OCHRONA SYSTEMÓW OPERACYJNYCH

Bezpieczeństwo, definicje, pojęcia

Autor: Dr inż. Zbigniew Sołtys

CYBERBEZPIECZEŃSTWO 2.0

Cyberbezpieczeństwo dla gospodarki przyszłości
nr umowy POWER.03.05.00-00-Z308/18-00

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Plan wykładu

1. Wprowadzenie
2. Definicje i pojęcia związane z bezpieczeństwem
3. Ataki na bezpieczeństwo
4. Zasady bezpieczeństwa
5. Zagadnienia bezpieczeństwa systemów operacyjnych

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Tematy wykładów

Lp	Temat wykładu
1	Wprowadzenie. Pojęcia związane z bezpieczeństwem systemów komputerowych.
2	Architektura systemów operacyjnych: jądro, systemy plików, procesy, pamięć, użytkownicy
3	Uwierzytelnianie: hasło, żeton, dane biometryczne. Zdalne uwierzytelnianie. Bezpieczeństwo uwierzytelniania - Kerberos, SASL, PAM, usługi katalogowe
4	Narzędzia ochrony sieciowej (zapory sieciowe bezstanowe, stanowe, aplikacyjne
5	Użytkownicy w systemie operacyjnym. Modele uprawnień: ACL - Access Control List, RBAC Role Base Access Control
6	Modele dostępu do zasobów: Mandatory Access Control (MAC), Discretionary Access Control (DAC)
7	Zagrożenia i ataki na system operacyjny

Fundusze Europejskie
Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska
Europejski Fundusz Społeczny

Tematy wykładów cd.

Lp	Temat wykładu
8	Planowanie i wzmacnianie bezpieczeństwa (utwardzanie) systemu operacyjnego
9	Bezpieczeństwo systemu Linux/Unix.
10	Bezpieczeństwo systemu Windows
11	Bezpieczeństwo aplikacji z uwzględnieniem bezpiecznego programowania
12	Bezpieczeństwo wirtualizacji
13	Strategie i tendencje w bezpieczeństwie systemów
14	Strategie i tendencje w bezpieczeństwie systemów cd. Kolokwium zaliczeniowe – termin 1
15	Kolokwium zaliczeniowe – termin 2

Literatura do wykładów

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

1. Bezpieczeństwo systemów informatycznych, zasady i praktyka, William Stallings, Lawrie Brown, wydanie IV, Helion, tom I i tom II.
2. Operating Systems: Internals and Design Principles, Eighth Edition By William Stallings
3. Bezpieczeństwo w Unixie i Internecie, Simson Garfinkel, Gene Spafford, O`Reilly & Associates, Inc. Wydawnictwo RM
4. Kali Linux, Ric Messier, Helion
5. Pamięć Nieulotna, Edward Snowden , Insignis Media
6. Zasoby internetowe

Ochrona a bezpieczeństwo 1/2

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Główna różnica między ochroną a bezpieczeństwem polega na tym, że:

Bezpieczeństwo koncentruje się na zagrożeniach zewnętrznych systemu komputerowego poprzez przyznawanie dostępu do systemu uwierzytelnionym użytkownikom.

Ochrona koncentruje się na zagrożeniach wewnętrznych w systemie komputerowym poprzez organizowanie dostępu do zasobów systemowych w oparciu o mechanizm autoryzacji.

Ochrona a bezpieczeństwo 2/2

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Bezpieczeństwo:

Systemy bezpieczeństwa obejmują bezpieczeństwo zasobów systemowych pod kątem złośliwych zmian, nielegalnego dostępu itp. Zabezpieczenie wykorzystuje mechanizm uwierzytelniania i szyfrowania w celu umożliwienia użytkownikowi korzystania z systemu.

Ochrona:

Zapewnia prawidłowy dostęp do zasobów systemowych tylko przez procesy uprawnionych użytkowników np. określa, które pliki mogą być dostępne lub modyfikowane przez użytkownika.

System operacyjny może działać na segmentach pamięci, procesorze i innych zasobach na innym poziomie ochrony.

Definicja bezpieczeństwa

Mówiąc bezpieczeństwo komputerowe (ang. computer security), mamy w istocie na myśli wszelkiego rodzaju aktywa (dobra, ang. assets) związane z komputerami, które są podatne na różnego rodzaju zagrożenia i których ochrona wymaga podejmowania różnego rodzaju działań.

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Wg Bezpieczeństwo Systemów Informatycznych — tłum. Helion

Zapewnianie bezpieczeństwa

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Zapewnienie bezpieczeństwa to środki i regulacje zapewniające poufność, nienaruszalność i dostępność **aktywów systemu informacyjnego**, w tym sprzętu, oprogramowania, programów fabrycznie wbudowanych oraz przetwarzanych, oraz przechowywanych danych i transmitowanych informacji.

Internal/Interagency **Report NISTIR 7298** (Glossary **of** Key Information Security Terms) — tłum. Helion

Cele bezpieczeństwa

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Bezpieczeństwo aktywów rozumiane jest więc jako:

- Poufność - danych, informacji
- Integralność – danych, programów ale także systemu informatycznego
- Dostępność – danych i systemów

Te trzy pojęcia określane są często jako triada CIA

– nazwa pochodzi od pierwszych liter słów confidentiality, integrity i availability

Informacja bezpieczna

Informacja bezpieczna to taka, która poprzez swoją zawartość udowadnia, że jest:

- Poufna (zaszyfrowana),
- Integralna (autentyczna - nie została zmieniona),
- Dostępna - była i jest dostępna tylko osobom do tego upoważnionym.

- Niekiedy także niezaprzeczalna (posiada cechy jednoznacznej identyfikacji z nadawcą - niezaprzeczalności nadania,)

Jeżeli informacja nie posiada którejś z wymienionych wyżej cech, to może się okazać że została ujawniona.

Bezpieczeństwo danych 1/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Poufność

Ochrona danych przed odczytem i kopiowaniem przez osobę nieupoważnioną.

Ten typ bezpieczeństwa obejmuje nie tylko ochronę danych w całości, ale również poszczególnych jej fragmentów.
Ochrona poufności polega również na zapewnieniu kontroli nad gromadzeniem, przechowywaniem i ujawnianiem informacji.

Bezpieczeństwo danych 2/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

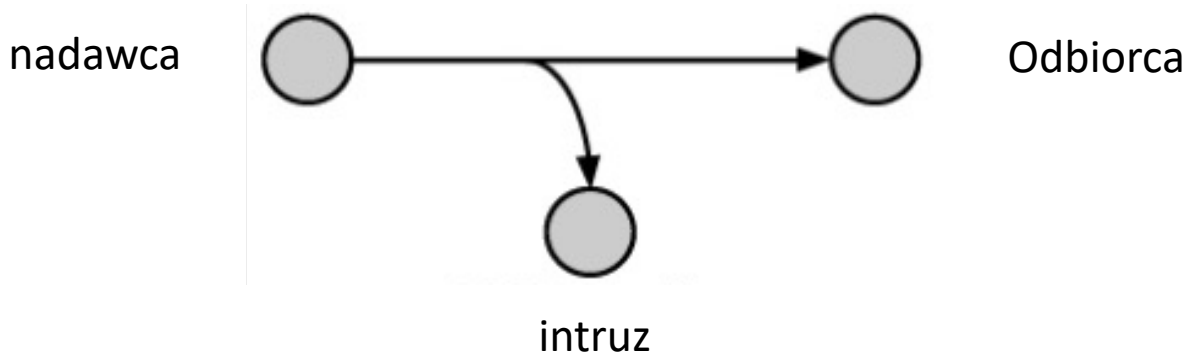
Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Atak na poufność:

- Przechwytywanie danych w sieci
- Kopiowanie plików lub programów



Bezpieczeństwo danych 3/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Integralność - Spójność danych:

- Ochrona informacji (w tym programów) przed usunięciem lub jakimikolwiek zmianami bez pozwolenia właściciela.
- Chronione informacje obejmują również system informatyczny - zapisy systemu rozliczania (logi systemowe), kopie zapasowe, atrybuty plików (dostęp do plików).

Bezpieczeństwo danych 4/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

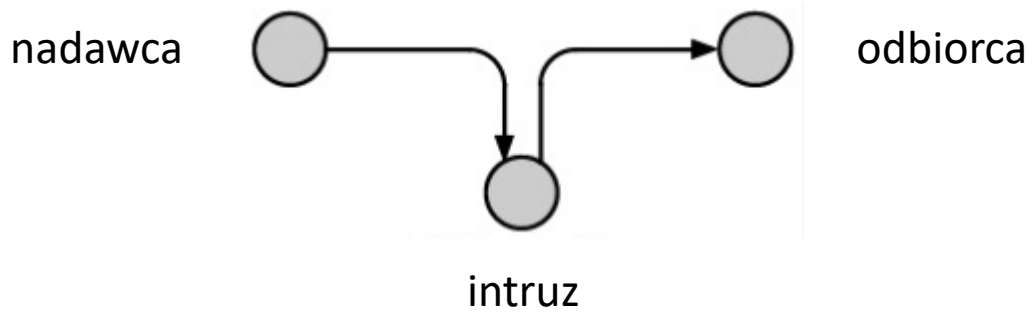
Unia Europejska
Europejski Fundusz Społeczny

Integralność

Strona nieautoryzowana uzyskuje dostęp do aktywów ale również je narusza

Atak na spójność to:

Zmiana wartości w plikach danych
Modyfikacja programu
Modyfikacja wiadomości transmitowanych siecią



Bezpieczeństwo danych 5/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Dostępność

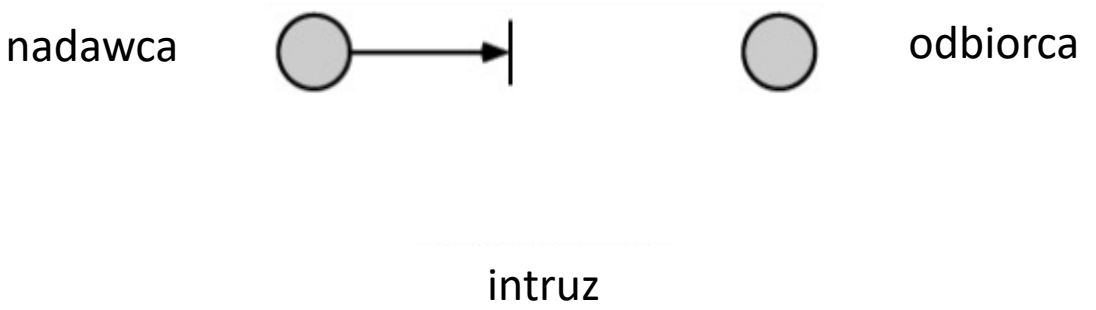
- Ochrona **świadczonych** usług przed zniekształceniem i uszkodzeniem.
- Zapewnienie natychmiastowego dostępu do usług przez upoważnionych użytkowników.

Jeśli użytkownik potrzebuje skorzystać z systemu, który jest niedostępny, skutek jest taki sam, jak gdyby z systemu usunięto dane.

Bezpieczeństwo danych 6/7

Atak na dostępność:

- Przerwanie przepływu
- Aktywa ulegają zniszczeniu – stają się niedostępne – zniszczenie dysku, zablokowanie sieci itp.



Bezpieczeństwo danych 7/7

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Ponadto

Niezaprzeczalność

- Brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych.
- Zapewnienie niezaprzeczalności transakcji jest jedną z cech podpisu kwalifikowanego.
- Podpis umieszczony jest na karcie kryptograficznej zawierającej poświadczony certyfikat, który wiąże dane osoby z kluczem publicznym. Karta zawiera również klucz prywatny.

Ataki na aktywa

Aktywa komputerowe i sieciowe z przykładami ataków

	Dostępność	Poufność	Nienaruszalność
Sprzęt	Wyposażenie zostało skradzione lub unieruchomione, uniemożliwiając świadczenie usług	Zdeszyfrowany napęd (jednostka pamięci) USB	
Oprogramowanie	Usunięto programy, co uniemożliwia dostęp do nich użytkownikom	Wykonano kopię oprogramowania bez upoważnienia	Działający program jest modyfikowany, aby spowodować awarię podczas wykonywania lub wykonać niepożądane zadanie

Wg. Bezpieczeństwo systemów operacyjnych - Helion

Ataki na aktywa cd.

Aktywa komputerowe i sieciowe z przykładami ataków

	Dostępność	Poufność	Nienaruszalność
Dane	Następuje usunięcie plików, co uniemożliwia dostęp do nich użytkownikom	Wykonano nielegalne czytanie danych. Analiza statystyczna danych ujawnia głębsze dane	Istniejące pliki zostały zmodyfikowane lub sfabrykowano nowe pliki
Linie i sieci komunikacyjne	Linie komunikacyjne lub sieci stają się niedostępne	Następuje czytanie komunikatów. Obserwowana jest charakterystyka ruchu komunikatów	Komunikaty są modyfikowane, usuwane, zmieniona zostaje ich kolejność. Dochodzi do fabrykowania fałszywych komunikatów

Wg. Bezpieczeństwo systemów operacyjnych - Helion

Ogólne zasady bezpieczeństwa 1/4

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

- Nie ma bezwzględnej miary bezpieczeństwa i nie ma całkowicie bezpiecznych systemów informatycznych.
- Mówimy o stopniu zaufania do systemu w odniesieniu do określonych w tym zakresie wymagań stawianych systemowi.
- Skuteczność zabezpieczeń zależy od ludzi. System bezpieczeństwa nie uchroni systemu informatycznego jeśli zawiedzie człowiek.

Ogólne zasady bezpieczeństwa 2/4

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

- Nie istnieje żaden algorytm który dla dowolnego systemu ochrony może określić czy ta ochrona jest skuteczna
- System bezpieczeństwa musi stosować łącznie różne metody ochrony w przeciwnym razie będzie posiadać luki.
- Poziom bezpieczeństwa jest taki jakie jest najsłabsze ogniwo (często człowiek)

Ogólne zasady bezpieczeństwa 3/4

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

- System informatyczny zabezpieczony dzisiaj nie jest bezpieczny jutro !
- Codziennie powstają nowe szkodliwe programy i wirusy
- Postęp technologiczny stwarza nowe możliwości (np. szybsze komputery to szybsze łamanie haseł)
- Bezpieczeństwo jest procesem i musi podlegać częstej weryfikacji.

Ogólne zasady bezpieczeństwa 4/4

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Podstawą do poprawienia bezpieczeństwa w systemach informatycznych jest odpowiedź na trzy podstawowe pytania:

- Co chronić?
- Przed czym chronić? – analiza ryzyka
- Jak chronić?

Ponadto: ocena ryzyka odpowiada na pytanie

Ile czasu, wysiłku i pieniędzy można poświęcić, aby zapewnić sobie odpowiednią ochronę?

Koszty bezpieczeństwa

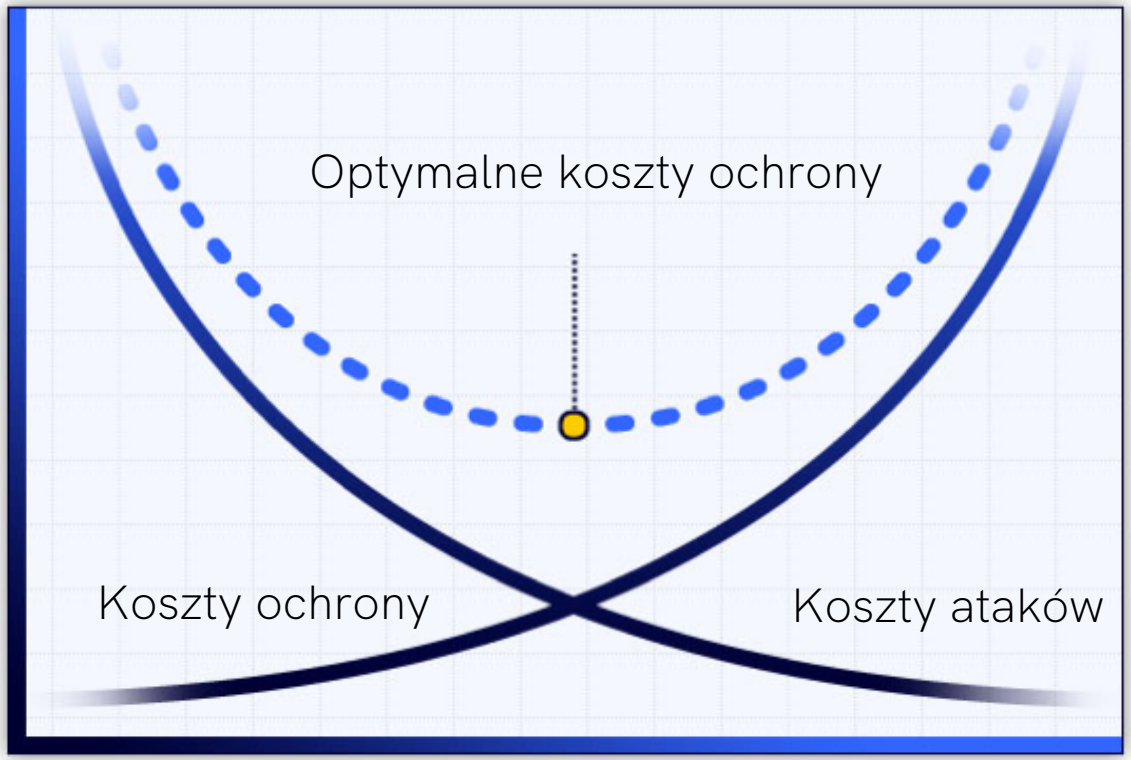
Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

koszt



bezpieczeństwo

Racjonalizacja kosztów. Na podstawie analizy ryzyka

Co chronić - Aktywa

Do elementów wymagających ochrony należy zaliczyć:

środki materialne, np.:

- komputery,
- dane o charakterze strategicznym,
- kopie zapasowe i archiwa,
- wydruki,
- nośniki z komercyjnym oprogramowaniem,
- urządzenia i okablowanie komunikacyjne,
- dane osobowe,
- dane audytu.

Co chronić - Aktywa cd.

Środki niematerialne, np.:

- bezpieczeństwo i zdrowie pracowników,
- prywatność użytkowników,
- hasła pracowników,
- wizerunek publiczny i reputacja,
- dobre imię klientów,
- zdolności produkcyjne lub do prowadzenia usług,
- dane konfiguracyjne sprzętu

Jak chronić - Analiza ryzyka

Analiza ryzyka obejmuje – prawdopodobieństwo wystąpienia zdarzenia i koszty szkody poniesionej w wyniku wystąpienia zdarzenia.

- trzęsienie ziemi ?
- powódź ?
- pożar ?
- awaria zasilania ?
- wirusy ?
- hakerzy ?
- niewyszkoleni pracownicy ?
- niezadowoleni administratorzy ?

Jak chronić

Stosować Politykę Bezpieczeństwa Informacji w organizacji.

Polityka to zbiór dokumentów opisujących zasady i sposoby ochrony informacji przetwarzanych w organizacji.
Norma PN-ISO/IEC 27002 zaleca aby organizacje określiły „politykę bezpieczeństwa informacji" zatwierdzoną przez kierownictwo, w której określono podejście organizacji do zarządzania jej celami bezpieczeństwa informacji.

Przykłady:
https://www.zarz.umed.wroc.pl/images/rektor/2017/109_0.pdf
https://www.wns.uni.wroc.pl/attachments/142_2017_Regulamin-bezp_info_2020-02-26_14-52-30.pdf

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Od czego zależy bezpieczeństwo

W normie ISO/IEC27001 wyróżniono jedenaście obszarów, mających wpływ na bezpieczeństwo informacji w organizacji:

1. Polityka bezpieczeństwa;
2. Organizacja bezpieczeństwa informacji;
3. Zarządzanie aktywami;
4. Bezpieczeństwo zasobów ludzkich;
5. Bezpieczeństwo fizyczne i środowiskowe;
6. Zarządzanie systemami i sieciami;
7. Kontrola dostępu;
8. Zarządzanie ciągłością działania;
9. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych;
10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
11. Zgodność z wymaganiami prawnymi i własnymi standardami

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Ogólnie - Techniki zabezpieczeń

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

- Organizacyjne – Polityka Bezpieczeństwa Informacji
- Administracyjne – wymagania w stosunku do pracowników
- Fizyczne – strefy chronione – serwerownie, urządzenia sieciowe
- Programowe – Firewall, programy detekcji intruzów

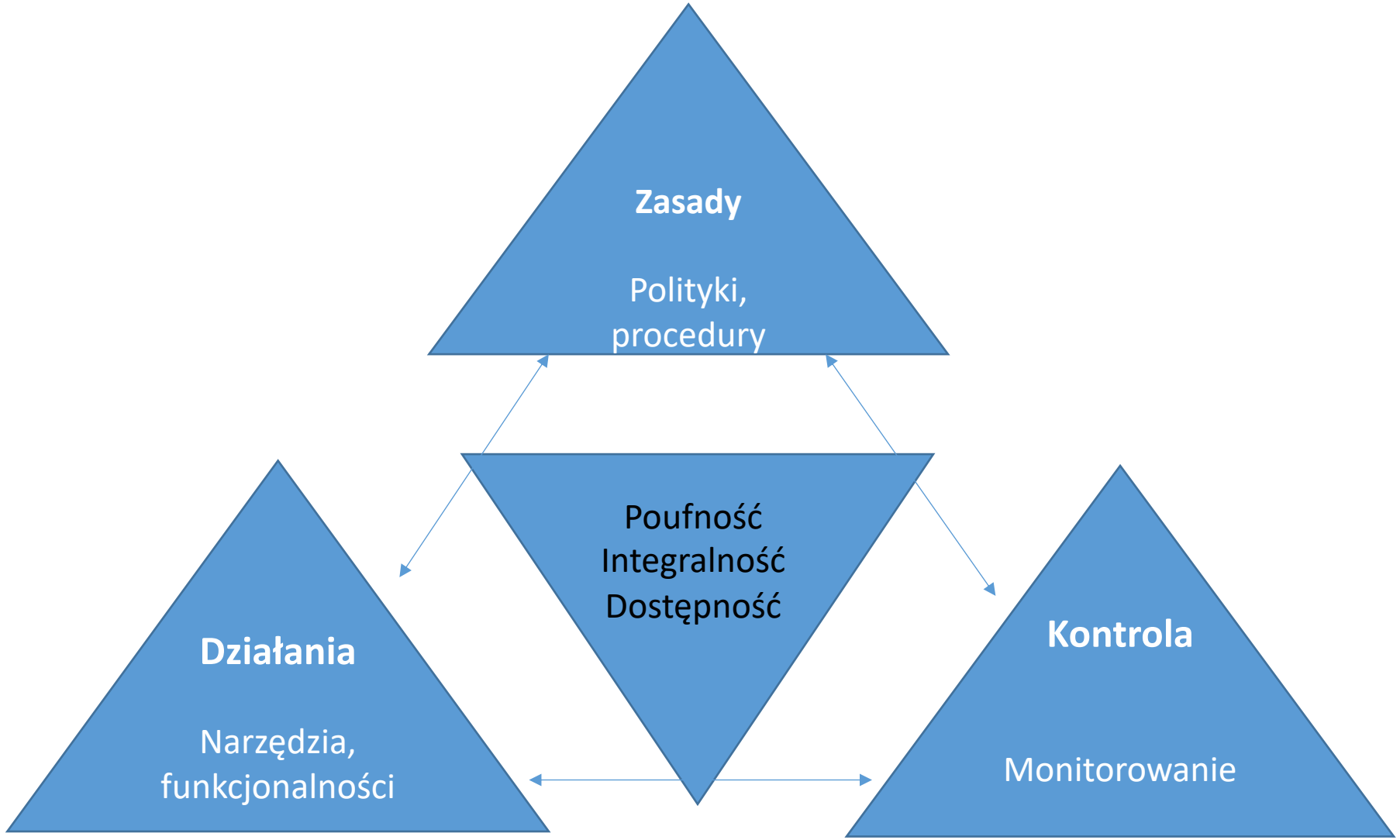
Składowe bezpieczeństwa informacji

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny



Dokumenty ISO związane z bezpieczeństwem

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Normy ISO

12207 Information technology — Software lifecycle processes, 1997

13335 Management of information and communications technology security, 2004

27000 ISMS — Overview and Vocabulary, luty 2016

27001 ISMS — Requirements, październik 2013

27002 Code of Practice for Information Security Controls, październik 2013

27003 Information security management system implementation guidance, 2010

27004 Information security management — Measurement, 2009

27005 Information Security Risk Management, czerwiec 2011

27006 Requirements for bodies providing audit and certification of information security management systems, 2015

31000 Risk management — Principles and guidelines, 2009

Źródła ataków

Zródło ataków	Częstość w %
Grupy cyberprzestępców	59 %
Pracownicy	55%
Haktywiści	53%
Hekerzy indywidualni	44%
Podwykonawcy w firmie	36 %
Organizacje rządowe	35 %
Dostawcy	14 %
Partnerzy biznesowi	12 %
Klienci	11 %
Inni	5 %

Systemy operacyjne – środowisko przetwarzania danych

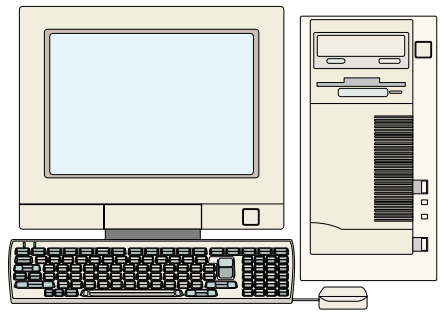
Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

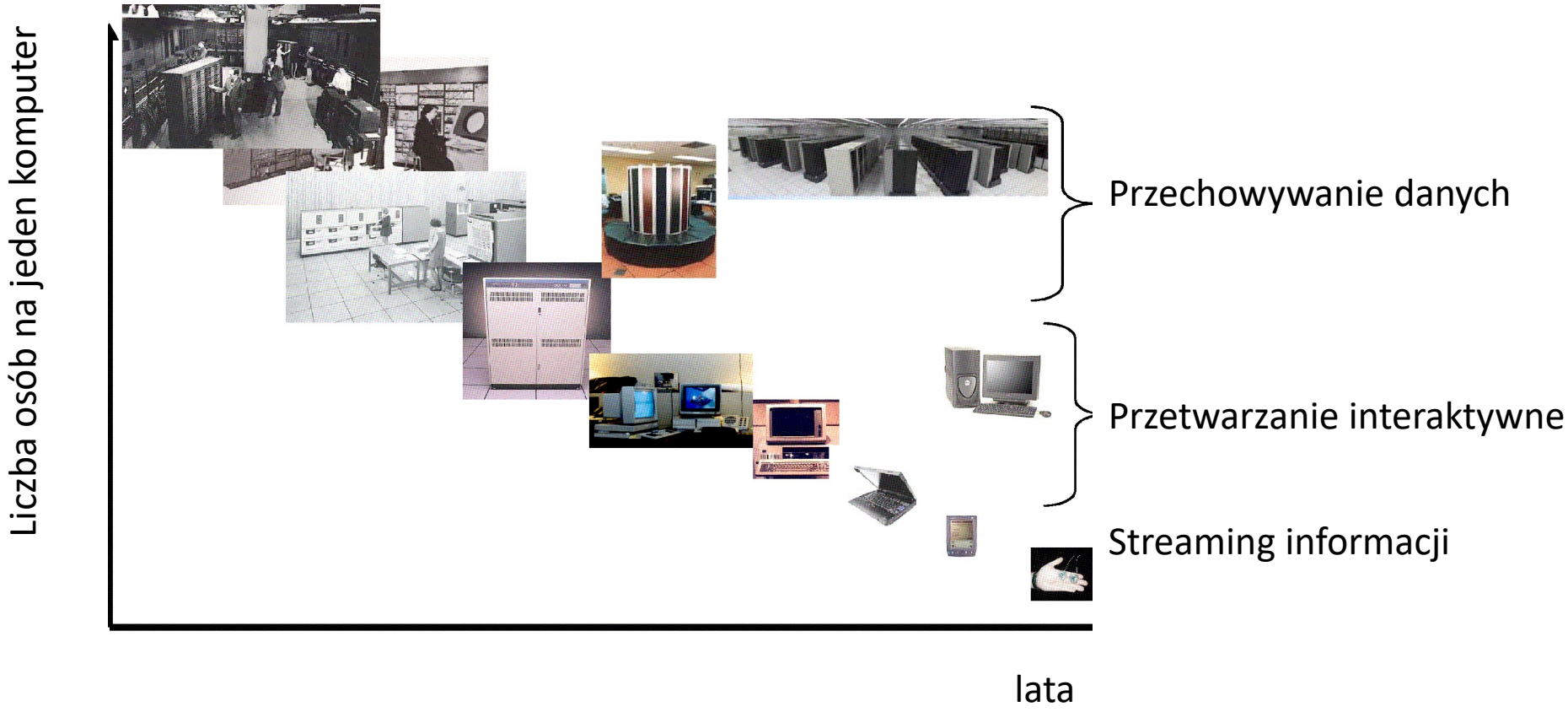
Wykorzystanie systemów operacyjnych miejsca przetwarzania danych



Wg Wiliam Stallings

Systemy operacyjne

Zmiana dostępności systemów operacyjnych w czasie – obecnie kilka systemów na osobę



Wg Wiliam Stallings

Fundusze Europejskie
Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska
Europejski Fundusz Społeczny

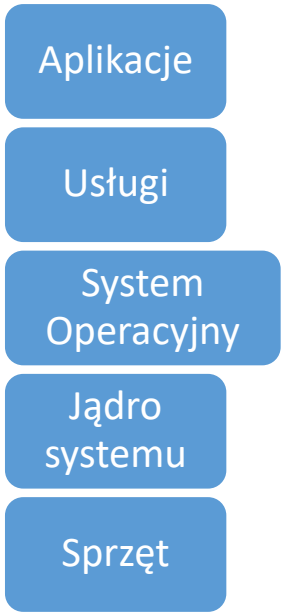
Systemy operacyjne - złożoność

System operacyjny	Liczba linii kodu w milionach
Windows NT 4.0 (1996)	11.50
Android	12.00
Boeing 787, total flight software	14.00
Windows Vista (2007)	50.00
Facebook (without backend code)	62.00
Debian 5.0 codebase	68.00
Mac OS X 10.4	86.00
Software in typical new car, 2013	100.00
Google	2,000.00

https://docs.google.com/spreadsheets/d/1s9u0uprmuJvwR2fkRqxJ4W5Wfomimmk9pwGTK4Dn_UI/edit#gid=5

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Warstwy systemu komputerowego



Na którym poziomie zabezpieczać ?

Zabezpieczenie warstwy wyższej zazwyczaj może być zaatakowane z warstw niższych

Zabezpieczanie systemów operacyjnych

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

Podstawa zabezpieczania to separacja.
Separacja może być realizowana na czterech poziomach:

- Fizycznym

Obiekty fizyczne jak CPU, drukarki, itp.

- Czasowym

Wykonywanie procesów w różnym czasie

- Logicznym

Tworzenie domen – użytkownik ma wrażenie że jest sam w systemie

- Kryptograficznym

Zakodowanie danych, inni nie mogą ich odczytać

Chronione obiekty systemów

Szczególnie chronione powinny być te zasoby , które można udostępniać, np.

- Pamięć
- Urządzenia I/O (dyski, drukarki, napędy itp.)
- Programy, procedury
- Dane

Inne mechanizmy systemu operacyjnego jak:

- zarządzanie plikami - logiczne,
- zarządzanie pamięcią - fizyczne
- sterowanie szyną systemową
- kontrola przerwań
- rejestry statusu

Systemy zaufane

Istnieje kilka podstawowych elementów, które są fundamentalne dla zaufanych systemów operacyjnych:

- **jądro**

to część systemu operacyjnego realizująca funkcjonalności na najniższym poziomie

- **jądro bezpieczeństwa**

jest odpowiedzialne za egzekwowanie mechanizmów bezpieczeństwa całego systemu operacyjnego

- **monitor referencyjny (RM)**

jest częścią jądra bezpieczeństwa, która kontroluje dostęp do obiektów

- **zaufana baza obliczeniowa (TCB)**

to wszystkie informacje w zaufanym systemie operacyjnym niezbędne do wymuszenia polityki bezpieczeństwa

Polityka bezpieczeństwa systemu operacyjnego

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Politechnika Wrocławska

Unia Europejska
Europejski Fundusz Społeczny

- Polityka bezpieczeństwa to deklaracja bezpieczeństwa, jakiego oczekujemy od systemu do egzekwowania.

Politykę można wyrazić jako szereg dobrze zdefiniowanych, spójnych i wykonalnych zasad.

- Model bezpieczeństwa jest reprezentacją polityki bezpieczeństwa dla systemu operacyjnego.

- Formalny model bezpieczeństwa to opis matematyczny zasad polityki bezpieczeństwa.

Model ten może być używany do przeprowadzenia formalnych dowodów bezpieczeństwa.

Budowa bezpiecznego systemu operacyjnego

Stworzenie bezpiecznego systemu operacyjnego może być wykonane w sześciu krokach:

- analiza systemu
- wybrać / zdefiniować politykę bezpieczeństwa
- wybrać / utworzyć model bezpieczeństwa (na podstawie polityki)
- wybrać metodę realizacji
- wykonać projekt (koncepcyjny)
- zweryfikować poprawność projektu
- dokonać implementacji
- zweryfikować realizację

Pomiędzy wszystkimi powyższymi krokami istnieją pętle sprzężenia zwrotnego

We wszystkich powyższych krokach mogą wystąpić błędy

Klasy bezpieczeństwa systemów operacyjnych

Trusted Computer System Evaluation Criteria (TCSEC, Orange Book)

TCSEC koncentruje się głównie na zapewnieniu poufności informacji.

Wyróżnia się w nim 4 poziomy kryteriów oznaczone D, C, B, A.

D - ochrona minimalna (ang. Minimal Protection)

C1 - ochrona uznaniowa (ang. Discretionary Protection)

C2 - ochrona z kontrolą dostępu (ang. Controlled Access Protection)

B1 - ochrona z etykietowaniem (ang. Labeled Security Protection)

B2 - ochrona strukturalna (ang. Structured Protection)

B3 - ochrona przez podział (ang. Security Domains)

A1 - konstrukcja zweryfikowana (ang. Verified Design)

Klasy bezpieczeństwa systemów operacyjnych cd.

Common Criteria Assurance Levels (EAL)

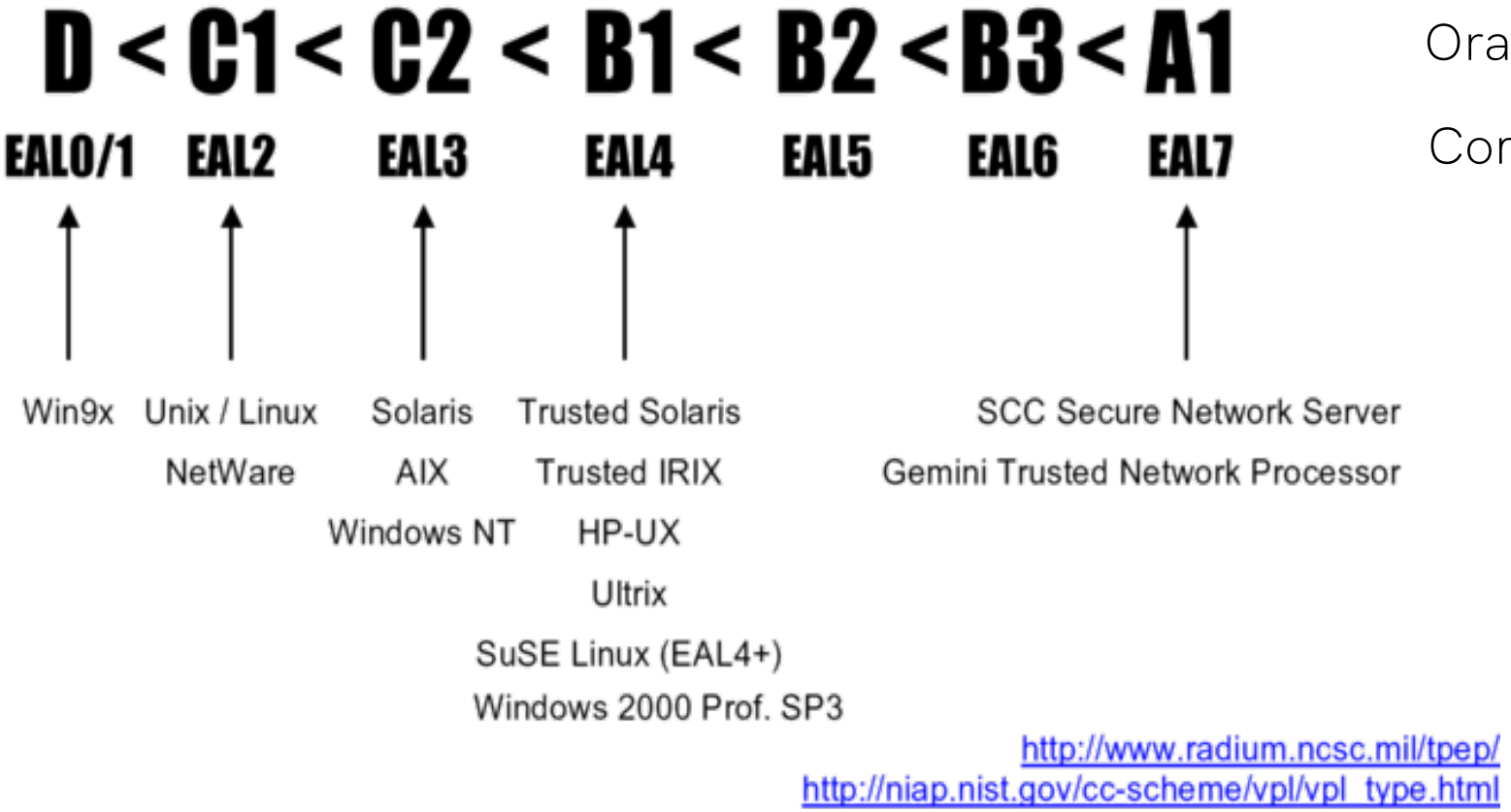
aktualnie obowiązujący standard będący w istocie złączeniem ITSEC, TCSEC oraz CTCPEC (Kanada).

Od 1996 powszechnie znany jako Common Criteria for Information Technology Security Evaluation (CC; http://www.commoncriteria.org).

Od 1999 roku zaakceptowany jako międzynarodowa norma ISO15408 (EAL v.2).

CC również definiuje poziomy kryteriów bezpieczeństwa (EAL 0 do EAL 7)

Porównanie klas bezpieczeństwa



Orange book

Common criteria

http://www.radium.ncsc.mil/tpep/
http://niap.nist.gov/cc-scheme/vpl/vpl_type.html

Podsumowanie

Najważniejsze pojęcia związane z bezpieczeństwem systemów informatycznych to Poufność, integralność, dostępność aktywów.

Ważne pytania to:

- Co chronić?

Aktywa -środki materialne i niematerialne

- Przed czym chronić?

Ataki na poufność, integralność dostępność - analiza ryzyka

- Jak chronić?

Realizacja ustalonych sposobów postępowania – polityki bezpieczeństwa w odniesieniu do aktywów i systemów operacyjnych

CYBERBEZPIECZEŃSTWO 2.0

Bezpieczeństwo systemów Operacyjnych

AUTOR Zbigniew Sołtys

E-MAIL zbigniew.soltys@pwr.edu.pl

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój, Priorytet III Szkolnictwo Wyższe dla gospodarki i rozwoju, Działanie 3.5 Kompleksowe programy szkół wyższych w ramach konkursu nr POWR.03.05.00-IP.08-00-PZ3/18 na Zintegrowane Programy uczelni – Ścieżka III, nr umowy POWR.03.05.00-00-Z308/18-00
Tytuł projektu: „Cyberbezpieczeństwo dla gospodarki przyszłości”