzupełniający względem kontroli wewnętrznej rozumianej jako proces, stanowi element jej monitoringu i nie odpowiada za tę kontrolę. Jest ukierunkowany bardziej na usprawnienie organizacji niż na wykrywanie nieprawidłowości. To intensywnie rozwijający się obszar działania, w którym aktywnie uczestniczymy. Ideę audytu wewnętrznego zaczerpnęliśmy 20 lat temu z Zachodu i na dobre zagościła ona w naszym kraju wraz z przystąpieniem Polski do Unii Europejskiej.

I. J.: Dodam, że jest kontrola wewnętrzna jako proces, tj. z pięcioma elementami ramowymi, ale jest też kontrola wewnętrzna instytucjonalna, czyli komórka kontroli wewnętrznej, której pracownicy są odpowiedzialni za monitorowanie oraz wykrywanie naruszeń i incydentów i zapobieganie im.

P. G.: Ten model zarządzania, te pięć komponentów kontroli wewnętrznej, można odnieść także do organizacji zarządzającej infrastrukturą krytyczną, w której wszystko powinno być poukładane i spójne, aby zwiększyć gwarancję prawidłowego działania. Czasami rodzi to przesadę. Mamy np. teren, który kilka czy kilkanaście lat temu był przeznaczony pod infrastrukturę krytyczną, a teraz to puste pole, ale nadal strzeżone. Mamy etat, trzeba go wypełnić, mamy pieniądze pod koniec roku, trzeba je wydać, mimo że z początkiem kolejnego można byłoby je przeznaczyć na bardziej uzasadnioną inwestycję. To pokazuje, że nie zawsze właściwie wykorzystujemy siły i środki. Należy zatem bardziej skupić się na tym, czemu coś ma służyć, dostosować przepisy prawa, opracować adekwatne procedury, przeprowadzić konsultacje społeczne.

I. J.: We współpracy z Pawłem Cybulskim, byłym wiceministrem finansów oraz szefem Krajowej Administracji Skarbowej, opracowaliśmy

i wdrożyliśmy nowatorską procedurę kontroli biznesowej. Jej wdrożenie daje przedsiębiorcy solidne fundamenty do eliminowania nadużyć oraz świadczy o jego rzetelności i dobrej organizacji. Dzięki takiej procedurze firma może przedstawić inspektorowi kontroli skarbowej jasne, uporządkowane zasady działania i udowodnić, że podejmuje realne działania w zakresie zarządzania ryzykiem podatkowym. To było – i nadal jest – ważnym elementem budowania wiarygodności przedsiębiorstwa wobec organów administracji publicznej. W późniejszym etapie została wdrożona w Ministerstwie Finansów tzw. biała lista podatników VAT, która znacznie zwiększyła transparentność relacji gospodarczych. Ukazały się też wytyczne wskazujące na najistotniejsze elementy niezbędne do poprawnej weryfikacji własnych kontrahentów. Wspomniana procedura kontroli biznesowej to weryfikowanie kontrahenta zarówno pod kątem jego obecności na tej liście, jak i jego ogólnej kondycji finansowej, scoringu[3] oraz potencjalnych czynników ryzyka, które mogą się z nim wiązać. Świadome zarządzanie relacjami biznesowymi stało się więc nie tylko elementem dobrej praktyki, lecz także formą zabezpieczenia przed nieświadomym udziałem w mechanizmach wyłudzeń czy nadużyć podatkowych.

P. G.: Weryfikacja kontrahentów jest bardzo istotna zwłaszcza tam, gdzie w grę wchodzi bezpieczeństwo dostaw produktów i usług zapewniających funkcjonowanie strategiczne i rozwój państwa. Tam bezwzględnie należy być nadmiernie ostrożnym.

Wróćmy jeszcze do konferencji. Czy zaskoczyło Panów zainteresowanie tym spotkaniem?

I. J.: Tak, było naprawdę duże, zwłaszcza ze strony odbiorców ze wschodnich województw – z Podkarpacia, Podlasia i Lubelszczyzny. Uczestnicy podkreślali, że ważnym aspektem ich działalności jest świadomość w zakresie nowych wyzwań i zagrożeń, a także wiedza o działaniach, które mogą podjąć na poziomie lokalnym, by zminimalizować ryzyko, zwiększyć bezpieczeństwo bądź przynajmniej utrzymać je na akceptowalnym poziomie. Wydaje mi się, że uruchomiliśmy tym wydarzeniem pewien proces – rozpaliliśmy umysły tych, którzy do tej pory nie zdawali sobie sprawy z pewnych problemów, ale też tych, którzy mieli już ich

[3] Scoring – metoda oceny wiarygodności kredytowej.

świadomość, ale poszukiwali nowych rozwiązań. Dodam, że konferencja miała wyłącznie formułę stacjonarną, przygotowania do niej rozpoczęliśmy późno i nie była intensywnie promowana, więc tak duża frekwencja była dla nas zaskoczeniem.

P. G.: Tematyka zarządzania ryzykiem i ochrony infrastruktury krytycznej najwyraźniej jest aktualna dla wielu grup. Wolności i bezpieczeństwa nie dostaliśmy na zawsze i nie będziemy ich mieć, jeśli nie będziemy o nie dbać. Wymagamy tego od odpowiednich instytucji i podmiotów, zatem czują się one zobligowane do pogłębiania swojej wiedzy, poznawania nowych mechanizmów służących temu, aby jak najlepiej zabezpieczyć ciągłość dostaw usług kluczowych czy produktów niezbędnych do życia.

> **Duża popularność wydarzenia potwierdza potrzebę organizowania tego typu spotkań w gronie kontrolerów i audytorów. W mojej ocenie brak formuły online był właściwą decyzją. Dzięki temu mogły zostać poruszone tematy związane z bezpieczeństwem, które nie powinny trafić w eter.**

I. J.: Takie spotkania to świetna platforma wymiany doświadczeń i wzajemnych inspiracji. Uczestnicy konferencji podkreślali, że była to unikalna okazja, by wspólnie przeanalizować proponowane zmiany i wypracować rekomendacje odpowiadające wyzwaniom – tym aktualnym, i tym prognozowanym. Wśród naszych gości byli analitycy, umysły ścisłe, osoby, które znają technologie, produkcję, ale brakuje im wiedzy na temat całokształtu bezpieczeństwa. Wielu z nich doceniło odmienne doświadczenia prelegentów – ze sfery cyber, militarnej, metodyki ryzyka, ochrony środowiska, finansów czy spółek działających w różnych obszarach gospodarki. Przedstawienie bezpieczeństwa z kilku stron – od ochrony i kamer, przez zabezpieczenia w sferze prawnej czy cyber, po pracowników dopuszczających się sabotażu, czyli tzw. sześciopaku bezpieczeństwa, okazało się dobrym pomysłem. Uczestnicy chwalili też otwartość prelegentów na głosy z sali, dzięki czemu nie zabrakło pytań, ciekawych dyskusji i konstruktywnych wniosków ze strony przedstawicieli różnych branż i sektorów. Dotarcie do rynku z informacją to jedno, dotarcie skuteczne, czyli przekazanie jej w sposób zrozumiały dla odbiorcy, to drugie. Byli i tacy, którzy przyznali, że przed przyjściem na konferencję nie mieli świadomości wielu rzeczy, mimo że reprezentują podmiot ważny z punktu widzenia bezpieczeństwa państwa.

P. G.: Chciałbym dodać, że wśród pracowników jest teraz tendencja do hermetyczności, skupiania się na sobie i wąskim obszarze swojego działania. A praca w miejscu, które wiąże się np. z zapewnieniem ciągłości dostaw, wymaga szerszego myślenia. Bardzo często pracownicy zapominają o roli instytucji, w której pracują, a kierownicy o wadze tego, co nadzorują, że to nie są przykładowo tylko dwa tory i podsyp, lecz infrastruktura krytyczna o znaczeniu strategicznym. Podczas konferencji dyskutowaliśmy również o jednostkach wojskowych. Okazuje się, że strzegą nas wojskowi, których strzeże cywilny ochroniarz. To absurd. I nie twierdzę, że taki ochroniarz nie może być świetnie wyszkolony, ale to powinno podlegać weryfikacji.

W kuluarach miałem okazję porozmawiać o problemie, jakim jest utrzymanie ciągłości zarządzania organizacją. Niech dochodzi do zmian na stanowiskach kierowniczych, ale średni szczebel powinien realizować długofalową politykę firmy. W praktyce natomiast często mamy do czynienia z cykliczną wymianą. Nowi pracownicy dopiero się uczą, a tych doświadczonych już nie ma. Ktoś coś wcześniej zaczął, potem się tego nie kończy. A bywa też tak, że skoro tamci zaczęli, to trzeba to porzucić, bo pewnie było złe. W ten sposób powstaje chaos. Nierzadko wynika to z nadania politycznego. Taki nominat nie myśli długoterminowo, dba wyłącznie o tu i teraz. I tu otwiera się kolejny temat – planowanie strategiczne. Wektor bezpieczeństwa powinien być jednoznaczny i zapewniać stabilizację. Jeśli następuje zmiana kierunku myślenia, to musi ona mieć racjonalne uzasadnienie. Nie powinno być tak, że każda zmiana na kluczowych stanowiskach czy zmiana władzy powoduje rewolucję w funkcjonowaniu organizacji, gdyż to hamuje rozwój podmiotu, a czasem wręcz go uwstecznia. Rosnąca liczba obiektów o ważnym czy kluczowym znaczeniu dla bezpieczeństwa kraju wymaga uświadamiania pracowników – co już kilkukrotnie podkreślaliśmy – jak ważne jest ich miejsce i rola w systemie bezpieczeństwa państwa. Muszą mieć oczy szeroko otwarte i dostrzegać niebezpieczeństwa – i te rzeczywiste, i te ewentualne. Takie konferencje czy szkolenia powinny być cykliczne, by myślenie o bezpieczeństwie – również przez pryzmat wyzwań i zagrożeń – było na porządku dziennym i prowadziło do pewnego automatyzmu w działaniu. Warto np. przeprowadzać ćwiczenia ewakuacyjne czy ćwiczenia tzw. pamięci mięśniowej. To pozwoli minimalizować ryzyko, wykrywać i badać słabe strony, luki, podatności i dywersyfikować odpowiedzi na nie.

Jednym z walorów tej konferencji było zgromadzenie ludzi z doświadczeniem. Nawet ci prelegenci, którzy mieli stopnie naukowe, byli jednocześnie praktykami.

I. J.: Tego nauczyła nas organizacja studiów podyplomowych. Zrozumieliśmy, że na tym szczeblu edukacji kształcący się poszukują wykładowców z doświadczeniem praktycznym. Zaczynaliśmy od podziału pół na pół, jeśli chodzi o kadrę uczelnianą i praktyków, ale szybko się okazało, że ci pierwsi powielali materiał ze studiów I czy II stopnia bądź przekazywali suchy materiał. Kadra z zewnątrz wzbogacała go przykładami z pracy i służby, co pozwalało na unaocznienie problemów i sprzyjało podejmowaniu dyskusji.

P. G.: Wychodzimy z założenia, że studia podyplomowe mają dostarczyć narzędzi do pracy. Oczywiście, nie wykluczamy ludzi nauki, bo jeśli teoria współgra z praktyką, to mamy idealne połączenie. Można wtedy szerzej spojrzeć na dane zjawisko, powiązać różne jego aspekty. Staramy się angażować do współpracy osoby, które łączą nie tylko wiedzę i doświadczenie, lecz także umiejętność przekazu.

W konferencji wzięli udział, m.in. jako prelegenci, byli funkcjonariusze formacji mundurowych, służb, inspekcji i straży. Są oni szkoleniowcami również na kursach i studiach podyplomowych prowadzonych przez PIKW. Jak oceniają Panowie tę współpracę?

I. J.: W naszej działalności chętnie korzystamy ze wsparcia byłych i obecnych funkcjonariuszy i żołnierzy. Połączenie wiedzy i doświadczenia jest – jak już powiedziałem – bezcenne. Praktycy dają gotowe *case study*, a uczestnicy szkoleń mogą to przenieść na własny grunt, zweryfikować swój punkt widzenia. Dla nas pionierem takiej formuły szkoleniowej był insp. Marek Dyjasz, były dyrektor Biura Kryminalnego Komendy Głównej Policji. Opracował on szkolenie „Weryfikacja autentyczności dokumentów", które było impulsem do zmian na rynku. Obecnie na pozyskiwanie i analizę informacji patrzy się inaczej.

P. G.: Jako jedni z pierwszych zachęcaliśmy przedstawicieli służb do tego, by dzielili się swoją wiedzą i umiejętnościami. Dobrze jest, gdy audytor, będący kimś w rodzaju cywilnego policjanta, może rozwijać swoje umiejętności, ucząc się od tych, którzy dysponują zapleczem praktycznym. My to szkolenie uzupełniamy o wiedzę psychologiczną,

umiejętności miękkie, czerpiąc m.in. od psychologów policyjnych. Ta wymiana, w mojej ocenie, jest korzystna dla obu stron, gdyż dzięki takim spotkaniom funkcjonariusze mogą poszerzyć swoje wyobrażenie o tym, jakie są rzeczywiste, aktualne problemy. To wartość dodana.

Czy taka aktywność funkcjonariuszy wpływa waszym zdaniem na bardziej pozytywny odbiór służb?

P. G.: Zdecydowanie tak. Na tym rynku często funkcjonują ludzie, którzy są pasjonatami. Funkcjonariusze, którzy brali udział w konferencji czy nasi szkoleniowcy, to osoby z charyzmą. A tego właśnie oczekuje audytorium.

***

Ireneusz Jabłoński

Doświadczony trener biznesu w zakresie miękkich aspektów zarządzania organizacją. Członek zarządu i dyrektor operacyjny w Polskim Instytucie Kontroli Wewnętrznej, z którym jest związany od 20 lat. Posiada wykształcenie wyższe na kierunku zarządzanie, ze specjalizacją z psychologii zarządzania. Był trenerem wewnętrznym w koncernie energetycznym Vattenfall, uczestniczył w procesie prywatyzacji i restrukturyzacji Elektrociepłowni Warszawskich, następnie pracował jako menedżer HR w Totalizatorze Sportowym.

Piotr Grzybowski

Członek zarządu w Polskim Instytucie Kontroli Wewnętrznej, z którym jest związany od ponad 20 lat. Odpowiada głównie za finanse, usługi doradcze oraz organizację jednego z największych i najstarszych w Polsce branżowych wydarzeń konferencyjnych, jakim jest Międzynarodowy Kongres Kontroli, Audytu Wewnętrznego, Antykorupcji i Zwalczania Oszustw.

***

Konferencja „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej"

Warszawa, 22 stycznia 2025 r.

Infrastruktura krytyczna to krwiobieg naszego kraju, który dostarcza niezbędnych składników do życia. Jeśli przestanie funkcjonować, to wszystko inne również nie będzie mogło właściwie działać i spełniać swoich zadań lub celów.

Od elektrowni po sieci wodociągowe – nasza infrastruktura jest jak dom, który trzeba stale remontować i zabezpieczać. Ta konferencja to mapa drogowa do bezpieczniejszej przyszłości.

Mariusz Brzozowski, ekspert ds. antyterrorystycznej ochrony IK

Konferencja pt. „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej", w której wzięło udział 120 osób, zgromadziła specjalistów z obszaru bezpieczeństwa infrastruktury krytycznej. Problematyka poruszana podczas konferencji została zgrupowana w czterech blokach tematycznych.

Blok I – „Nowy porządek legislacyjny w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej", obejmujący wystąpienia:

1. „CER – nowatorskie rozwiązania w zarządzaniu bezpieczeństwem infrastruktury krytycznej".
2. „NIS 2 i DORA – dlaczego są istotne?".

Blok II – „Rozwój nowych technologii i ich wpływ na bezpieczeństwo", obejmujący wystąpienia:

1. „Zagrożenia cyber dla kluczowej infrastruktury RP".
2. „Cyberbezpieczeństwo z perspektywy atakującego. Zobacz, gdzie jest uchylone okno".
3. „Najlepszy zamek jest bezużyteczny, gdy stracimy klucze – bezpieczna orkiestracja kluczami kryptograficznymi".

Blok III – „Rozwój zasobów niezbędnych do życia – nowe wyzwania – nowe ramy prawne do ich ochrony", obejmujący wystąpienia:

1. „Ochrona transgranicznych inwestycji energetycznych".
2. „AI – jak wykorzystać potencjał rozwoju nowej technologii w bezpieczeństwie?".

Blok IV – „Połączenia potencjału wojskowego z cywilnym w ochronie infrastruktury krytycznej", obejmujący wystąpienia:

1. „Perspektywy zarządzania bezpieczeństwem morskiej infrastruktury krytycznej – koncepcja Cyfrowego Bałtyku".
2. „Zagrożenia wywiadowcze dla obiektów wojskowych i cywilnych – insider".

Uzupełnieniem wykładów były panele dyskusyjne z udziałem ekspertów reprezentujących różne obszary bezpieczeństwa.

Zdjęcie 1. Michał Krzykowski, prawnik, kierownik Laboratorium Infrastruktury Krytycznej i Energetyki WPiA UWM.

Zdjęcie 2. Radosław Kucik, ekspert ds. bezpieczeństwa, dyrektor sprzedaży w firmie Pentera.

Zdjęcie 3. Od lewej: Anna Mroczek (PGE S.A., PGE Baltica Sp. z o.o.), Artur Gębicz (IPS-SGB), Włodzimierz Cieślak (ekspert PISA), Gabriela Barwińska-Szczutkowska (RDOŚ w Bydgoszczy).

Zdjęcie 4. Alicja Hoc-Rolińska i Ireneusz Jabłoński z PIKW, prowadzący.

Zdjęcie 5. Paweł Cybulski, były wiceminister finansów i zastępca szefa Krajowej Administracji Skarbowej.

Źródło: materiały własne.