SAFETY PROJECT

NATO OTAN
Defence Education Enhancement Programme (DEEP) eAcademy

PIBiO

XXI OGÓLNOPOLSKIE WARSZTATY PRAKTYCZNO-TECHNICZNE

BEZPŁATNE I CERTYFIKOWANE WYDARZENIE ONLINE

Nowelizacja ustawy

o ZK epizod II

Praktyczne wdrożenie nowych obowiązków

ADMINISTRACJI, OPERATORÓW IK I PODMIOTÓW KRYTYCZNYCH

7 WRZEŚNIA | 10:00–14:00 | PLATFORMA CLICKMEETING

XXI Ogólnopolskie Warsztaty Praktyczno-Techniczne

Nowelizacja ustawy o ZK epizod II

– praktyczne wdrożenie nowych obowiązków administracji, operatorów IK i podmiotów krytycznych

Czas i miejsce:

- 7 września 2026 roku – 10.00-14.00
- Platforma ClickMeeting – udział otwarty i bezpłatny, ograniczony do 5 000 uczestników
- Zapisy: https://safetyproject.pl/wydarzenia/xxi-ogolnopolskie-warsztaty-praktyczno-techniczne/

Organizatorzy:

- Safety Project sp. z o.o.
- Fundacja Polski Instytut Bezpieczeństwa i Obronności we Wrocławiu

Wsparcie organizacyjno-merytoryczne:

- Polska Izba Systemów Alarmowych
- Polska Izba Systemów Bezzałogowych
- Polska Izba Ochrony

Patronaty honorowe:

- Dyrektor NATO Deep eAcademy

Problematyka warsztatów:

1. Jak skutecznie przygotować administrację publiczną do wdrożenia nowych obowiązków wynikających z nowelizacji ustawy o zarządzaniu kryzysowym?
2. Jak identyfikować, chronić i rozwijać infrastrukturę krytyczną zgodnie z nowymi wymaganiami prawnymi i organizacyjnymi?
3. Jak zbudować system bezpieczeństwa i odporności podmiotu krytycznego spełniający wymagania ustawy oraz dyrektywy CER?
4. Jak wdrożyć zintegrowany system bezpieczeństwa obejmujący bezpieczeństwo fizyczne, techniczne, osobowe, cyberbezpieczeństwo, bezpieczeństwo prawne oraz ciągłość działania?
5. Jak przygotować organizację oraz jej liderów bezpieczeństwa do pełnienia nowych funkcji koordynatora ochrony IK i pełnomocnika bezpieczeństwa podmiotu krytycznego?
6. Jak zbudować nowoczesny i spójny system odporności państwa, administracji oraz organizacji po wejściu w życie nowych przepisów?

Adresaci Warsztatów:

- Zarządzający i liderzy bezpieczeństwa infrastruktury krytycznej oraz podmiotów krytycznych;
- Przedstawiciele zarządów, rad nadzorczych i kadry kierowniczej przedsiębiorstw komunalnych, wod-kan, energetycznych, transportowych, produkcyjnych i usługowych;
- Kierownicy bezpieczeństwa, pełnomocnicy ds. ochrony informacji niejawnych, IK, ZK, ciągłości działania i cyberbezpieczeństwa;
- Przedstawiciele administracji rządowej i samorządowej odpowiedzialni za organizację OLiOC oraz ZK
- Wojewodowie, starostowie, wójtowie, burmistrzowie, prezydenci oraz kadra kierownicza urzędów;
- Przedstawiciele organów, podmiotów i zasobów OLiOC.

Wartość warsztatów:

- Aktualna i zweryfikowana wiedza dotycząca nowelizacji ustawy o ZK oraz nowych regulacji dotyczących IK i podmiotów krytycznych;
- Praktyczna mapa drogowa wdrożenia nowych obowiązków dla administracji publicznej, operatorów IK oraz podmiotów krytycznych;
- Omówienie nowych obowiązków związanych z oceną ryzyka, planowaniem, ochroną IK, budowaniem odporności oraz audytami;
- Praktyczne rozwiązania dotyczące projektowania zintegrowanych systemów bezpieczeństwa obejmujących bezpieczeństwo fizyczne, techniczne, osobowe, cyberbezpieczeństwo, bezpieczeństwo prawne i ciągłość działania;
- Możliwość zadawania pytań ekspertom oraz konsultacji konkretnych problemów wdrożeniowych dotyczących nowych przepisów;
- Elektroniczny pakiet materiałów, źródeł wiedzy oraz rekomendacji wdrożeniowych przygotowanych przez ekspertów;
- Imienny certyfikat uczestnictwa oraz możliwość otrzymania materiałów edukacyjnych i publikacji eksperckich;
- Udział w formule otwartej i bezpłatnej.

Komitet Organizacyjny Warsztatów:

- mjr rez. dr hab. inż. Jarosław Stelmach, prof. uczelni – Przewodniczący Komitetu Organizacyjnego
- Alicja Błędowska – Zastępca Przewodniczącego Komitetu Organizacyjnego i Kierownik Projektu
- Radosław Woźniak, Damian Ucieszyński – Kierownicy Merytoryczni
- Patrycja Stelmach – Specjalista ds. komunikacji i marketingu

Kontakt:

- Sekretariat Warsztatów, tel. (+48) 574 800 166, e-mail: kongres@safeplace.edu.pl

Plan warsztatów

Godzina	Temat
10:00 – 10:30	**Otwarcie warsztatów** dr hab. Piotr Gawliczek, d.h.c. multi – NATO DEEP eAcademy mjr rez. dr hab. inż. Jarosław Stelmach, prof. uczelni – Safety Project
10:30 – 11:00	**Praktyczny wymiar nowelizacji ustawy o ZK** ● Jakie zmiany wprowadza ustawa w zakresie planowania cywilnego? ● Jakie zmiany wprowadza ustawa w zakresie IK i podmiotów krytycznych? ● Jak budować odporność IK i podmiotów krytycznych wg nowych rozwiązań ustawowych? ● Jakie akty wykonawcze już obowiązują i jakie to powoduje konsekwencje dla ludzi i liderów bezpieczeństwa? ● Pytania, wnioski i podsumowanie **Prowadzący:** mjr rez. dr hab. inż. Jarosław Stelmach, prof. uczelni – Safety Project
11:00 – 11:20	**Bezpieczeństwo fizyczne: Projektowanie i organizacja systemu bezpieczeństwa fizycznego infrastruktury krytycznej zgodnie z minimalnymi wymaganiami ochrony** **Zagadnienia:** 1. Jak prawidłowo projektować system bezpieczeństwa fizycznego na podstawie analizy zagrożeń i szacowania ryzyka? 2. W jaki sposób wyznaczać strefy ochrony oraz określać zasady kontroli dostępu osób, pojazdów i materiałów? 3. Jak integrować ochronę fizyczną, zabezpieczenia techniczne oraz procedury reagowania w jeden spójny system bezpieczeństwa? 4. Jak projektować ochronę przed współczesnymi zagrożeniami, w tym atakami z wykorzystaniem BSP oraz pojazdów? 5. Jak przygotować organizację do audytów i oceny zgodności systemu bezpieczeństwa fizycznego? **Prowadzący:** mjr rez. dr hab. inż. Jarosław Stelmach, prof. uczelni – Safety Project Marcin Kożuszek – Safety Project

11:20 – 11.40	**Bezpieczeństwo techniczne. Zapewnienie niezawodności technicznej infrastruktury krytycznej oraz odporności procesów technologicznych** **Zagadnienia:** 1. Jak identyfikować krytyczne elementy infrastruktury oraz techniczne punkty awarii? 2. Jak projektować redundancję urządzeń, instalacji i systemów wspierających ciągłość działania? 3. Jak organizować utrzymanie techniczne infrastruktury z wykorzystaniem analizy ryzyka? 4. Jak zapewnić odporność infrastruktury na utratę zasilania, mediów oraz systemów transmisji danych? 5. Jak budować strukturę zarządzania bezpieczeństwem technicznym operatora? **Prowadzący:** Przedstawiciel pionu technicznego IK
11.40 – 12.00	**Bezpieczeństwo osobowe. Bezpieczeństwo osobowe jako element budowania odporności infrastruktury krytycznej** Zagadnienia 1. Jak skutecznie zarządzać ryzykiem związanym z personelem własnym, usługodawcami i podwykonawcami? 2. Jak organizować proces weryfikacji kompetencji, kwalifikacji oraz dostępu do infrastruktury? 3. Jak projektować system uprawnień oraz zarządzania dostępem do obiektów i informacji? 4. Jak ograniczać zagrożenia wewnętrzne (Insider Threat) w organizacji? 5. Jak budować kulturę bezpieczeństwa poprzez szkolenia i rozwój kompetencji personelu? **Prowadzący:** Przedstawiciel kancelarii prawnej
12.00-12.20	**Cyberbezpieczeństwo. Cyberbezpieczeństwo infrastruktury krytycznej – integracja środowisk IT, OT oraz usług chmurowych** Zagadnienia 1. Jak budować architekturę cyberbezpieczeństwa zgodną z wymaganiami nowych regulacji? 2. Jak zabezpieczać systemy sterowania przemysłowego (OT) przed współczesnymi zagrożeniami? 3. Jak bezpiecznie zarządzać dostępem zdalnym, serwisem oraz podwykonawcami? 4. Jak przygotować organizację do reagowania na incydenty cyberbezpieczeństwa i odbudowy zasobów? **5.** Jak wykorzystać wymagania norm ISO/IEC 27001, IEC 62443 i ISO 22301 podczas wdrażania systemu bezpieczeństwa? **Prowadzący:** **Przedstawiciel PISA**

12.20 – 12.40	**Bezpieczeństwo prawne. Bezpieczeństwo prawne operatora infrastruktury krytycznej – zgodność regulacyjna oraz zarządzanie ryzykiem kontraktowym** **Zagadnienia** 1. Jak zorganizować system monitorowania zmian przepisów dotyczących IK i podmiotów krytycznych? 2. Jak ograniczać ryzyko prawne wynikające z umów zawieranych z dostawcami i usługodawcami? 3. Jak zabezpieczać kluczowe zasoby organizacji od strony własnościowej, kontraktowej i regulacyjnej? 4. Jak przygotować organizację do współpracy z organami administracji oraz realizacji obowiązków raportowych? 5. Jak ograniczać ryzyko uzależnienia od pojedynczych dostawców technologii i usług? **Prowadzący:** **Przedstawiciel kancelarii prawnej**
12.40 – 13.00	**Ciągłość działania. System zarządzania ciągłością działania jako fundament odporności infrastruktury krytycznej** **Zagadnienia** 1. Jak przeprowadzić analizę wpływu na działalność (BIA) oraz identyfikację procesów krytycznych? 2. Jak projektować strategię ciągłości działania zgodnie z wymaganiami nowelizacji ustawy o ZK? 3. Jak opracować plan ciągłości działania, plan zarządzania kryzysowego oraz procedury odtworzeniowe? 4. Jak planować i prowadzić testy oraz doskonalenie systemu ciągłości działania? 5. Jak zintegrować BCM z bezpieczeństwem fizycznym, technicznym, cyberbezpieczeństwem oraz zarządzaniem kryzysowym? **Prowadzący:** **Przedstawiciel infrastruktury krytycznej**
13:00 - 14:00	**Debata ekspercka** **Nowy model zarządzania kryzysowego i odporności państwa – czy administracja, operatorzy IK i podmioty krytyczne są przygotowani do wdrożenia nowych przepisów?** **Moderator:** mjr rez. dr hab. inż. Jarosław Stelmach, prof. uczelni – Safety Project **Zaproszeni goście:** Przedstawiciele PISA, PIO, PISB Przedstawiciele samorządów Przedstawiciele IK **Zagadnienia:** ● Jakie będą największe wyzwania administracji rządowej i samorządowej związane z wdrożeniem nowelizacji ustawy o ZK ● Czy operatorzy IK oraz inwestorzy potencjalnej IK są przygotowani do realizacji nowych obowiązków wynikających z ustawy oraz projektowanych aktów wykonawczych? ● Jak budować odporność – procesowo czy projektowo i co jest punktem wyjścia tych działań? ● Jaką rolę powinien pełnić lider bezpieczeństwa w nowym systemie odporności państwa? ● Jakie działania należy podjąć w ciągu najbliższych 12 miesięcy? ● Sesja pytań i odpowiedzi.

14:00	Zakończenie warsztatów Ogłoszenie zwycięzców konkursów i losowań Wirtualne wręczenie nagród i pamiątek