PROJEKT REKOMENDACJI
DOTYCZĄCYCH KOMPETENCJI
MIĘDZYBRANŻOWYCH Z OBSZARU

Wzmacnianie bezpieczeństwa cyfrowego w środowisku Pracy w MŚP

5 MAJA 2026

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

NASK PIB

Paweł Zegarow

EKSPERT DS. ANALIZ STATEGICZNYCH Z OBSZARU CYBERBEZPIECZEŃSTWA

- Od 7 lat pracuję na rzecz CSIRTU NASK.
- Specjalizuję się w krajowych i europejskich regulacjach z obszaru cyberbezpieczeństwa, a także w problematyce czynnika ludzkiego, cyberpsychologii oraz podejściu human-centered cybersecurity.
- Prowadzę działania związane z budową i rozwojem partnerstwa strategicznego - Program Partnerstwo dla Cyberbezpieczeństwa (PdC NASK).
- Posiadam wieloletnie doświadczenie dydaktyczne.
- Regularnie występuję jako prelegent na wydarzeniach branżowych.
- Jestem absolwentem programu International Visitor Leadership Program realizowanego przez United States Department of State.
- Jestem członkiem zespołu ekspertów CyberNET EU.

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

Wzmacnianie bezpieczeństwa cyfrowego w środowisku pracy w MŚP

Kompetencja przeznaczona jest dla przedsiębiorców oraz pracowników sektora mikro, małych i średnich przedsiębiorstw, którzy w codziennej pracy korzystają z poczty elektronicznej, systemów online, bankowości elektronicznej oraz narzędzi komunikacji cyfrowej.

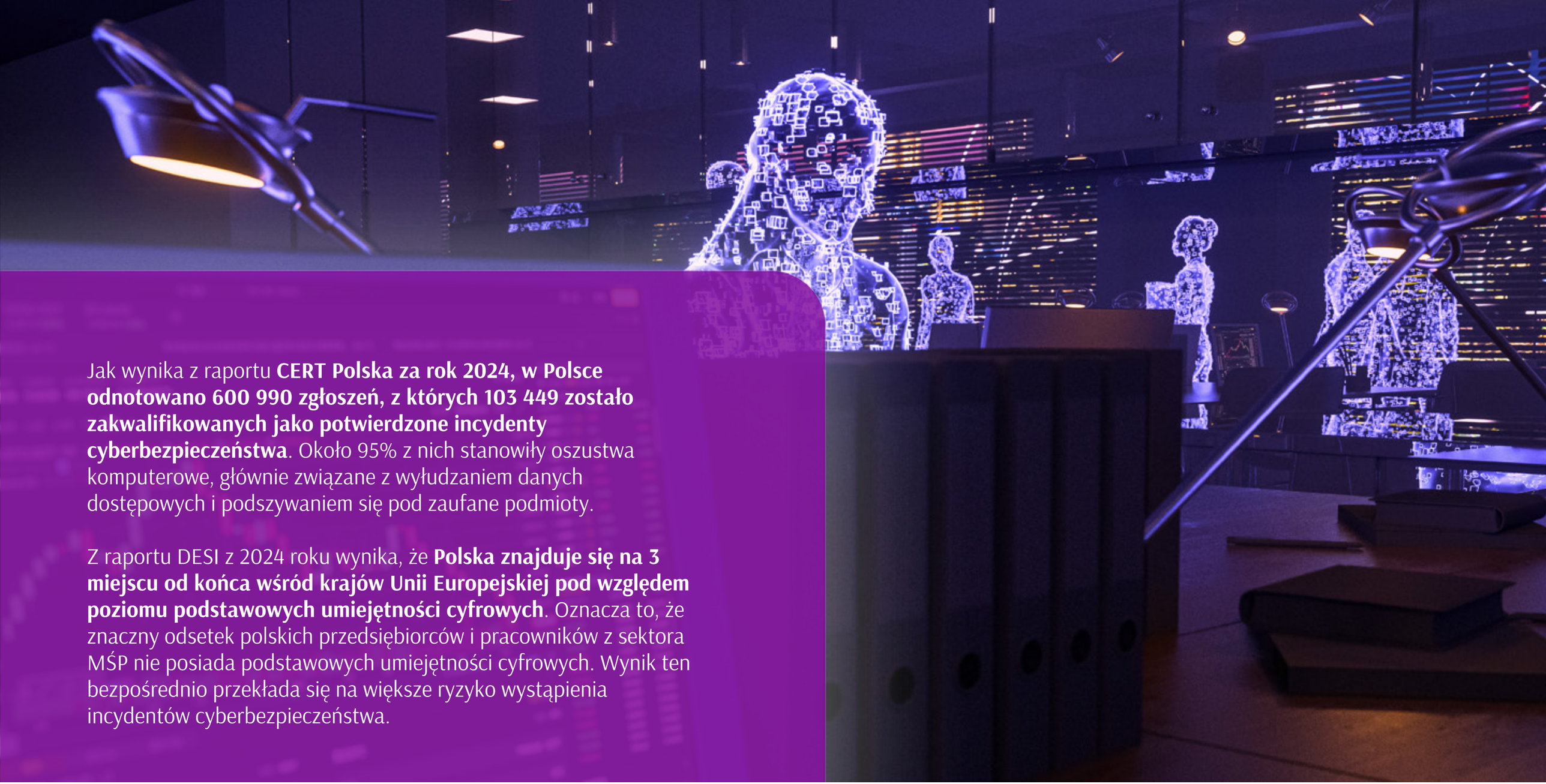
Celem uzyskania kompetencji jest rozwinięcie wiedzy i umiejętności umożliwiających:

- identyfikowanie i analizowanie oszustw komputerowych;
- stosowanie zasad cyberhigieny w środowisku pracy, w szczególności w zakresie bezpiecznego korzystania z urządzeń, systemów, sieci oraz ochrony dostępu i danych;
- rozpoznawanie i analizowanie mechanizmów manipulacji psychologicznej wykorzystywanych w atakach socjotechnicznych oraz podejmowanie decyzji ograniczających podatność na tego typu zagrożenia;
- bezpieczne przetwarzanie, przechowywanie oraz udostępnianie danych i informacji w działalności przedsiębiorstwa;
- identyfikowanie incydentów cyberbezpieczeństwa oraz podejmowanie podstawowych działań ograniczających ich skutki w środowisku pracy.

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

Wzmacnianie kompetencji w zakresie cyberbezpieczeństwa jest szczególnie istotne **wśród osób niebędących specjalistami IT, ponieważ to one najczęściej obsługują kluczowe procesy operacyjne,** a także stanowią pierwszą linię kontaktu z potencjalnymi zagrożeniami w sektorze mikro, małych i średnich przedsiębiorstw.

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



Jak wynika z raportu **CERT Polska za rok 2024, w Polsce odnotowano 600 990 zgłoszeń, z których 103 449 zostało zakwalifikowanych jako potwierdzone incydenty cyberbezpieczeństwa**. Około 95% z nich stanowiły oszustwa komputerowe, głównie związane z wyłudzaniem danych dostępowych i podszywaniem się pod zaufane podmioty.

Z raportu DESI z 2024 roku wynika, że **Polska znajduje się na 3 miejscu od końca wśród krajów Unii Europejskiej pod względem poziomu podstawowych umiejętności cyfrowych**. Oznacza to, że znaczny odsetek polskich przedsiębiorców i pracowników z sektora MŚP nie posiada podstawowych umiejętności cyfrowych. Wynik ten bezpośrednio przekłada się na większe ryzyko wystąpienia incydentów cyberbezpieczeństwa.

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

Obszary kompetencji

Szkolenie trwa 56 godzin i składa się z niezależnych bloków, które mogą być elastycznie łączone w zależności od potrzeb uczestników oraz specyfiki stanowiska pracy. Blokowa organizacja szkolenia pozwala na delegowanie pracowników na krótsze, jedno- lub dwudniowe bloki szkoleniowe, co ogranicza wpływ na bieżące funkcjonowanie przedsiębiorstwa. Natomiast, w odniesieniu do właścicieli oraz osób zarządzających w sektorze mikro, małych i średnich przedsiębiorstw zalecamy szkolenie w formie spójnego programu obejmujące wszystkie bloki

Obszar A

Rozpoznawanie oszustw komputerowych

Obszar B

Cyberhigiena

Obszar C

Wzmacnianie odporności na socjotechniki wykorzystywane przez cyberprzestępców

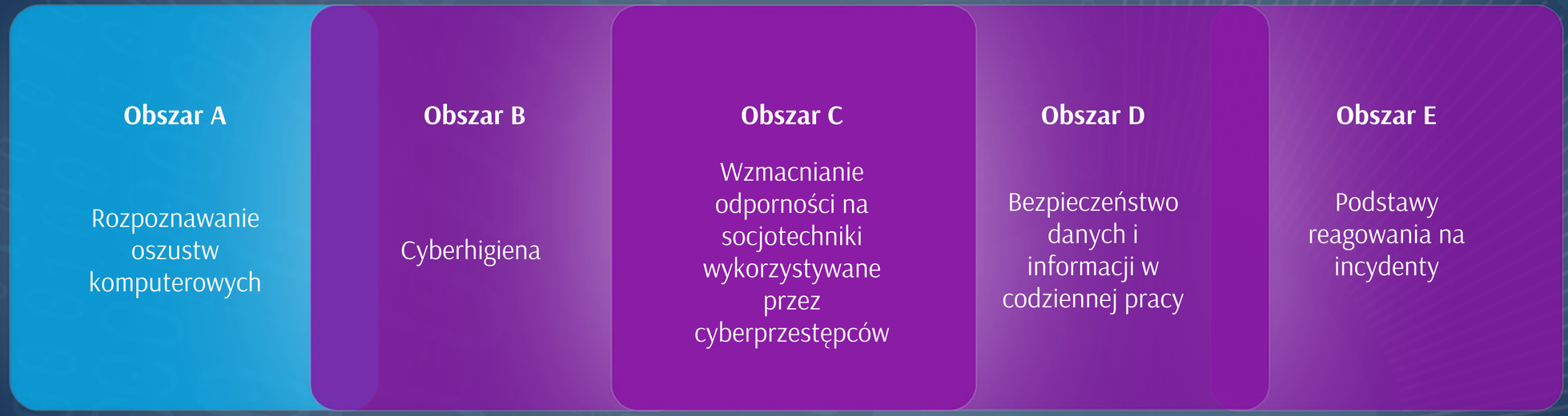
Obszar D

Bezpieczeństwo danych i informacji w codziennej pracy

Obszar E

Podstawy reagowania na incydenty

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



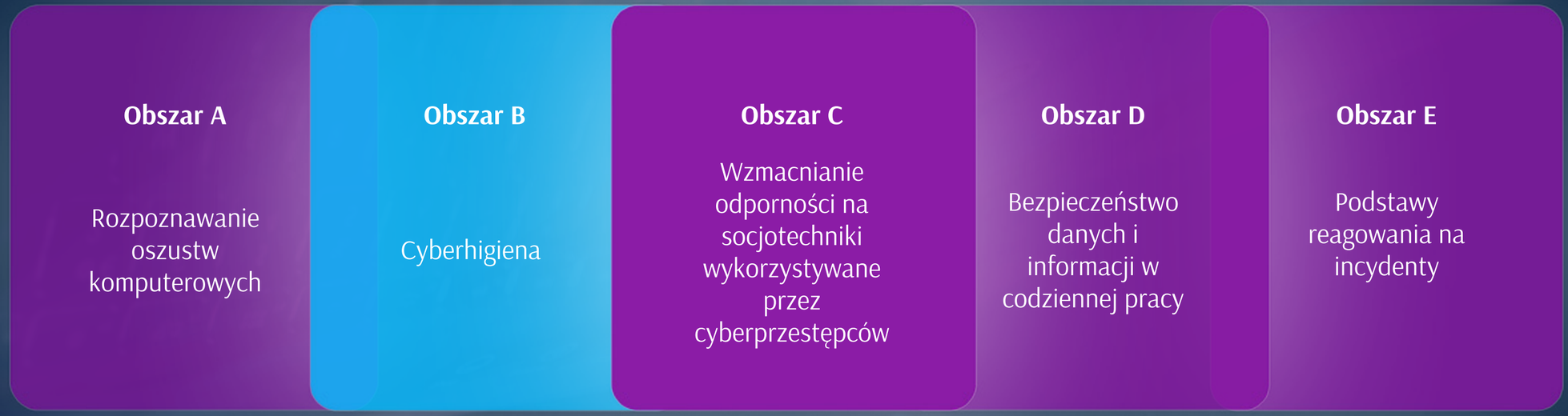
BLOK 1 - Identyfikowanie i analizowanie oszustw komputerowych w MŚP (8 godzin)

1.1. Charakteryzuje najczęściej występujące rodzaje oszustw komputerowych (2 godziny)

1.2. Rozpoznaje elementy ostrzegawcze w komunikacji elektronicznej (2 godziny)

1.3. Analizuje realne scenariusze oszustw komputerowych (4 godziny)

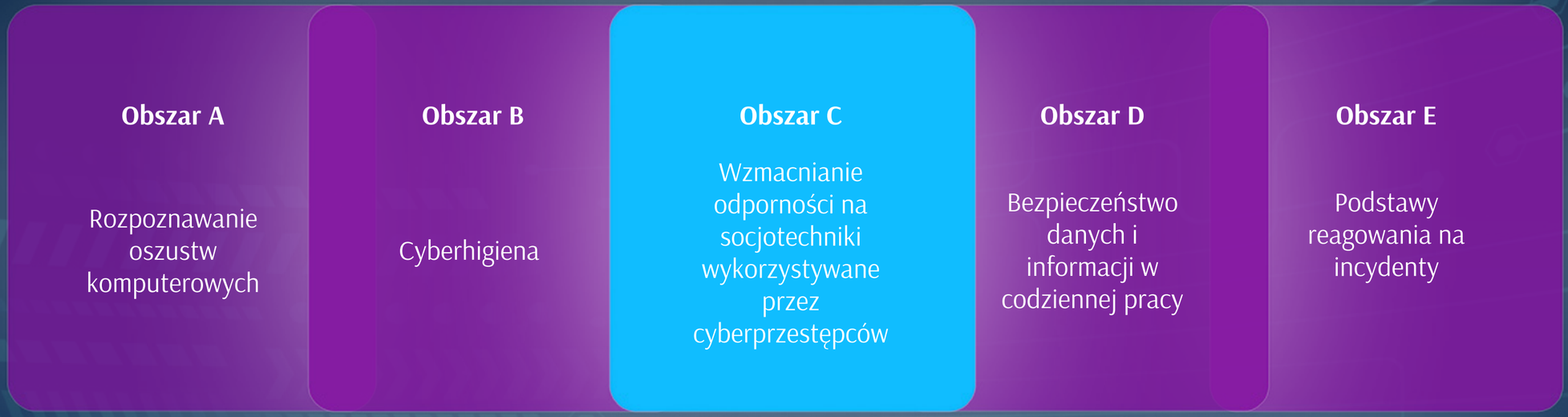
Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



BLOK 2 -Stosowanie zasad cyberhigieny w codziennej pracy z narzędziami cyfrowymi i urządzeniami końcowymi w MŚP (16 godzin)

2.1. Rozumie zasad cyberhigieny (4 godziny)
2.2. Stosuje zasady bezpiecznego zarządzanie hasłami i dostępem (3 godziny)
2.3. Stosuje zasady bezpieczeństwa urządzeń i oprogramowania (3 godziny)
2.4. Stosuje zasady bezpiecznego korzystania z sieci (3 godziny)
2.5. Stosuje podstawowe zasad tworzenia kopii zapasowych (3 godziny)

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



BLOK 3 - Rozpoznawanie i neutralizowanie technik manipulacji psychologicznej stosowanych w cyberatakach. (8 godzin)

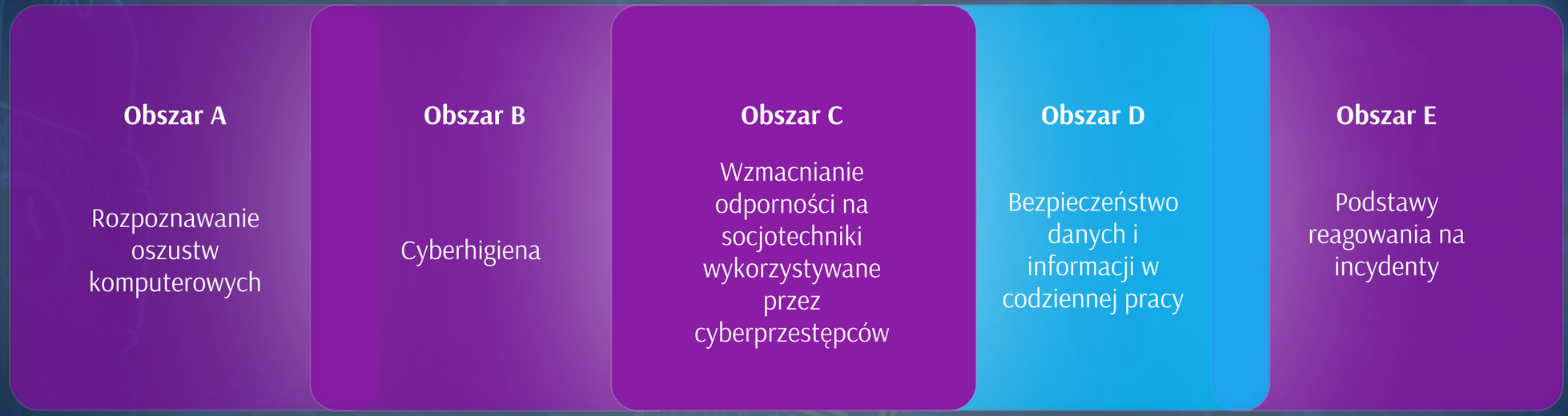
3.1. Charakteryzuje mechanizmy socjotechniczne wykorzystywane w cyberatakach (2 godziny)

3.2. Rozpoznaje fazy ataku socjotechnicznego (2 godziny)

3.3. Buduje nawyki decyzyjne zwiększające odporność na socjotechniki (2 godziny)

3.4. Rozpoznaje technik manipulacji psychologicznej stosowane w atakach socjotechnicznych (2 godziny)

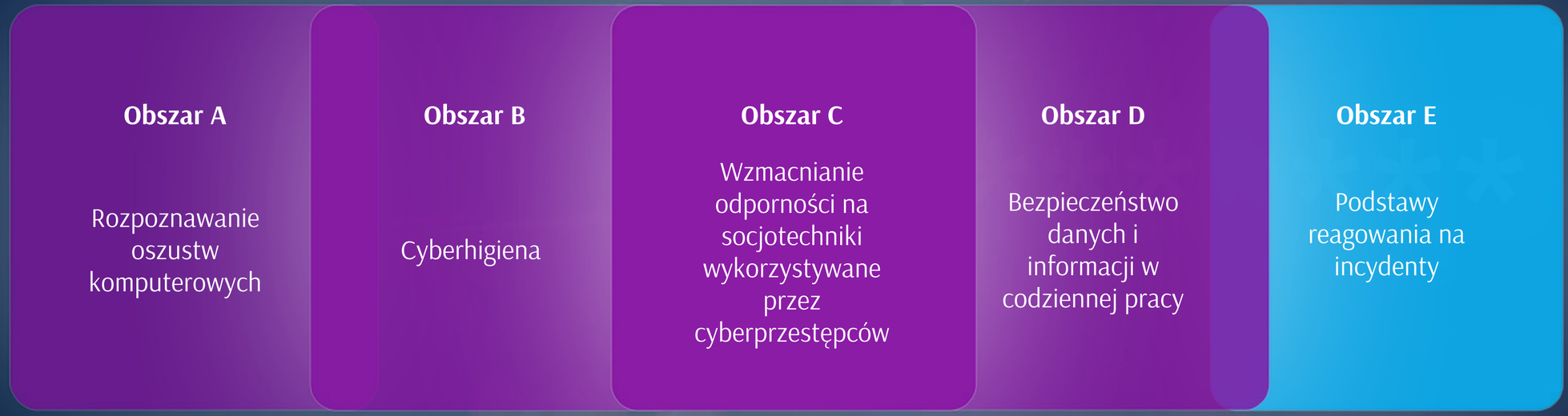
Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



BLOK 4 - Stosowanie zasad bezpiecznego przetwarzania, przechowywania i udostępniania danych w codziennej pracy (16 godzin)

4.1. Charakteryzuje rodzaje danych i informacji w przedsiębiorstwie (4 godziny)
4.2. Stosuje zasad bezpiecznego przetwarzania i przechowywania danych (4 godziny)
4.3. Zapobiega wyciekom danych (4 godziny)
4.4. Postępuję zgodnie z zasadą odpowiedzialności i zgodności z przepisami o ochronie danych (4 godziny)

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR



BLOK 5 - Rozpoznawanie incydentów cyberbezpieczeństwa oraz podejmowanie podstawowych działań ograniczających ich skutki (8 godzin)

5.1. Identyfikuje zdarzenia mogące stanowić incydent cyberbezpieczeństwa (2 godziny)

5.2. Podejmuje podstawowe działania ograniczające skutki incydentu cyberbezpieczeństwa (2 godziny)

5.3. Stosuje działania ograniczające ryzyko ponownych incydentów (4 godziny)

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

Sposób oraz metody realizacji usługi

W trakcie realizacji usługi powinny być wykorzystywane metody pozwalające na rozwój umiejętności, w szczególności case study, ćwiczenia do samodzielnego lub grupowego wykonania przez uczestników usługi. Usługa musi zostać zakończona weryfikacją nabytych przez uczestników usługi efektów uczenia się, przeprowadzoną zgodnie ze standardami określonymi w rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686).

Rekomenduje się, żeby walidacja efektów uczenia została przeprowadzona z wykorzystaniem:

- testu wiedzy w formie ustnej lub pisemnej (elektronicznej),
- zadań praktycznych w warunkach symulowanych,
- zadań decyzyjnych,
- wywiadu walidacyjnego,
- obserwacji w warunkach symulowanych lub odgrywania ról, umożliwiającej ocenę zachowań uczestnika w zakresie komunikacji z innymi pracownikami.