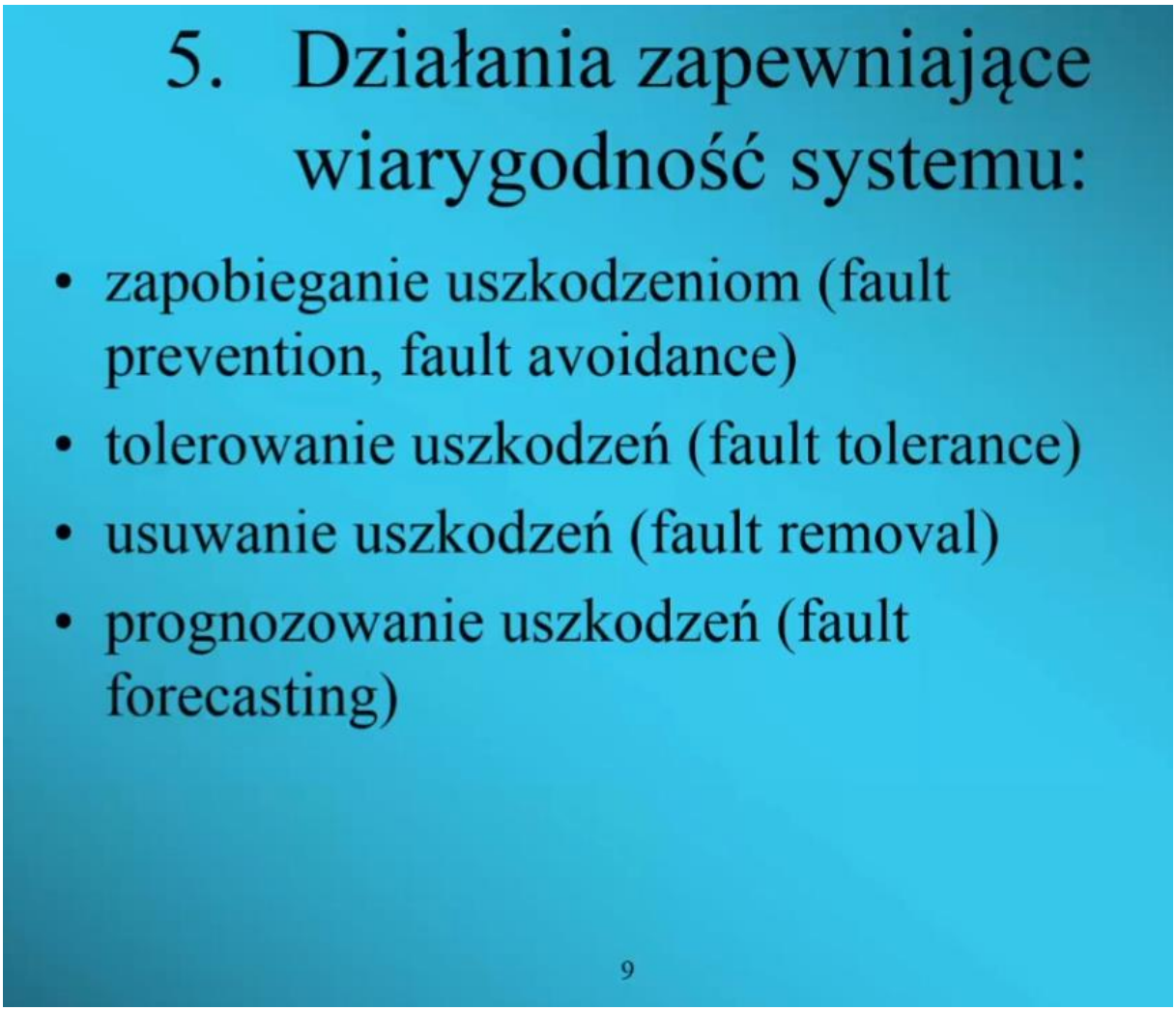
1 **Pytanie 1**

Które z poniższych działań zapewniają wiarygodność systemu:
Wybierz jedną lub więcej odpowiedzi

- ☐ usuwanie uszkodzeń (fault removal)
- ☐ zapobieganie uszkodzeniom (fault prevention, fault avoidance)
- ☐ tolerowanie uszkodzeń (fault tolerance)
- ☐ prognozowanie uszkodzeń (fault forecasting)
- ☐ wymuszanie awarii (fault forcing)

1,2,3,4



2 **Pytanie 2**

Napastnik atakujący system komputerowy **najczęściej**:
Wybierz odpowiedź:

- ○ obchodzi zabezpieczenia
- ○ pokonuje słabe zabezpieczenia
- ○ pokonuje średnie zabezpieczenia

1

3 **Pytanie 3**

Brak odnotowanych symptomów naruszenia bezpieczeństwa systemu oznacza, że:
Wybierz odpowiedź:

- ○ bezpieczeństwo systemu na pewno nie zostało naruszone
- ○ posiadamy na 100% sprawny system monitorowania bezpieczeństwa
- ○ bezpieczeństwo systemu mogło zostać naruszone ale możemy o tym nie wiedzieć

3 1?

4 **Pytanie 4**

Które z niżej wymienionych zasobów wymagają ochrony?
Wybierz odpowiedź:

- ○ każda informacja uznana za wrażliwą przez jej autora lub dysponenta
- ○ tylko strategiczne dla firmy informacje handlowe
- ○ tylko informacje z audytów bezpieczeństwa
- ○ tylko informację związane ze zdrowiem pracowników
- ○ tylko dane osobowe

1

5 **Pytanie 5**

Ustaw etapy analizy ryzyka we właściwej kolejności:

Dopasuj wartości:

	3	5	4	1	2	6
Określenie ryzyka akceptowalnego i szczątkowego,	○	○	○	○	○	○
Określenie wartości poszczególnych zasobów	○	○	○	○	○	○
Określenie podatności poszczególnych zasobów	○	○	○	○	○	○
Pełna identyfikacja oraz inwentaryzacja zasobów	○	○	○	○	○	○
Określenie skutków naruszenia bezpieczeństwa zasobu	○	○	○	○	○	○
Identyfikacja zagrożeń dla każdego zasobu	○	○	○	○	○	○

4,2,3,6,5,1

6 **Pytanie 6**

Podczas wdrażania bezpiecznych metod ochrony systemów:
Wybierz odpowiedź:

- ○ W pierwszej kolejności należy szkolić i uświadamiać kadrę a następnie wdrożyć zabezpieczenia
- ○ W pierwszej kolejności należy wdrożyć zabezpieczenia a następnie szkolić i uświadamiać kadrę
- ○ Wdrażanie zabezpieczeń i szkolenie i uświadamianie kadry powinno odbywać się równolegle

3

7 **Pytanie 7**

Podczas wdrażania bezpiecznych metod ochrony systemów:
Wybierz odpowiedź:

- ○ Proces uświadamiania pracowników musi objąć głównie szeregowych pracowników
- ○ Proces uświadamiania pracowników musi objąć całe przedsiębiorstwo
- ○ Proces uświadamiania pracowników musi objąć głównie prezesa/dyrektora

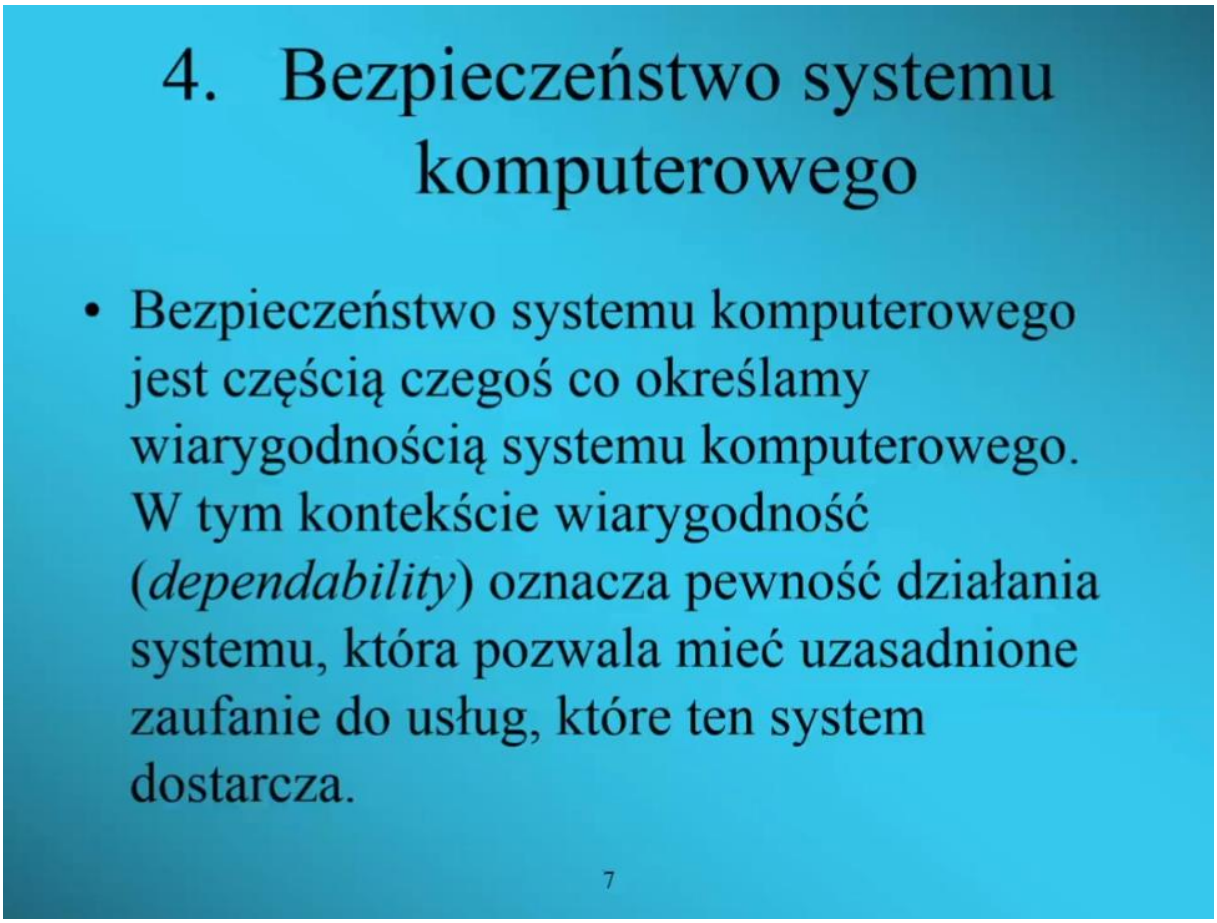
2

8 **Pytanie 8**

Podaj definicję bezpiecznego systemu komputerowego
Wprowadź odpowiedź

3. Czy istnieje bezpieczny system komputerowy?

- **Bezpieczny system komputerowy** to taki system komputerowy, którego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.
- Zgodnie z tą definicją, system możemy uznać za bezpieczny, jeśli można od niego oczekiwać, że wprowadzone na stałe dane nie zostaną utracone, nie ulegną zniekształceniu i nie zostaną pozyskane przez nikogo nieuprawnionego – tym samym ufamy, że system komputerowy będzie przechowywał i chronił te dane. (2)



Bezpieczny system komputerowy to taki system komputerowy, którego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją. Zgodnie z tą definicją, system możemy uznać za bezpieczny, jeśli można od niego oczekiwać, że wprowadzone na stałe dane nie zostaną utracone, nie ulegną zniekształceniu i nie zostaną pozyskane przez nikogo nieuprawnionego – tym samym ufamy, że system komputerowy będzie przechowywał i chronił te dane.

Bezpieczny system komputerowego jest częścią czegoś co określamy wiarygodnością systemu komputerowego.

9 **Pytanie 9c**

Co oznacza następujący atrybut wiarygodności systemu - **dostępność** (availability)?
Wprowadź odpowiedź

System wiarygodny =

- dyspozycyjny (*available*) = dostępny na bieżąco
- niezawodny (*reliable*) = odporny na awarie
- bezpieczny (*secure*) = zapewniający ochronę danych
- bezpieczny (*safe*) = bezpieczny dla otoczenia, przyjazny dla środowiska

• poufność (confidentiality) – informacja jest dostępna jedynie dla podmiotów do tego upoważnionych; • spójność/integralność (integrity) – wszelkie nieuprawnione modyfikacje informacji są niedozwolone; • dostępność (availability) – do informacji można uzyskać dostęp w każdych okolicznościach, które są dopuszczone przez politykę bezpieczeństwa informacji. • Do tej trójki z czasem dołączono także: możliwość rozliczania/rozliczalność (accountability), czyli ustalenia odpowiedzialnych za wykonane operacje.

Dostępność - Informacja jest dostępna i użyteczna na żądanie uprawnionego podmiotu .

Niezawodność - jest spójny i zachowanie jest zgonie z zamierzonym i skutki są takie jakie przewidywane.

Poufność - Informacje są zabezpieczane i udostępnione podmiotom według ich uprawnień.

Integralność - dane są korpulentne i tworzą całość.

Rozliczalność - Wiadomo jakie, gdzie i kiedy dany podmiot wykonał działania.

10 **Pytanie 9d**

Co oznacza następujący atrybut wiarygodności systemu - **autentyczność** (authenticity)?
Wprowadź odpowiedź

Autentyczność Tożsamość podmiotu lub zasobu taka jak jest deklarowana.

11 **Pytanie 10**

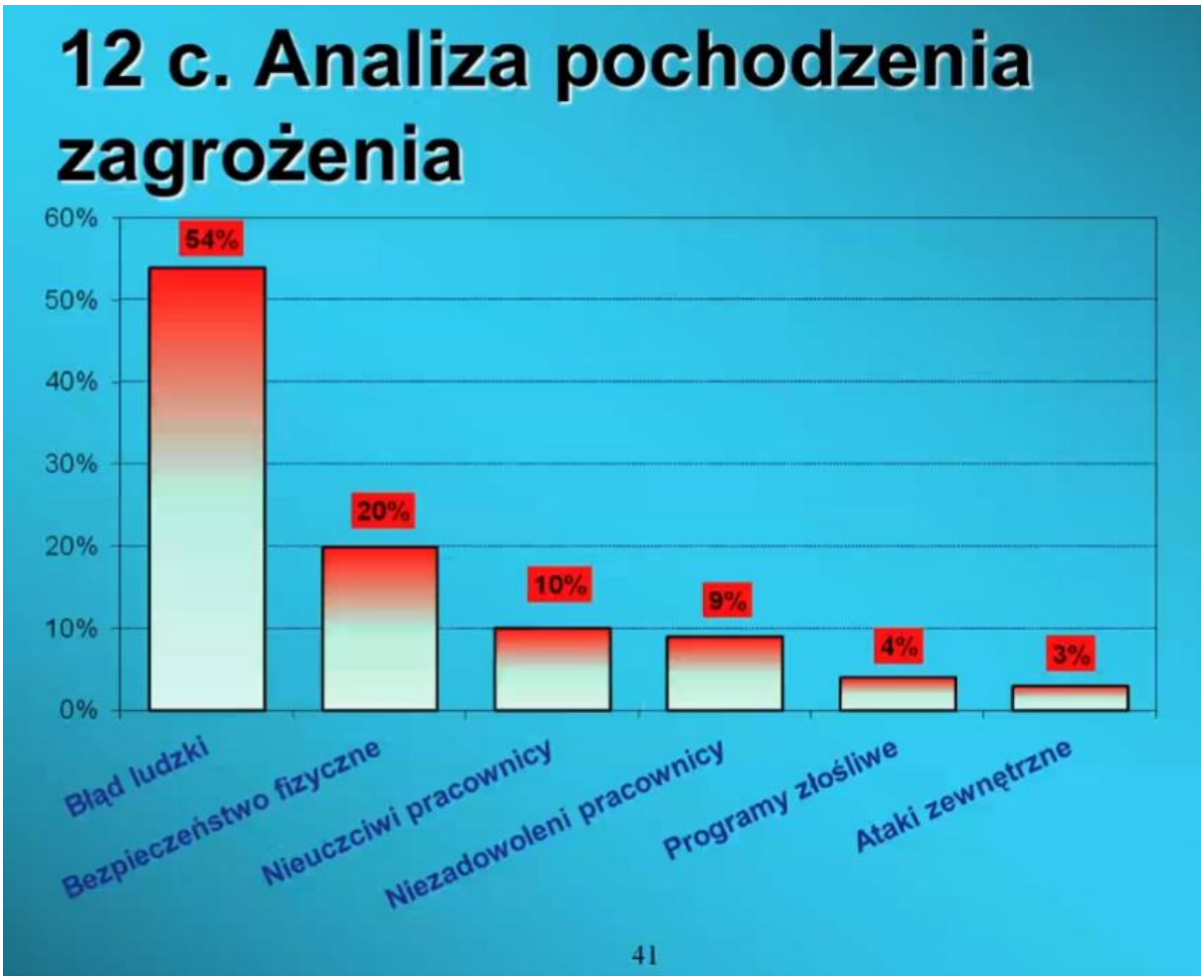
Wymień i krótko opisz minimum cztery najczęściej spotykane zagrożenia dla bezpieczeństwa systemu.
Wprowadź odpowiedź

Błąd ludzki -

Bezpieczeństwo fizyczne –

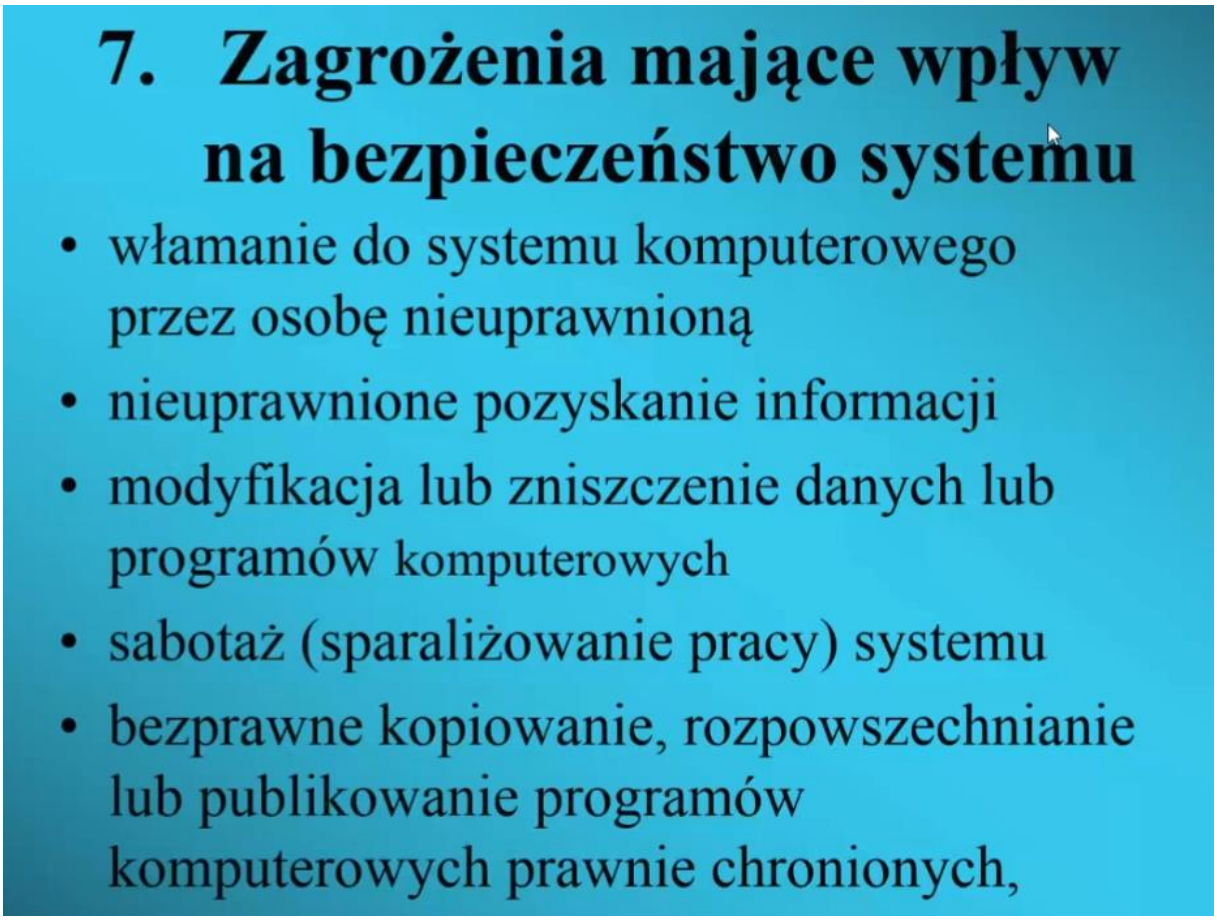
Nie uczciwy pracownik -

Niezadowolony pracownik -



Formy ataku elektronicznego

- **podszywanie** (masquerading)
- **podsłuch** (eavesdropping)
- **odtwarzanie** (replaying)
- **manipulacja** (tampering)
- **wykorzystywanie luk** (exploiting, penetration)



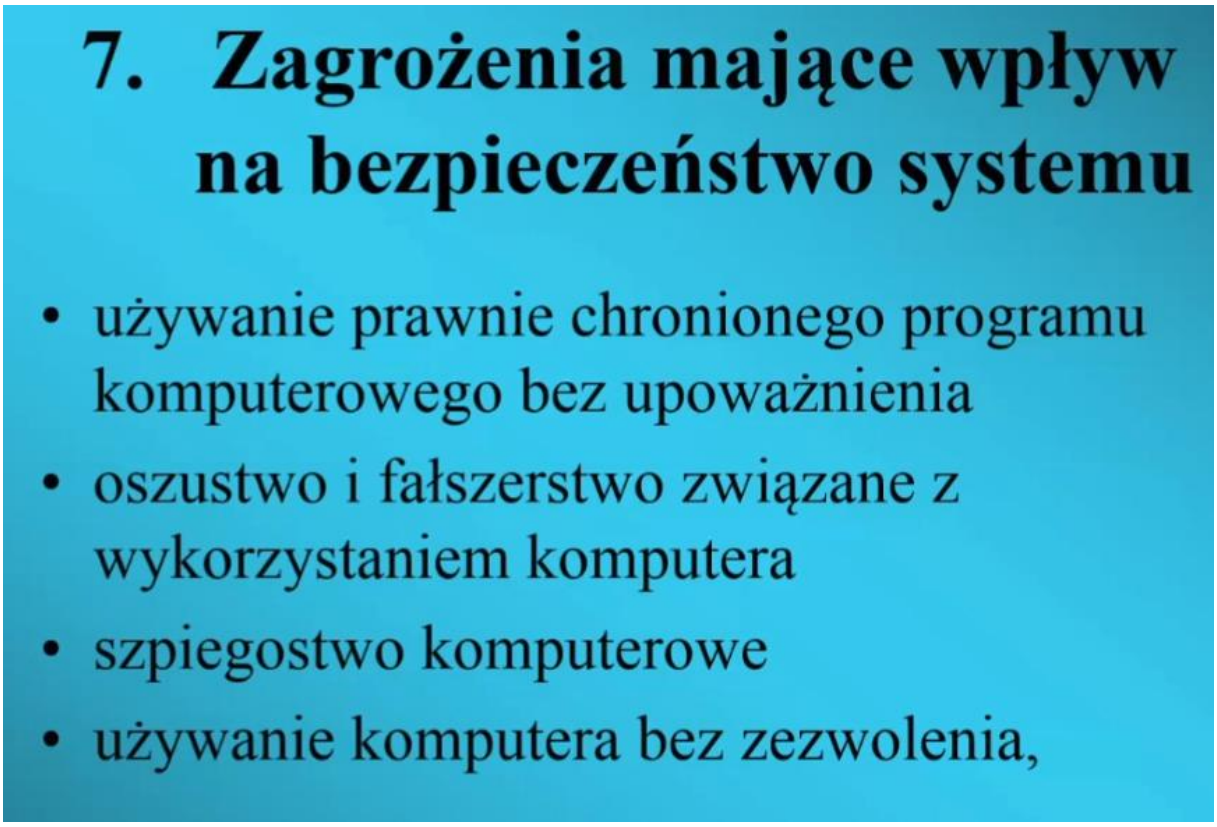
Włamanie do system komputerowego przez osobę nieuprawnioną

Nieuprawnione pozyskanie informacji

Modyfikacja lub zniszczenie danych lub programów komputerowych

Sabotaż systemu

Bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych



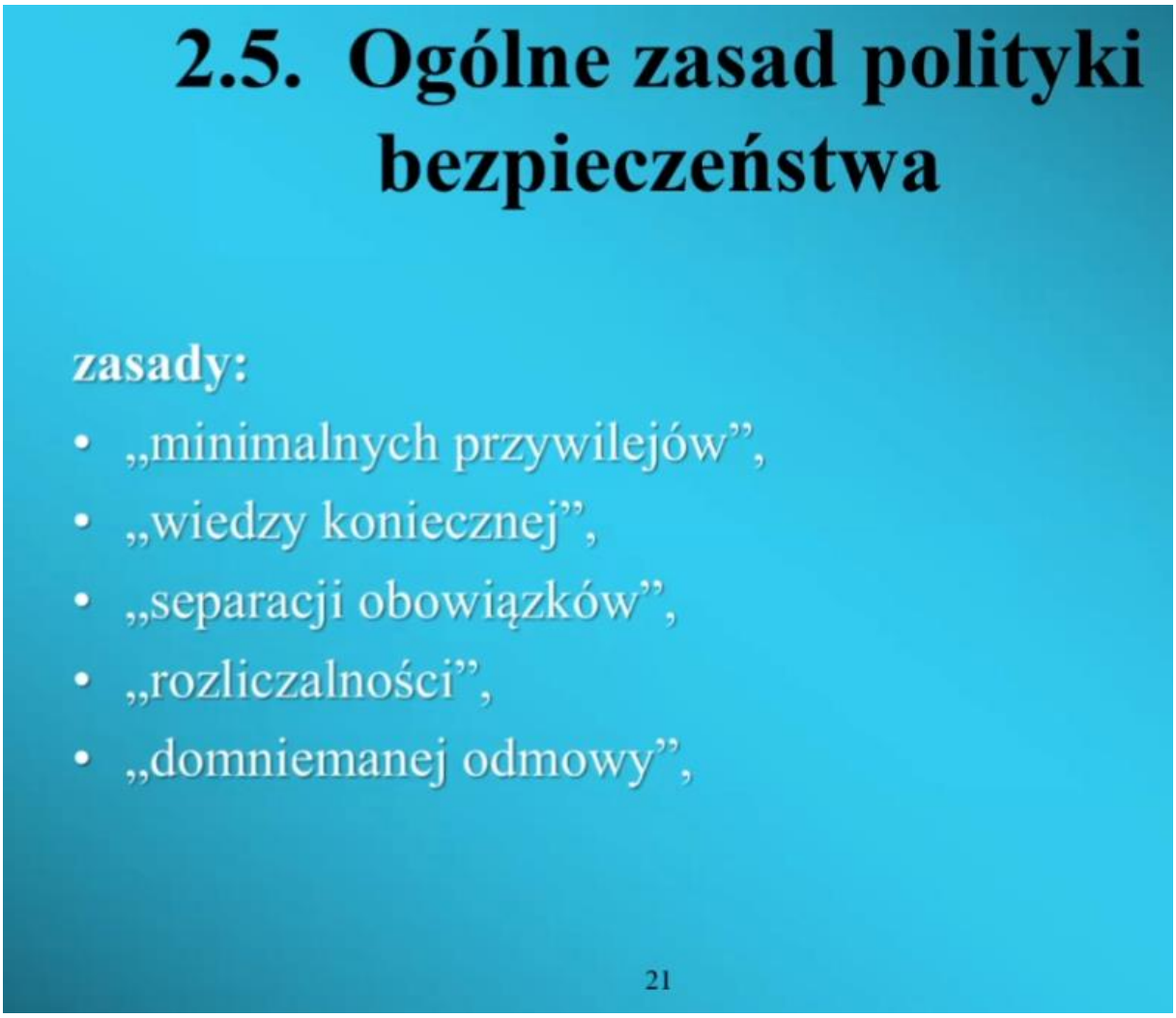
Używanie prawnie chronionego programu komputerowego bez upoważnienia

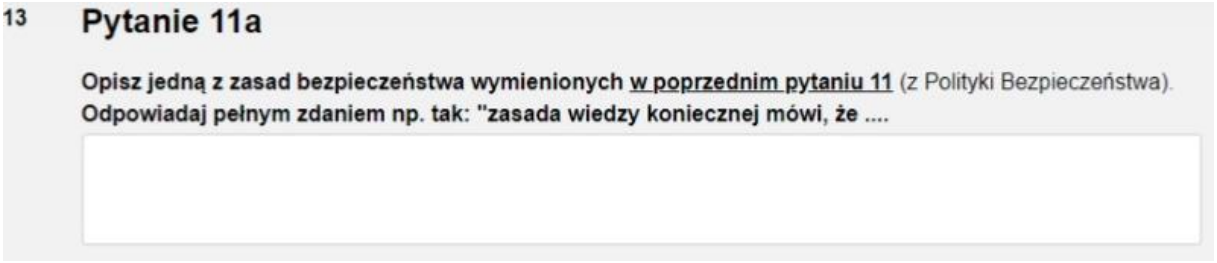
Oszustwo i fałszerstwo związane z wykorzystaniem komputera

Szpiegostwo komputerowe

Używanie komputera bez zezwolenia

1,2,3,4,5





Minimalne przywileje – Przydzielane są tylko takie prawa które są niezbędne do wykonania określonego zadania.

Wiedza konieczna - Użytkownik sytemu dostaje taki zakres wiedzy o swoich zasobach do których ma prawo dostępu.

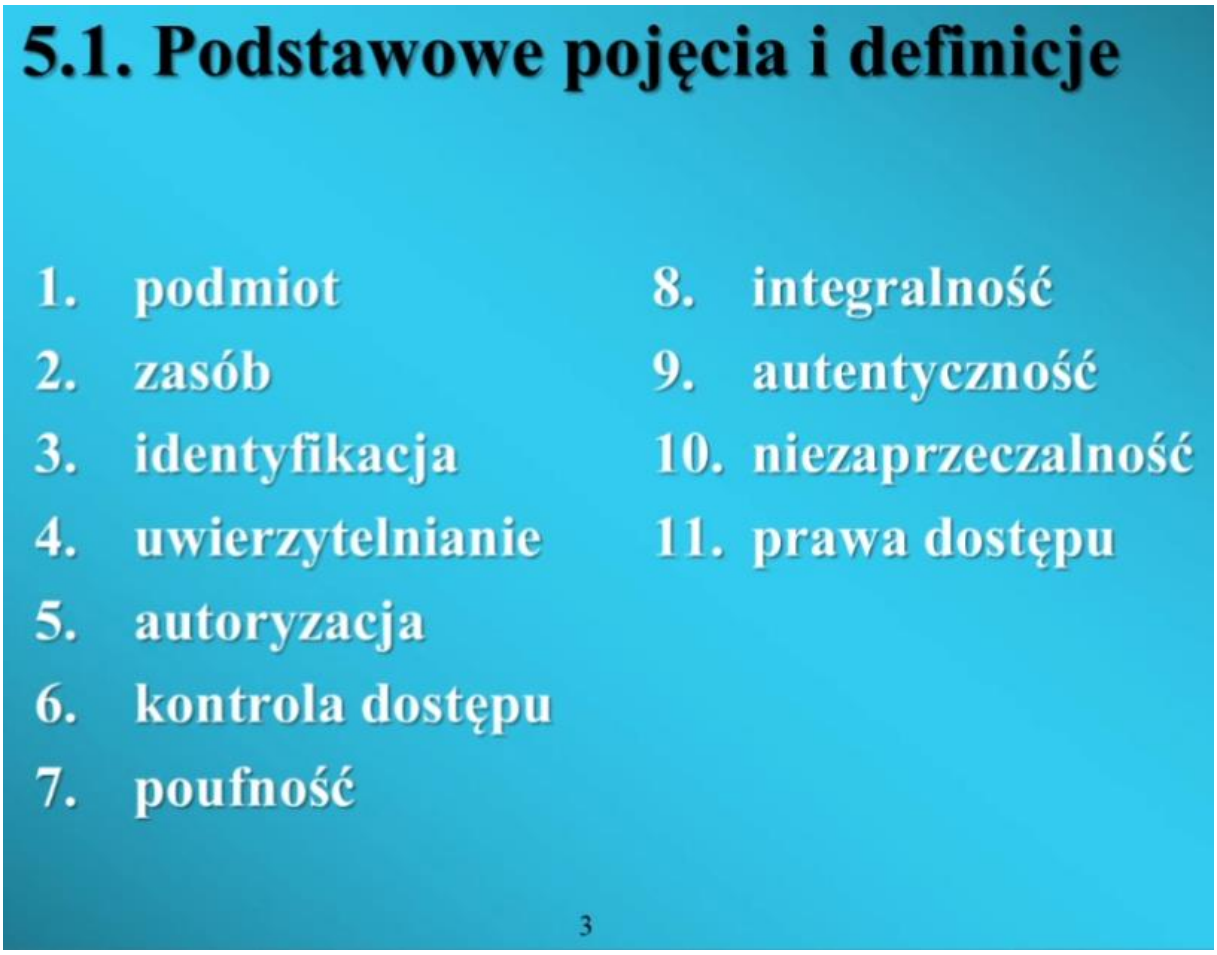
Separacja bojowisku – krytyczne zadnia nie mogą być realizowane przez jedną osobę

Rozliczalność – zapewnienie jednoznacznej odpowiedzialności

Domniemanej odmowy – jeśli nie wiadomo czy jest dozwolone to jest zabraniane

14 **Pytanie 12c**

Co to jest Podatność ? (podaj definicję)
(vulnerability) odpowiadaj pełnym zdaniem: Podatność jest to lu ...



Podmiot to byt który jakim sposób dostępu do zasobów co może być użytkownik , grupa urzędników, terminale, komputery, aplikacje, procesy

Zasób - wszystko to co dla instytucji ma jakąś wartość

Identyfikacja - rozróżnienie

Uwierzytelnienie - weryfikacja tożsamości użytkownika

Autoryzacja – prawa dostępu do zasobów

Kontrola dostępu – zidentyfikować podmiot i nadzorować prawa dostępu przez ten podmiot

Podatność jest to ochrona informacji przed nieautoryzowanym dostępem.

Integralność – ochrona przed nieautoryzowaną zmianom

Atletyczność – pewność do pochodzenia danych zasobów

Niezaprzeczalność – ochrona przed fałszywy zaprzeczeniem

Prawo dostępu – dopuszczalne sposoby wykorzystania zasobów przez podmiot

15 **Pytanie 12d**

Co to jest Incydent Bezpieczeństwa? (podaj definicję)
(security incident) odpowiadaj pełnym zdaniem np. tak" Incydent bezpieczeństwa jest to niekorzystne ...

Incydent bezpieczeństwa jest to niekorzystne zdarzenie związane z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

16 **Pytanie 13**

Dopasuj opisy podstawowych elementów systemu IDS/IPS

Dopasuj elementy systemu do ich opisów:

	sonda	baza danych	analizator logów
element analizujący ruch sieciowy i wykrywający ataki	○	○	○
element zbierający informacje o atakach z grupy sensorów	○	○	○
element umożliwiający wizualizację i analizę logów z grupy sensorów	○	○	○

1

2

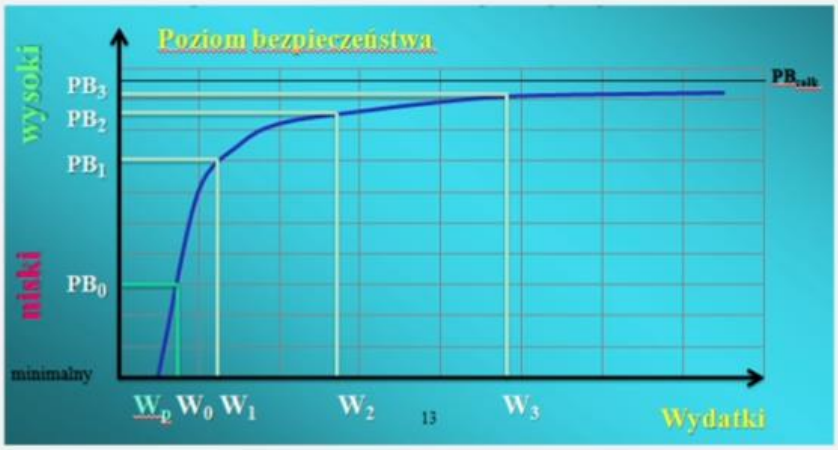
3

3.3.3. Ważne definicje

- IDS, IPS – urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym.
- Typowe elementy systemu IDS/IPS to:
  - sonda (ang. sensor) – element analizujący ruch sieciowy i wykrywający ataki,
  - baza danych – zbierająca informacje o atakach z grupy sensorów,
  - analizator logów – umożliwiający wizualizację i analizę logów z grupy sensorów.

Zródło: Wikipedia

17 **Pytanie 14**



Na podstawie powyższego rysunku omów zależności pomiędzy ponoszonymi wydatkami a poziomem bezpieczeństwa (zaznacz tylko prawdziwe odpowiedzi).
Wybierz jedną lub więcej odpowiedzi

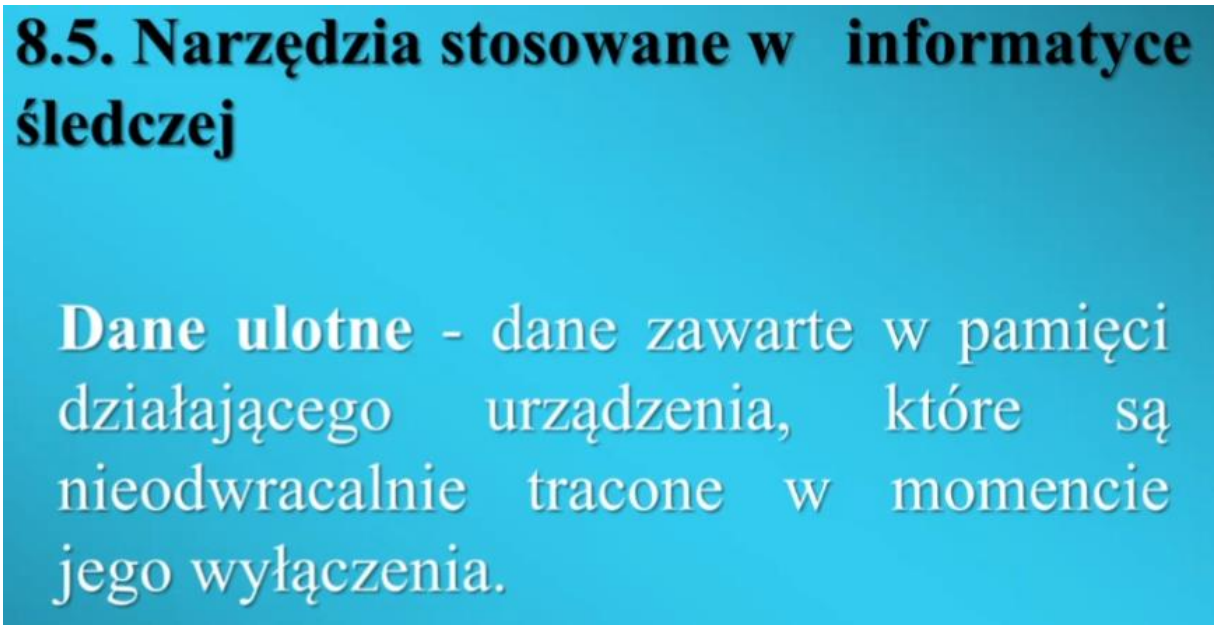
- ☐ w systemie o małym poziomie bezpieczeństwa, już niewielkie zwiększenie wydatków (W0 do W1) powoduje znaczny wzrost poziomu bezpieczeństwa (z PB0 do PB1)
- ☐ w systemie o bardzo wysokim poziomie bezpieczeństwa, nawet bardzo duże (W2 do W3) zwiększenie wydatków powoduje niewielki wzrost poziomu bezpieczeństwa (z PB2 do PB3)
- ☐ minimalny poziom bezpieczeństwa mamy zagwarantowany w każdym systemie
- ☐ w systemie o małym poziomie bezpieczeństwa, niewielkie zwiększenie wydatków (W0 do W1) nie powoduje żadnego wzrostu poziomu bezpieczeństwa (z PB0 do PB1)
- ☐ w systemie o bardzo wysokim poziomie bezpieczeństwa, bardzo duże (W2 do W3) zwiększenie wydatków powoduje wzrost poziomu bezpieczeństwa (z PB2 do PB3) nawet do 100%
- ☐ w praktyce nigdy nie osiągniemy maksymalnego (całkowitego) poziomu bezpieczeństwa
- ☐ jeśli chcemy osiągnąć tylko minimalny poziom bezpieczeństwa to i tak wymaga to wydatków (WP)

1,2,6,7

18 **Pytanie 15**

Podaj definicją „danych ulotnych”
Wprowadź odpowiedź pełnym zdaniem:

Dane ulotne – dane zawarte w pamięci działającego urządzenia, które są nieodwracalne tracone w momencie jego wyłączenia.



19 **Pytanie 15a**

Zaznacz które z poniższych to „dane ulotne”
Wybierz jedną lub więcej odpowiedzi

- ☐ otwarte pliki i rejestry
- ☐ działające procesy i usługi
- ☐ typ i model komputera
- ☐ kolor samochodu dwóch ostatnich użytkowników
- ☐ pliki SWAP
- ☐ aktualna data i czas (zarówno komputera jak i w realnym świecie)
- ☐ zawartość RAM
- ☐ informacja o komputerach "w otoczeniu sieciowym"
- ☐ informacja o połączeniach sieciowych (np. otwarte porty, adresy)

1,2,5,6,7,8,9

8.5.1. Przykłady danych ulotnych

- **aktualna data i czas,**
- **zawartość pamięci ulotnej** (pamięć RAM i pliki swap),
- **połączenia sieciowe** (otwarte porty TCP lub UDP, NetBIOS, informacja o komputerach znajdujących się w tej samej sieci, pakiety sieciowe),
- **zalogowani użytkownicy, konta użytkowników,**
- **zawartość schowka systemowego,**

8.5.1. Przykłady danych ulotnych

- **działające procesy i usługi,**
- **zaplanowane zadania,**
- **otwarte pliki i rejestry,**
- **dane z autouzupełnienia** (np. z przeglądarek, hasła, itp.),
- **zrzut ekranu,**
- **skasowane dane**

20 **Pytanie 16**

Ustaw fazy ataku elektronicznego **we właściwej kolejności**:

kolumny oznaczają kolejne kroki ataku

	krok 6	krok 2	krok 3	krok 4	krok 5	krok 1
Propagacja ataku (jeśli przygotowaliśmy opanowany system do dalszych działań)	○	○	○	○	○	○
Skanowanie – szukanie słabości, np. sondowanie usług, badanie portów	○	○	○	○	○	○
Wyznaczenie celu, np. niezabezpieczona usługa, znany exploit, (najlepiej podatność 0-Day)	○	○	○	○	○	○
Atak na system	○	○	○	○	○	○
Usuwanie śladów (ukrycie ataku i jego skutków)	○	○	○	○	○	○
Modyfikacja systemu (jeśli planujemy np. późniejszy powrót, chcemy zatrzeć ślady)	○	○	○	○	○	○

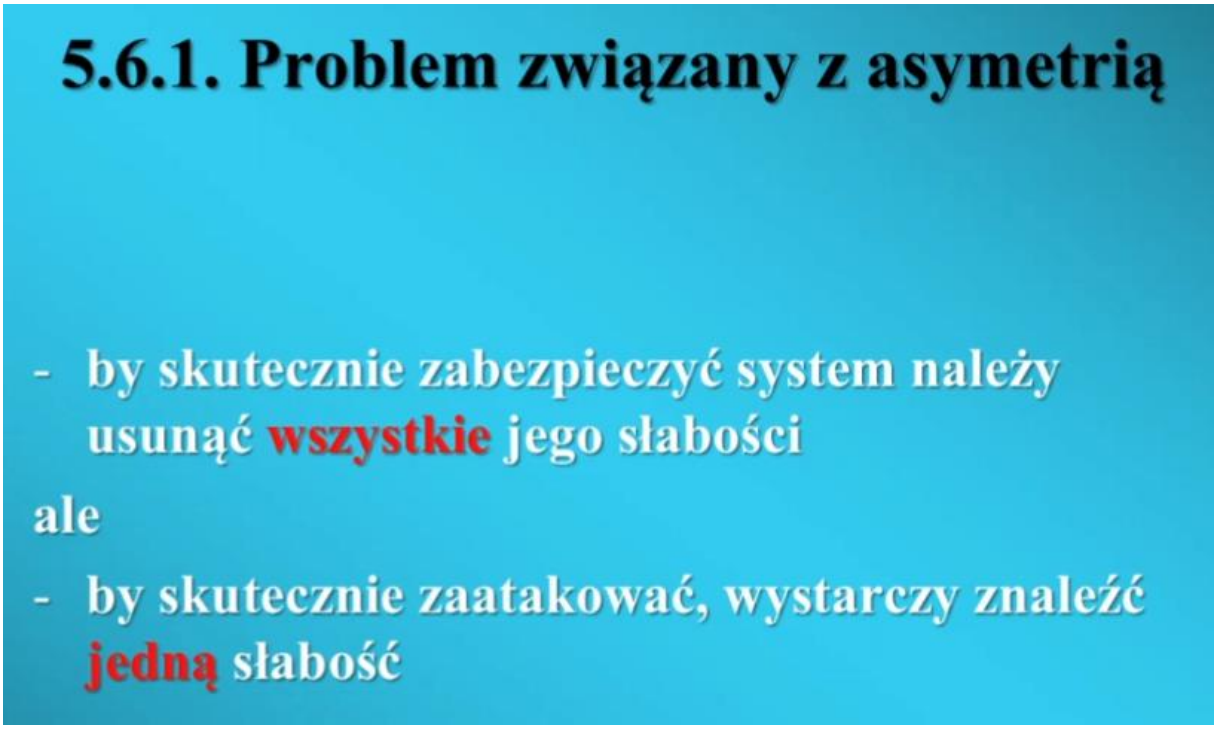
2,3,4,6,5,1

21 **Pytanie 17**

W kontekście bezpieczeństwa systemu połącz prawidłowo poniższe zdania:

Dopasuj wartości z kolumn tak by pasowały w zdaniach w miejsce kropek:

	wszystkie	żadną	minimum JEDNĄ	minimum DWIE	tylko przesłanki
by skutecznie zaatakować, wystarczy znaleźć ..... słabość	○	○	○	○	○
by skutecznie zabezpieczyć system należy usunąć ..... jego słabości	○	○	○	○	○



3

1

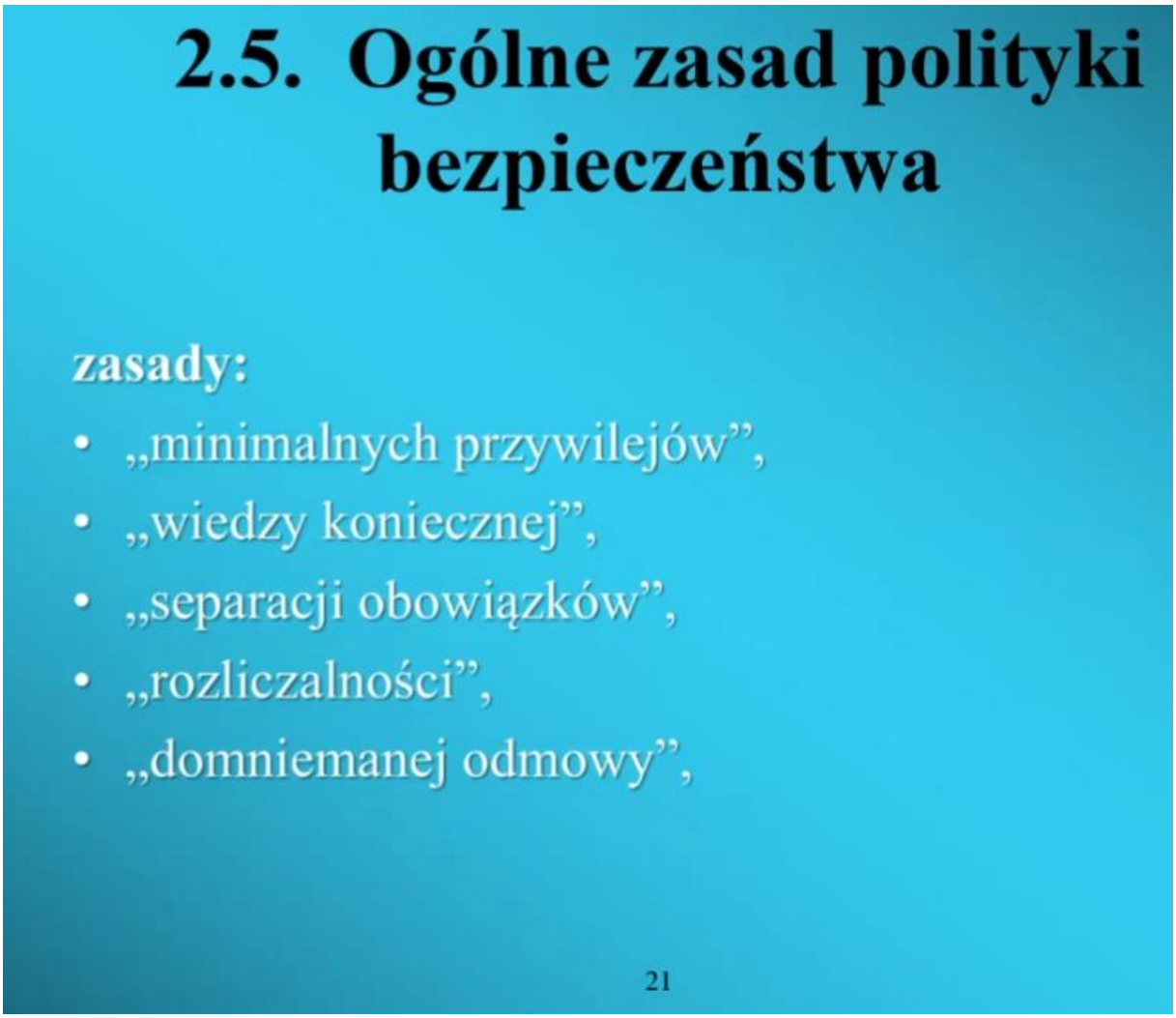
Egzamin 2

10 **Pytanie 9b**

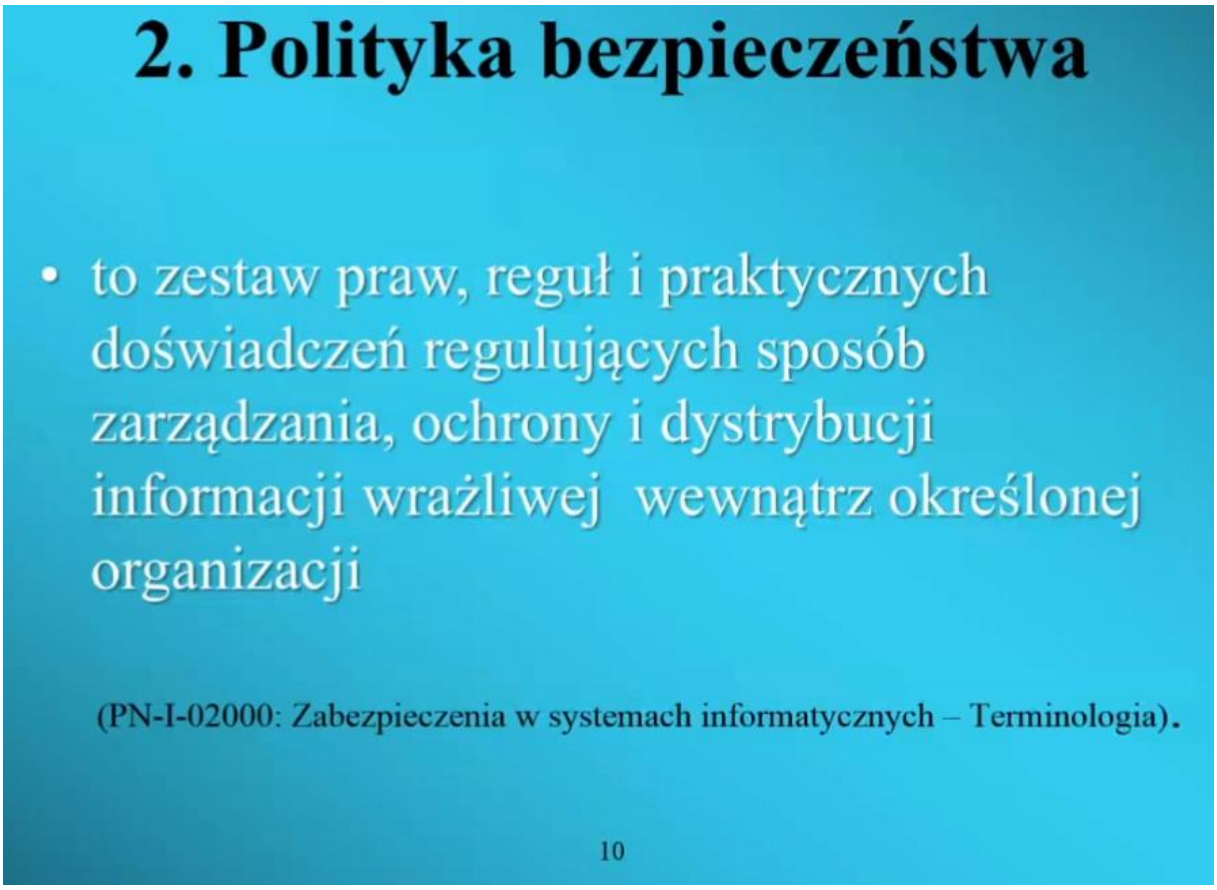
Co oznacza następujący atrybut wiarygodności systemu - **rozliczalność** (accountability)

Wprowadź odpowiedź

Rozliczalność - Wiadomo jakie, gdzie i kiedy dany podmiot wykonał działania.



Polityka Bezpieczeństwa jest to zbiór/zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji.



15 **Pytanie 12b**

Co to są Zasoby/Aktywa (podaj definicję)
(sets) jest to wszystko to co ...

Zasób - wszystko to co dla instytucji ma jakąś wartość

Określenie zasobów = „Co chronić?”

Zasoby jakie mogą podlegać ochronie obejmują m.in. (w zależności od typu instytucji, dziedziny działalności itp.):

sprzęt komputerowy

infrastruktura sieciowa

wydruki

strategiczne dane

kopie zapasowe

wersje instalacyjne oprogramowania

dane osobowe

dane audytu

zdrowie pracowników

prywatność pracowników

zdolności produkcyjne

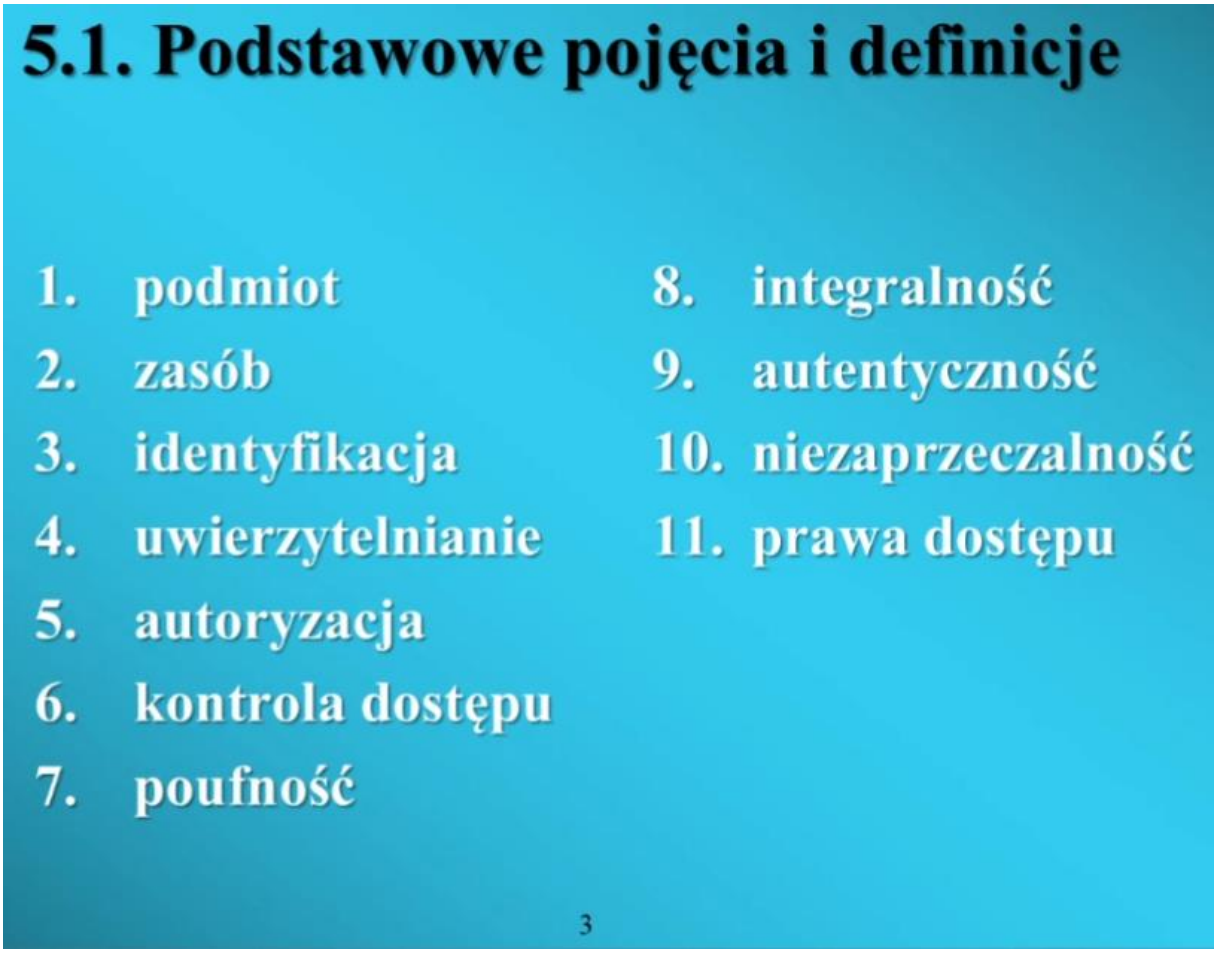
wizerunek publiczny i reputacja

Zasób (obiekt)

* jest jednostką, do której dostęp podlega kontroli

* przykłady: programy, pliki, relacje bazy danych, czy całe bazy danych

* obiekty o wysokiej granulacji: poszczególne elementy bazy danych



Brudnopis:

związane z polityk polityką bezpieczeństwa, to zasady: – pełnej świadomości (bardzo (bardzo ważna) – niezbędnych usług – niemożliwego do osiągnięcia stanu całkowitego całkowitego

bezpieczeństwa – konieczności stosowania stosowania norm, standardów standardów i tzw.

„dobrych „dobrych praktyk” praktyk” – równowagi równowagi kosztów kosztów zabezpiecze zabezpieczeń i wartości zasobów zasobów – równowagi równowagi pomiędzy zastosowanymi zastosowanymi mechanizmami mechanizmami

ochrony ochrony a zmianami zmianami w systemie(systemie(-ach)

Zasób - wszystko to co dla instytucji ma jakąś wartość

Jednostka do które mamy kontrole dostępu do wszystko to co dla instytucji ma jakąś wartość

Zasób jest to wszystko to co dla instytucji ma jakąś wartość

Polityka Bezpieczeństwa jest to zbiór/zestaw zasad

zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonej organizacji

danych osobowych wewnątrz określonej organizacji.