

1. Atrybuty informacji

Tajność (dostęp do określonych danych i informacji posiadają tylko uprawnione osoby), integralność (dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji), dostępność (dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika)

2. Czego dotyczy norma 27001?

Systemów zarządzania bezpieczeństwem informacji

3. Czy w polskim prawie karnym jest paragraf na włamania komputerowe

TAK

4. Jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa

niejawny / zastrzeżony / do użytku wewnętrznego

5. Jakie klauzule odpowiadają tajemnicy państowej

Tajność, ścisła tajność

6. Zasada dostępu tylko do takich informacji przez pracownika, które mu są w tej chwili potrzebne to

Zasada wiedzy koniecznej

7. Hoax – co to

Akt socjotechniczny

8. Miara bezpieczeństwa w common criteria (norma iso 15194)

Jest to poziom uzasadnionego zaufania

9. Cechy podpisu elektronicznego

Integralność, autentyczność, niezaprzeczalność

10. Jaka norma jest od systemu zarządzania bezpieczeństwem/ wymagania dotyczące bezpieczeństwa teleinformatycznego

Norma ISO27001

11. Różnica pomiędzy pełnym audytem informatycznym, a audytem bezpieczeństwa teleinformatycznego

Pełny audit jest nadzorem audytu bezpieczeństwa

12. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państowa

Tajność, ścisła tajność

13. Jaki powinien być dokument „Planowania bezpieczeństwa dla...”, polityka

Jawny

14. Na czym bazuje autoryzacja dostępu

Na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy

15. Co zapewnia Common Criteria i standard ISO/IEC 15408

Odp ze słowem zaufanie, odpowiedni poziom zaufania

16. Do czego wykorzystywany jest outsourcing

Transfer ryzyka

17. Metody uwierzytelniania pracowników / na czym bazuje autoryzacja dostępu

Weryfikacja przedmiotu posiadanego przez użytkownika (przepustka)

**Weryfikacja cech fizycznych użytkownika (odcisk palca, oko, długość fallusa)**

**Weryfikacja wiedzy użytkownika (piny, hasła)**

18. Co zapewnia podpis cyfrowy

**Jednoznaczność, autentyczność, niezaprzecjalność, (odp z największą liczbą wymienionych cech)**

19. Jakie klauzule odpowiadają tajemnicy służbowej

**Poufne i zastrzeżone**

20. Co nie jest plikiem systemowym NTFS

**\$Sector**

21. Co to jest informacja

**Obiekt abstrakcyjny, który może zwiększyć obszar wiedzy. Z teorii informacji to miara niepewności zajścia pewnego zdarzenia ze zbioru skończonego zdarzeń prawdziwych**

22. Co to jest zagrożenie pasywne i aktywne

**Aktywne – dowolne zagrożenie związane z zamierzoną, nieuprawnioną zmianą stanu systemu przetwarzania danych**

**Pasywne – nie będące skutkiem celowego działania**

23. Ubezpieczenie zalicza się do

**Transferu ryzyka**

24. Co się dzieje z plikiem po usunięciu z dysku

**Wpis w \$MFT zostaje, dane zostają i zmieniają się dwie flagi**

25. Minimalny zestaw wymagań na system zabezpieczeń

**Dywersyfikacja, niezaprzecjalność, spójność i organizacja według zasady ochrony „w głąb”**

26. Zasada, żeby pracownik do wykonywania pracy miał tylko dostęp do tych programów i usług, których potrzebuje, to

**Zasada minimalnego środowiska pracy**

27. Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania

**Minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia**

28. Jeśli wysłemy sygnał na port 80 sprawdzający czy jest otwarty i odpowiedź dostaniemy z flagą RST to znaczy, że port jest

**Zamknięty**

29. Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuj uzyskać dostęp do pliku nazywa się

**weryfikacja autoryzacji**

30. W których Windowsach domyślnie włączony jest dziennik zdarzeń

**Vista + win 7**

31. W którym Windowsie było logowanie zdarzeń

**Od 2000 w góre**

32. Ile jest well known portów

**1024**

33. Co to jest SNORT  
**IDS/IPS ...**
34. Usługa kolokacji  
**Udostępnienie miejsca, własny sprzęt**
35. Co to jest SandBox  
Służy do izolacji/separacji programów
36. Co to jest Recovery Point Object  
**A w cudzysłowie / był szacowany podczas analizy ryzyka – określa maksymalny.**  
Szacowany czas pracy możliwy do zaakceptowania przez kierownictwo organizacji
37. Co to jest UTM  
**Wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia**
38. Na czym polega hosting  
**Udostępnienie centrum danych i sprzętu**
39. Na czym polega personal firewall  
**Filtracja pakietów, kontroluje ruch sieciowy do i z komputera**
40. Zapis plików przez tydzień, klonowanie plików  
**Przyrostowe**
41. Co to jest steganografia  
**Metoda ukrywania/utajniania informacji**
42. Promieniowanie ujawniające  
**Jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanej w systemie komputerowym**
43. Zasada Kerchoffa  
**B klucz jest tajny a nie shaker**
44. Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową jest równoważne co do skutków prawnych, użyciu bezpiecznego podpisu elektronicznego weryfikowanego klasyfikowanym certyfikatem  
**tak**
45. retencja aktywna
46. od poniedziałku do czwartku o 18 jest backup niepełny a w piątek o 18 pełny, jeśli w czwartek o 17:50 zepsuje się system to ile dysków z backupem potrzeba żeby odnowić system  
**jeden backup = jeden dysk**
47. Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym  
**Zapis najważniejszych ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa**
48. Zgodnie z ustawą o ochronie informacji niejawnych informacje nie jawne oznacza się klauzulą

**Ścisłe tajne lub tajne lub poufne lub zastrzeżone**

49. Podpis cyfrowy ma za zadanie zapewnić

**Niezaprzecjalność, autentyczność, integralność informacji**

50. Za pomocą VPN nie da się zabezpieczyć

**Dostępności**

51. Test penetracyjny to

**Metoda zbierania informacji o badanym systemie**

52. Postępowanie i wdrożenie planów zapewniania ciągłości działania w ramach metod postępowania z ryzykiem to

**Kontrolowania ryzyka**

53. w zakresie bezpieczeństwa informacyjnego

**Wymaga tzw wzorca audytowego i niezależności podmiotu wykonującego audit**

54. Wymagania na system zarządzania bezpieczeństwem informacji (SZBI) są opisane w normie

**PN-ISO/IEC-27001**

55. Zasada ochrony w głąb

**Jak przedostanie się przez zaporę to napotyka drugą**

56. Backup, który zapisuje raz pełny a potem tylko modyfikacje

**Różnicowy**

57. RTA time actual

**Eksperymenty do wyznaczania czasu/ czas przywrócenia danych (eksperimentalny)**

58. Audytem wewnętrznym w SZBI

**Audyt strony trzeciej**

59. Podstawą sukcesu procesów biznesowych i projektowych w SZBI

**Wszystkie wymienione powyżej**

60. Atrybuty informacji podlegające ochronie

**Wszystkie wymienione powyżej**

61. Przyczyny utraty tajności, integralności i dostępności informacji

**Wszystkie wymienione powyżej**

62. W windows XP dzienniki są

**Aplikacji, zabezpieczeń, system(domyślnie włączone)**

63. Co jest wyposażeniem teleinformatycznym wg PN-EN ISO/IEC 17025

**Najdłuższa odp, oprogramowanie, urządzenia ...**

64. Plan bezpieczeństwa powinien być

**Dostępny zgodnie z zasadą wiedzy koniecznej**

65. Kolejność wykonywania exploita

**Mfsconsole -> mfsupdate -> use exploit <nazwa> -> RHOST <ip ofiary> -> LHOST <ip intruza> -> exploit**

66. Island hopping

**Atakowanie najsłabszego systemu i skakanie na inne**

67. Ochrona danych osobowych

Tylko dla żyjących

**1. Podstawowe atrybuty informacji związane z bezpieczeństwem**

- tajność, integralność, dostępność
- tajność integralność długość (w znakach)
- tajność integralność długość (w bajtach)
- integralność, metoda szyfrowania, dostępność

**2. Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym**

**- zapis najważniejszych ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa**

- wykaz stosowanych podstawowych zabezpieczeń informacji
- instrukcje i procedury dla osób korzystających z systemów teleinformatycznych
- szczegółowy plan obiegu informacji i schematu sieci telefonicznych

**3. Zgodnie z ustawą o ochronie informacji niejawnych informacje niejawne oznacza się klauzulą**

- ścisłe tajne lub tajne lub poufne lub zastrzeżone
- ścisłe tajna lub tajne
- poufne lub zastrzeżone
- jawne

**4. Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku nazywa się**

- weryfikacja tożsamości
- weryfikacja autoryzacji**
- weryfikacja poziomu ochrony
- weryfikacja uwierzytelniania

**5. Norma 27001 dotyczy**

- klas metod kryptograficznych
- konstrukcji bezpiecznych produktów informatycznych
- sposobów archiwizowania informacji
- systemów zarządzania bezpieczeństwem informacji**

**6. Podpis cyfrowy ma za zadanie zapewnić**

- tylko integralność informacji
- tylko poufność i autentyczność informacji
- dostępność informacji
- niezaprzecalność, autentyczność, integralność informacji**

**7. Za pomocą VPN nie da się zabezpieczyć**

- dostępności**
- integralności
- czytelności

**8. Test penetracyjny to**

- to samo co audyt bezpieczeństwa informacyjnego
- metoda zbierania informacji o badanym systemie**
- metoda włamywania się do systemu informatycznego
- to samo co atak socjotechniczny

**9. Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informatycznych obejmuje**

- dywersyfikacja i spójność
- dywersyfikacja, niezaprzeczalność i organizacja wg zasady ochrony w głęb
- dywersyfikacja, niezaprzeczalność, spójność i organizacja wg zasady ochrony w głęb**
- dywersyfikacja i organizacja wg zasady ochrony w głęb

**10. Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową jest równoważne, co do skutków prawnych, użyciu bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem?**

- tak**
- nie

**11. Postępowanie i wdrożenie planów zapewniania ciągłości działania w ramach metod postępowania z ryzykiem to**

- retencji ryzyka
- transferu ryzyka
- unikania ryzyka
- kontrolowania ryzyka**

**12. Podstawowe metody realizacji operacji uwierzytelniania tożsamości użytkownika to:**

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja wiedzy użytkownika, weryfikacja jego uprawnień systemowych
- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja komputera z którego loguje się użytkownika
- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja wiedzy użytkownika**

**13. Audyt w zakresie bezpieczeństwa informacyjnego**

- wykonuje się przy okazji sporządzania spisu zasobów informacyjnych
- jest tym samym co test penetracyjny
- wymaga tzw wzorca audytowego i niezależności podmiotu wykonującego audit**
- polega na sprawdzeniu logów systemowych przez administratora systemu teleinformatycznego

**14. Wymagania na system zarządzania bezpieczeństwa informacji (SZBI) są opisane w normie**

- PN-ISO/1EC-9001
- PN-ISO/1EC-15408
- PN-ISO/1EC-27001**
- nie są opisane w żadnej normie

**15. Promieniowanie ujawniające**

- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności i integralności informacji przetwarzanych w systemie komputerowym
- jest promieniowaniem elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanym w systemie komputerowym
- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanej w systemie komputerowym**
- nie stanowi zagrożenia

**17. Czy obowiązujący w Polsce Kodeks Karny przewiduje sankcje za nieuprawnione, szkodliwe działanie wobec systemu komputerowego i informacji w nich przetwarzanej?**

- tak**
- nie

**18. Dokument „Polityka bezpieczeństwa teleinformatycznego dla...” powinien być dokumentem**

- do użytku wewnętrznego
- jawnym**
- nie ma znaczenia
- poufnym

**19. Uznaniowe sterowanie dostępem wykorzystuje:**

- atrybut własności obiektu**
- nadanie obiektem i podmiotom etykiety
- przypisane podmiotom role
- przypisane do podmiotów i obiektów: atrybuty, warunki opisujące środowisko i zbiory zasad

**(MOŻNA JESZCZE SIĘ NAUCZYĆ:**

**1. Uznaniowe sterowanie dostępem (ang. *Discretionary Access Control*, DAC).**

Środki ochronne ograniczające dostęp do obiektów wykorzystują atrybut własności obiektu, umożliwiający podmiotowi-właścicielowi nadanie lub odebranie innemu podmiotowi (lub grupie podmiotów) prawa dostępu do obiektu, którego jest właścicielem.

**2. Obowiązkowe sterowanie dostępem (ang. *Mandatory Access Control*, MAC).**

Środki ochronne ograniczające dostęp do obiektów wykorzystują przypisane do obiektów etykiety określającej wymagany poziom siły ochrony obiektu oraz formalnie nadane podmiotom poziomy uprawnień (ang. *clerance level*).

**3. Sterowanie dostępem wykorzystujące role (ang. *Role Based Access Control*, RBAC).**

Uprawnienia dostępu do obiektów zamiast podmiotowi przypisane są rolom, które taki podmiot może pełnić.

**4. Sterowanie dostępem wykorzystujące atrybuty (ang. *Attribute Based Access Control*, ABAC)**

Środki ochronne ograniczające dostęp do obiektów wykorzystują przypisane do podmiotów i obiektów atrybuty, warunki opisujące środowisko i zbiory zasad wyspecyfikowane w terminach opisujących ww. atrybuty i warunki.

**20. Poprawna treść Zasady Kerckhoffsa to:**

- Odporność kryptosystemu powinna zależeć od utrzymania tajności klucza wybierającego konkretne przekształcenie, a nie od tajności przekształceń używanych w tym kryptosystemie
- Odporność kryptosystemu powinna zależeć od utrzymania tajności przekształceń używanych w tym kryptosystemie, a nie od tajności klucza wybierającego konkretne przekształcenie

<sup>8</sup> Nie należy mylić uwierzytelniania podmiotów z uwierzytelnianiem danych, tj. procesem wykorzystywanym do weryfikacji integralności danych, np. weryfikacji przeprowadzanej w celu stwierdzenia, czy dane otrzymane są identyczne z danymi wyslanymi (w tym celu można wykorzystać np. podpis cyfrowy).

**21. Do uwierzytelniania danych stosuje się:**

- hasła
- sumy kontrolne i podpisy cyfrowe**
- metody biometryczne
- tokeny

**22. Norma PN-ISO/IEC-15408 dotyczy**

- Sposobów archiwizowania informacji
- Klas metod kryptograficznych
- Konstrukcji i oceny "bezpiecznych" produktów informatycznych**
- System zarządzania bezpieczeństwem informacji

**23. Czy w polskim prawie karnym istnieje paragraf na włamania? (niedosłowne pytanie)**

Odpowiedź: TAK - włamanie jest aktem vandalizmu (skrypt 96-99)

**24. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:**

- Zasadą dwóch osób
- Zasadą rotacji obowiązków
- Zasadą minimalnego środowiska pracy
- Zasadą wiedzy koniecznej**

**2. Zasada wiedzy niezbędnej („wiedza konieczna”):**

*pracownik powinien wiedzieć tylko tyle, ile jest mu niezbędne do rzetelnego wykonywania jego obowiązków służbowych.*

**25. Jaki poziom ochrony powinien mieć dokument “instrukcja bezpieczeństwa”**

Odpowiedź: jawnny

**Polityka bezpieczeństwa informacyjnego** -> jawnny

**Plan bezpieczeństwa informacyjnego** -> udostępniany zgodnie z zasadą „wiedzy koniecznej”

**Instrukcja bezpieczeństwa informatycznego** -> do użytku wewnętrznego

**Plan zapewniania ciągłości działania** -> do użytku wewnętrznego, podlegający specjalnej ochronie

**26. Sandbox to:**

- rodzaj testu penetracyjnego wykonywany z zewnątrz, bez znajomości struktury oraz konfiguracji testowanego środowiska
- metoda porównania analizowanego obiektu z bazą sygnatur wirusów
- mechanizm służący do separacji programów oraz wykonywania niezaufanego kodu w odizolowanym środowisku**
- skaner portów

**27. Atak na system informacyjny i informację w nim przetwarzaną jest:**

- zagrożeniem
- sposobem realizacji zagrożenia**
- elementem socjotechniki
- narzędziem intrusa

**28. Terminem "hoax" określa się:**

- programowy obiekt złośliwy przeprowadzający działania destrukcyjne w systemie
- sprzętowy obiekt złośliwy posiadający zdolność powielania się
- rodzaj ataku socjotechnicznego - żart rozsyłany pocztą elektroniczną**
- programowy obiekt złośliwy posiadający zdolność powielania się

**29. Incydent z zakresu bezpieczeństwa informacyjnego to:**

- Stan systemu informacyjnego, którego powoduje lub może spowodować niepożądaną zmianę wartości istotnych kryteriów jakości informacji
- Zdarzenie lub ciąg zdarzeń (składających się na realizację zagrożenia) które powoduje lub może spowodować niepożądaną zmianę wartości istotnych kryteriów jakości informacji**
- Zawsze i tylko rezultat działania cyberprzestępcy
- Proces ujawniania podatności w systemie informacyjnym

**30. Czy podatność jest warunkiem koniecznym realizacji zagrożenia:**

- nie
- tak**

**31. Para (poziom atrybutu, kategoria informacji) wyznacza klasę:**

- bezpieczeństwa**
- sterowania dostępem
- uwierzytelniania
- autoryzacji

**32. Jakie klauzule odpowiadają tajemnicy państowej i tajemnicy służbowej:**

Informacje niejawne zaklasyfikowane jako stanowiące **tajemnicę państwową** oznacza się klauzulą:

- 1) "ściśle tajne"** - zgodnie z wykazem stanowiącym załącznik nr 1 do ustawy (część I);
- 2) "tajne"** - zgodnie z wykazem stanowiącym załącznik nr 1 do ustawy (część II).

2. Informacje niejawne zaklasyfikowane jako stanowiące **tajemnicę służbową** oznacza się klauzulą:

- 1) "poufne"** - w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli;
- 2) "zastrzeżone"** - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

**33. Podmiot świadczący usługi kolokacji:**

- szkoli pracowników klienta z ochrony zasobów informacyjnych
- serwisuje sprzęt komputerowy w siedzibie klienta
- udostępnia swoje centrum danych (infrastrukturę), a klient wstawia tam swój sprzęt**
- udostępnia klientowi swoje centrum danych (infrastrukturę) i swój sprzęt

**(WARTO UMIEĆ TEŻ**

**Hosting** – realizacja usługi (np. składowania danych) przez jej dostawcę na jego zasobach sprzętowych i programowych, w jego centrum danych.

**Kolokacja** – usługa polegająca na wynajęciu miejsca w centrum danych dostawcy usługi i umieszczeniu w nim własnego sprzętu komputerowego.

)

**34. Różnica pomiędzy pełnym audytem informatycznym, a audytem bezpieczeństwa teleinformatycznego**

-różnica jest taka, że pełny audit jest nadzorem audytu bezpieczeństwa

**35. Czy dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym:**

- TAK, chyba że przepisy odrębne stanowią inaczej**
- NIE

**36. Jakie etykiety ma wiadomość sklasyfikowana jako tajmenica państwową**

-tajność, ścisła tajność

**37. Parametr Recovery Time Actual (RTA) określa**

- maksymalny, możliwy do zaakceptowania przez kierownictwo organizacji ze względu na ponoszone straty, czas pracy bez możliwości korzystania z usług całości lub części systemu informatycznego
- ustalony drogą eksperymentalną czas przywrócenia działania systemu informatycznego i odtworzenia zbiorów danych**
- “akceptowanie straty w danych” (aktualność danych odtwarzanych po katastrofie) mierzone czasem od ostatniej kopii zapasowej do chwili katastrofy
- wymaganą długość przerwy w przetwarzaniu danych, niezbędnych do wykonania kopii zapasowej

**Recovery Time Actual (RTA)** – parametr ten określa, ustalany eksperymentalnie, czas odtworzenia systemu (RTO był szacowany podczas analizy ryzyka). Powinna być spełniona zależność  $RTA \leq RTO$ .

**38. UTM (Unified Threat Management) oznacza:**

- metodę szyfrowania danych uwierzytelniających
- metodykę analizy ryzyka na potrzeby bezpieczeństwa informacyjnego
- zespół zarządzający w firmie bezpieczeństwem teleinformatycznym
- integrację oprogramowania zabezpieczającego w jeden kompleksowy system ochrony, osadzany na specjalizowanej platformie sprzętowej**

**39. Inspektora bezpieczeństwa teleinformatycznego wyznacza się zgodnie z odpowiednią ustawą, w przypadku przetwarzania w systemach teleinformatycznych:**

- informacji wrażliwych
- danych osobowych
- informacji niejawnych**
- danych bankowych

**40. Założenia: kopia pełna jest wykonywana w każdy piątek o godz. 18:00; w dni robocze wykonywane są kopie różnicowe o godz. 18:00; każda kopia (także pełna) zajmuje jeden nośnik. Pytanie: nośniki z kopiami różnicowymi z jakich dni są niezbędne do odtworzenia zbiorów informacyjnych, jeżeli oryginalne zbiory zostały zniszczone w czwartek o 17:50 :**

- piątek, środa
- poniedziałek, wtorek, środa
- czwartek
- środa**

**41. Kopiowanie ( w celu wytworzenia kopii bezpieczeństwa), w którym w wybranym dniu tygodnia zapisujemy komplet danych, natomiast w pozostałe dni robocze zapisujemy jedynie dane zmienione od ostatniego kopирования nazywamy:**

- lustrzanym
- pełnym
- przyrostowym**
- różnicowym

INNY WARIANT -|

## kopiowanie z pełnym

Kopiowanie (w celu wytworzenia kopii bezpieczeństwa), w którym w wybranym dniu tygodnia z od ostatniego kopowania pełnego nazywamy:

Wybierz jedną odpowiedź:

- a. lustrzanym
- b. różnicowym
- c. przyrostowym
- d. pełnym

Odnacz mój wybór

**Odp. B**

## (WARTO SPRAWDZIĆ INNE

### 1. Kopia pełna

W ustalonych czasie (np. codziennie o godz. 17.00) kopiuje się na nośniki zapasowe zasoby informacyjne zgodnie ze specyfikacją z „Planu odtwarzania”, bez względu na to, czy zostały one zmodyfikowana czy też nie. Podstawową wadą tego rodzaju kopiowania jest wysokie zapotrzebowanie na nośniki danych.

### 2. Kopia różnicowa (tygodniowa)

W wybranym dniu (np. w piątek) zapisuje się komplet danych, natomiast w pozostałe dni robocze zapisuje jedynie dane zmienione od ostatniego kopiowania pełnego. Przechowywane są jedynie kopie pełne, nośniki z kopiami różnicowymi są kasowane po wykonaniu kolejnej kopii pełnej i używane ponownie, o ile takie działanie dopuszcza wdrożona polityka bezpieczeństwa.

### 3. Kopia przyrostowa (tygodniowa)

W wybranym dniu (np. w piątek) zapisuje się komplet danych, natomiast w pozostałe dni robocze zapisuje jedynie dane zmienione od ostatniego kopiowania. Przechowywane są jedynie kopie pełne, nośniki z kopiami przyrostowymi są kasowane po wykonaniu kolejnej kopii pełnej i używane ponownie, o ile takie działanie dopuszcza wdrożona polityka bezpieczeństwa.

)

## 42. Do czego wykorzystywany jest outsourcing?

Outsourcing -> przekazywanie (transfer) ryzyka

Outsourcing bezpieczeństwa może być korzystny dla organizacji, które nie posiadają wystarczających zasobów wewnętrznych lub specjalistycznej wiedzy, aby skutecznie zarządzać swoim bezpieczeństwem informatycznym. Pozwala to firmom skoncentrować się na swojej podstawowej działalności, jednocześnie korzystając z ekspertyzy specjalistów w dziedzinie bezpieczeństwa informatycznego. Jednakże, przed zastosowaniem outsourcingu, organizacje powinny dokładnie ocenić dostawców i dostosować usługi do swoich konkretnych potrzeb i regulacji branżowych.

## 43. Co zapewnia Common Criteria / standard ISO/IEC 15408:

Odpowiedni poziom zaufania (odp. ze słowem “Zaufanie”)

Common Criteria (CC), znane również jako ISO/IEC 15408, to międzynarodowy standard bezpieczeństwa informatycznego, który określa kryteria oceny bezpieczeństwa produktów i systemów informatycznych. Głównym celem Common Criteria jest ułatwienie porównywania i oceny poziomu bezpieczeństwa różnych produktów i systemów.

## 44. Produkty klasy SIEM służą do:

- nadzorowania obiegu informacji w systemie informatycznym i wspomagania przeciwdziałania jej wyciekowi
- kontroli tożsamości użytkowników systemu informatycznego
- korelowania wyników działania różnych narzędzi z zakresu bezpieczeństwa (IPS, WAF, itd.) oraz automatyzacji prezentacji wybranych zdarzeń i reakcji na te zdarzenia
- analizy i korelacji informacji wieloźródłowej o zdarzeniach zachodzących w systemie informatycznym i przedstawią w czasie zbliżonym do rzeczywistego spójnego, kompleksowego obrazustanu tego systemu

**SIEM** (ang. *Security Information and Event Management*) – oprogramowanie do analizy i korelacji informacji wieloźródłowej o zdarzeniach zachodzących w systemie informatycznym (pozyskiwanej z własnych agentów i z dzienników zdarzeń różnych urządzeń i programów zainstalowanych w systemie nadzorowanym) i na tej podstawie przedstawiający w czasie zbliżonym do rzeczywistego (ang. *near real-time*) spójny, kompleksowy obraz stanu systemu informatycznego przydatny do zarządzania ryzykiem operacyjnym IT.

**45. Co nie jest plikiem systemowym NTFS:**

Odpowiedź: \$Sector.

**46. Korzystanie z systemu ochrony fizycznej i technicznej obiektów, w ramach metod postępowania z ryzykiem, należy do:**

- a. kontrolowania ryzyka
- b. transferu ryzyka
- c. unikania ryzyka
- d. retencji ryzyka

**48. Ubezpieczenie zalicza się do...:**

- kontroli ryzyka
- retencji ryzyka
- transferu ryzyka

**49. Co się dzieje z plikiem po usunięciu go z dysku:**

- wpis w \$MFT jest usuwany, dane zostają
- wpis w \$MFT zostaje, dane zostają i zmieniają się dwie flagi
- wpis w \$MFT jest usuwany, dane są usuwane
- wpis w \$MFT zostaje, dane zostają

**50. Urządzenia forward proxy:**

- kontrolują dostęp procesów do konkretnych aplikacji
- ukrywają tożsamość klienta przed serwerem usługi
- kontrolują dostęp użytkowników do konkretnych aplikacji
- ukrywają tożsamość serwera usługi przed klientem

**Forward Proxy – ukrywają tożsamość klienta (przed serwerem usługi)**

**52. Informacja, której zmanipulowanie, uniedostępnienie lub ujawnienie może wyrządzić szkody w firmie lub osobie prywatnej to informacja**

- wrażliwa
- publiczna

- niejawną
- podatną

**54. Zasada, żeby pracownik do wykonywania pracy miał tylko dostęp do tych programów i usług, których potrzebuje, to:**

- zasada minimalnego środowiska pracy
- zasada wiedzy koniecznej
- zasada dwóch ludzi

**55. Ustalony eksperymentalnie czas przywrócenia działania systemu informatycznego i odtworzenia zbiorów danych określa parametr:**

- RTO
- BWO
- RPO
- RTA

**(WARTO ZOBACZYĆ TEŻ:**

Recovery Time Objective (RTO) – parametr ten określa maksymalny, możliwy do zaakceptowania przez kierownictwo organizacji, ze względu na ponoszone straty, czas pracy organizacji bez możliwości korzystania z określonych usług (w tym całości lub części systemu informatycznego).

Jest to jednocześnie maksymalny, szacowany czas odtworzenia systemu. RTO jest ustalany podczas analizy ryzyka, podlega zatwierdzeniu przez naczelnego kierownictwo organizacji.

Recovery Time Actual (RTA) – parametr ten określa, ustalany eksperymentalnie, czas odtworzenia systemu (RTO był szacowany podczas analizy ryzyka). Powinna być spełniona zależność  $RTA \leq RTO$ .

Recovery Point Objective (RPO) – parametr ten określa „akceptowalne straty w danych” mierzone ultraconym wolumenem zmian danych w czasie od ostatniej kopii zapasowej do chwili „katastrofy” (tj. wyznacza ostatni przed „katastrofą”, możliwy do odtworzenia, stan systemu).

Backup Window Objective (BWO) – parametr ten określa wymaganą długość przerwy w przetwarzaniu danych, niezbędną do wykonania kopii zapasowej.

Maximum Data Loss (MDL) – parametr ten określa maksymalną wielkość utraconych danych z uwzględnieniem dodatkowych możliwości odtwarzania (logi transakcji, dokumenty papierowe itp.).

**56. Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania:**

- minimalizujemy ryzyko
- minimalizujemy zagrożenia
- minimalizujemy podatności
- minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia

**57. Zapora osobista ma za podstawowe zadanie:**

- szyfrować transmitowane lokalnie pakiety
- wymuszać logowanie użytkownika stacji roboczej
- filtrować pakiety wchodzące/wychodzące do/z stacji roboczej**
- chronić centralny serwer sieci LAN przed nieuprawnionymi działaniami

**(WARTO SPRAWDZIĆ**

**AF** (zapora aplikacyjna) to rozwinięcie tradycyjnych zapór sieciowych o mechanizmy rozpoznawania aplikacji (poprzez dekodowanie pakietów w warstwie 7) i kontroli dostępu użytkowników do konkretnych aplikacji.

**WAF** (ang. *Web Application Firewall*) to w zasadzie specjalizowany do analizy aplikacji webowych IPS. Wymagania, które powinna spełniać zapora sieciowa typu WAF, są sformułowane w:

*Payment Card Industry Data Security Standard – PCI DSS – (sekcje 6.5.i 6.6).*

)

**58. Protokoły dostarczające mechanizmów uwierzytelniania**

Odp. TACACS, RADIUS, IPSec

**59. Jeśli wyślemy sygnał na port 80 sprawdzający czy jest otwarty i odpowiedź dostaniemy z flagą RST to znaczy, że port jest:**

Odpowiedź: port jest zamknięty, powtarzam port jest zamknięty do chuja

**60. Które z poniższych przedsięwzięć są podstawą skutecznej ochrony informacji?**

- a) Przygotowanie planów ciągłości działania.
- b) Nadzór kontrole i szkolenia.
- c) Redundancje sprzętowe i architektury bez pojedynczego punktu awarii.
- d) Wszystkie wymienione powyżej.**

**61. Który z poniższych sposobów gwarantuje bezpieczny i niezakłócony przekaz informacji niejawnej od nadawcy do odbiorcy?**

- a) Zaszyfrowanie treści przekazu kluczem publicznym odbiorcy i podpisanie kluczem prywatnym nadawcy.
- b) Zaszyfrowanie treści przekazu kluczem publicznym odbiorcy | podpisanie, czyli zazwyczaj zaszyfrowanie skrótu kluczem prywatnym nadawcy.**

- c) Zaszyfrowanie treści przekazu kluczem prywatnym nadawcy i podpisanie kluczem publicznym nadawcy.
- d) Zaszyfrowanie treści przekazu i skrótu kluczem prywatnym nadawcy i podpisanie kluczem prywatnym nadawcy.

**62. Które z poniższych przedsięwzięć decyduje o skuteczności zarządzania tożsamością jako najbardziej efektywnej metody autoryzacji?**

- a) Analiza ról pracowników, na każdym szczeblu organizacji i nadaniu roliom (wirtualnym użytkownikom) uprawnień do działania w systemie i uprawnień do aplikacji.
- b) Połączone z SSO (Single Sign-On) przypisanie użytkowników do ról (wirtualnych użytkowników).
- c) Wszystkie z powyższych.
- d) Żadne z powyższych

**63. Które z poniższych działań powinna wykonać organizacja w ramach ustanowienia SZBI?**

- a) Zdefiniować zakres, granice i politykę SZBI oraz podejście do szacowania ryzyka,
- b) Zidentyfikować aktywa informacyjne, zagrożenia i podatności,
- c) Określić, analizować i oceniać ryzyka,
- d) Wszystkie wyżej wymienione.

**64. W którym z poniższych dokumentów SZBI można ewentualnie umieścić zapisy wyłączające stosowanie zabezpieczeń?**

- a) Politykach SZBI,
- b) Planach Ciągłości Działania,
- c) Planach Postępowania z Ryzykiem,
- d) Deklaracji Stosowania Zabezpieczeń.

**65. Dyrektywa Parlamentu Europejskiego i Rady UE znana pod nazwą RODO, dotyczy:**

- a) środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE,
- b) systemu zarządzania bezpieczeństwem informacji (SZBI),

- c) sposobów archiwizowania informacji,
- d) ochrony danych osobowych.**

**66. Co możemy minimalizować stosując zabezpieczenia?**

- a) Zagrożenia.
- b) Podatności.**
- c) Obydwa z powyższych.
- d) Żadne z powyższych.

**67. Które z poniższych przedsięwzięć decydują o maksymalnej skuteczności planów ciągłości działania?**

- a) Spisanie PCD w formie procedur i szkolenie z nich personelu.
- b) Regularne testy działania PCD i dokumentowanie ich wyników.
- c) Wszystkie wymienione powyżej.**
- d) Żadne z wymienionych powyżej.

**68. Stosowanie (w razie konieczności) planów ciągłości działania ma celu zminimalizowanie:**

- a) zagrożenia,
- b) strat powstałych na skutek realizacji zagrożenia,**
- c) podatności,
- d) czasu realizacji audytu teleinformatycznego

**69. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które są niezbędne do realizacji zadań służbowych nazywa się:**

- a) zasadą wiedzy koniecznej,**
- b) zasadą minimalnego środowiska pracy,
- c) zasadą rotacji obowiązków,
- d) zasadą dwóch osób.

**70. Kopia bezpieczeństwa, na której zapisuje się dane zmienione od ostatniego kopiowania pełnego to kopia:**

- a) różnicowa,**
- b) przyrostowa,
- c) pełna,

- d) Tygodniowa.

**71. Przez co określane jest ryzyko?**

- a) Szkody, które mogą powstać podczas realizacji zagrożenia.
- b) Prawdopodobieństwo realizacji zagrożenia.
- c) Obydwa z powyższych.
- d) Żadne z powyższych.

**72. Który z rodzajów audytu SZBI jest audytem wewnętrzny?**

- a) Audyt strony pierwszej.
- b) Audyt strony drugiej.
- c) Audyt strony trzeciej.
- d) Wszystkie wymienione powyżej.

**73. Co jest podstawą sukcesu wszelkich procesów biznesowych i projektowych, w tym dotyczących SZBI?**

- a) Analiza ryzyka.
- b) Ocena ryzyka.
- c) Opracowanie zasad postępowania z ryzykiem.
- d) Wszystkie wymienione powyżej.

**74. Które z poniższych atrybutów informacji podlegają ochronie?**

- a) Tajność.
- b) Integralność.
- c) Dostępność.
- d) Wszystkie wymienione powyżej.

**75. Co może być przyczyną utraty tajności, integralności i dostępności informacji i stanowić podstawowe klasy zagrożeń?**

- a) Siły wyższe.
- b) Nieuprawnione i przestępctwa działania ludzi.
- c) Błędy ludzi i błędy w organizacji przetwarzania, przesyłania i przechowywania informacji.

d) Awarie sprzętu i błędy w oprogramowaniu.

e) Wszystkie wymienione powyżej.

**POZDRAWIAM WSZYSTKICH UCZĄCYCH SIĘ**  
!!!!!! pozdro

**dziena byczku nie usuwaj tego!**

**kmwtw**

**9. Inspektora bezpieczeństwa teleinformatycznego wyznacza się, zgodnie z odpowiednią ustawą w przypadku przetwarzania w systemach teleinformatycznych.**

**10. Informacja, której zmanipulowanie, udostępnienie lub ujawnienie może wyrządzić szkody firmie lub osobie prywatnej to informacja:**

Pytanie 9 Nie udzielono odpowiedzi Punkty: 1,00 Offlaguj pytanie	Inspektora bezpieczeństwa teleinformatycznego wyznacza się, zgodnie z odpowiednią ustawą, w przypadku przetwarzania w systemach teleinformatycznych:  Wybierz jedną odpowiedź: <input type="radio"/> a. danych bankowych <input type="radio"/> b. informacji wrażliwych <input checked="" type="radio"/> c. danych osobowych <input type="radio"/> d. informacji niejawnych  <a href="#">Odnacz moj wybór</a>
Pytanie 10 Odpowiedzi zaakceptowano Punkty: 1,00 Offlaguj pytanie	Informacja, której zmanipulowanie, udostępnienie lub ujawnienie może wyrządzić szkody firmie lub osobie prywatnej to informacja:  Wybierz jedną odpowiedź: <input checked="" type="radio"/> a. wrażliwa <input type="radio"/> b. publiczna <input type="radio"/> c. niejawna <input type="radio"/> d. podatna  <a href="#">Odnacz moj wybór</a>

**1. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:**

**2. Czy dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym:**

Pytanie 1 Nie udzielono odpowiedzi Punkty: 1,00 Offlaguj pytanie	<p><b>Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:</b></p> Wybierz jedną odpowiedź: <input checked="" type="radio"/> a. zasadą wiedzy koniecznej <input type="radio"/> b. zasadą dwóch osób <input type="radio"/> c. zasadą rotacji obowiązków <input type="radio"/> d. zasadą minimalnego środowiska pracy  <a href="#">Odnacz moj wybór</a>
Pytanie 2 Nie udzielono odpowiedzi Punkty: 1,00 Offlaguj pytanie	<p><b>Czy dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym:</b></p> Wybierz jedną odpowiedź: <input checked="" type="radio"/> a. TAK, chyba że przepisy odrębne stanowią inaczej <input type="radio"/> b. NIE  <a href="#">Odnacz moj wybór</a>

01-20 11-46-55

## 7. Parametr Recovery Time Actual (RTA) określa:

### 8. Podmiot świadczący usługi kolokacji:

Pytanie 7  
Odpowiedź zapisana  
Punkty: 1,00  
▼ Oflaguj pytanie

#### Parametr Recovery Time Actual (RTA) określa:

Wybierz jedną odpowiedź:

- a. „akceptowalne straty w danych” (aktualność danych odtworzonych po katastrofie) mierzone czasem od ostatniej kopii zapasowej do chwili katastrofy · RPO - Recovery Point Objective - max czas przez który może ponosić straty
- b. wymaganą długość przerwy w przetwarzaniu danych, niezbędną do wykonania kopi zapasowej
- c. ustalany drogą eksperymentów czas przywrócenia działania systemu informatycznego i odtworzenia zbiorów danych · RTA - praktyczny czas wstawiania systemu
- d. maksymalny, możliwy do zaakceptowania przez kierownictwo organizacji, ze względu na ponoszone straty, czas pracy bez możliwości korzystania z usług całości lub części systemu informatycznego

Odnacz moj wybór

RTA <= RTO

RPO - Recovery Point Objective - max czas przez który może ponosić straty

RTA - Recovery Time Object - teoretyczny czas potrzebny na wstawianie systemu po awarii (nie rzeczywisty nie potwierdzony)

Pytanie 8  
Odpowiedź zapisana  
Punkty: 1,00  
▼ Oflaguj pytanie

#### Podmiot świadczący usługi kolokacji:

Wybierz jedną odpowiedź:

- a. udostępnia swoje centrum danych (infrastrukturę), a klient wstawia tam swój sprzęt komputerowy
- b. udostępnia klientowi swoje centrum danych (infrastrukturę) i swój sprzęt komputerowy · hosting
- c. szkoli pracowników klienta z ochrony zasobów informacyjnych
- d. serwisuje sprzęt komputerowy w siedzibie klienta

Odnacz moj wybór

5. Założenia: kopia pełna jest wykonywana w każdy piątek o godz. 18:00; w dni robocze wykonywane są kopie różnicowe o godz. 18:00

6. Inspektora bezpieczeństwa teleinformatycznego wyznacza się, zgodnie z odpowiednią ustawą, w przypadku przetwarzania w systemach teleinformatycznych:

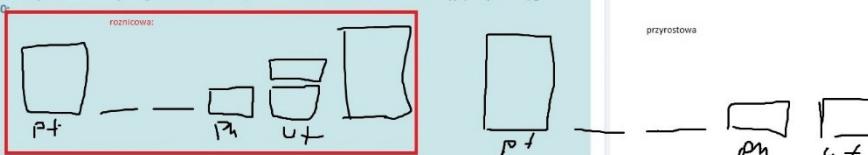
Pytanie 5  
Nie udzielono odpowiedzi  
Punkty: 1,00  
▼ Oflaguj pytanie

Założenia: kopia pełna jest wykonywana w każdy piątek o godz. 18:00; w dni robocze wykonywane są kopie różnicowe o godz. 18:00; każda kopia (także pełna) zajmuje jeden nośnik. Pytanie: nośniki z kopiami różnicowymi z jakich dni są niezbędne do odtworzenia zbiorów informacyjnych, jeżeli oryginalne zbiory zostały zniszczone w czwartek o 17:50:

Wybierz jedną odpowiedź:

- a. poniedziałek, wtorek, środa
- b. czwartek
- c. piątek, środa
- d. środa

Odnacz moj wybór



przyrostowa

Pytanie 6  
Nie udzielono odpowiedzi  
Punkty: 1,00  
▼ Oflaguj pytanie

Inspektora bezpieczeństwa teleinformatycznego wyznacza się, zgodnie z odpowiednią ustawą, w przypadku przetwarzania w systemach teleinformatycznych:

Wybierz jedną odpowiedź:

- a. informacji wrażliwych
- b. danych osobowych
- c. informacji niejawnych

danych bankowych

Odnacz moj wybór

01-20 11-46-55

5. Kopiowanie(w celu wytworzenia kopii bezpieczeństwa), w którym w wybranym dniu tygodnia zapisujemy komplet danych, natomiast w pozostałe dni robocze zapisujemy jedynie dane zmienione od ostatniego kopiowania nazywamy:

6. Terminem "hoax" określa się:

Pytanie 5  
Nowe pytanie do odpowiedzi  
Punkty: 100  
▼ Odpowiedz pytanie

Kopiowanie (w celu wytworzenia kopii bezpieczeństwa), w którym w wybranym dniu tygodnia zapisujemy komplet danych, natomiast w pozostałe dni robocze zapisujemy jedynie dane zmienione od ostatniego kopiowania **nazywamy**:

Wybierz jedną odpowiedź:

- a. pełnym
- b. lustrzanym
- c. przyrostowym
- d. różnicowym

[Oznacz moj wybór](#)

Pytanie 6  
Nowe pytanie do odpowiedzi  
Punkty: 100  
▼ Odpowiedz pytanie

Terminem „hoax” określa się:

Wybierz jedną odpowiedź:

- a. programowy obiekt złożływy przeprowadzający działania destrukcyjne w systemie
- b. sprzętowy obiekt złożływy posiadający zdolność powielania się
- c. atak odtoku socjotechnicznego – zarządzony pocztą elektroniczną
- d. programowy obiekt złożływy posiadający zdolność powielania się

[Oznacz moj wybór](#)

[Poprzednia strona](#) [Następna strona](#)

PREVIOUS ACTIVITY [◀ Ogłoszenia](#) Przejdz do... [▶](#)

7.Czy podatność jest warunkiem koniecznym realizacji zagrożenia:

8. Sandbox to:

Pytanie 7  
Odpowiedz zapisana  
Punkty: 100  
▼ Odpowiedz pytanie

Czy podatność jest warunkiem koniecznym realizacji zagrożenia:

Wybierz jedną odpowiedź:

- a. AK
- b. NIE

[Oznacz moj wybór](#)

Pytanie 8  
Odpowiedz zapisana  
Punkty: 100  
▼ Odpowiedz pytanie

Sandbox to:

Wybierz jedną odpowiedź:

- a. rodzaj testu penetracyjnego wykonywany z zewnątrz, bez znajomości struktury oraz konfiguracji testowanego środowiska
- b. metoda poruszanego analizowanego obiektu z baza sygnatur wirusów
- c. mechanizm służący do separacji programów oraz wykonywania niezaufanego kodu w odizolowanym środowisku
- d. skaner portów

[Oznacz moj wybór](#)

[Poprzednia strona](#) [Następna strona](#)

PREVIOUS ACTIVITY [◀ Ogłoszenia](#) Przejdz do... [▶](#)

3. Do uwierzytelniania danych stosuje się:

4. UTM (Unified Threat Management) oznacza:

Pytanie 3

Odpowiedź zapisana

Punkty: 1,00

▼ Oflaguj pytanie

Do uwierzytelniania danych **stosuje się**:

Wybierz jedną odpowiedź:

- a. tokeny
- b. sumy kontrolne i podpisy cyfrowe
- c. hasła
- d. metody biometryczne

[Odnacz mój wybór](#)

Pytanie 4

Odpowiedź zapisana

Punkty: 1,00

▼ Oflaguj pytanie

UTM (*Unified Threat Management*) oznacza:

Wybierz jedną odpowiedź:

- a. zespół zarządzający w firmie bezpieczeństwem teleinformatycznym
- b. integrację oprogramowania zabezpieczającego w jeden kompleksowy system ochrony, osadzany na specjalizowanej platformie sprzętowej
- c. metodę analizy ryzyka na potrzeby bezpieczeństwa informacyjnego
- d. metodę szyfrowania danych uwierzytelniających

[Odnacz mój wybór](#)

9. Dokument „Plan bezpieczeństwa informacyjnego dla ...” powinien być dokumentem:

10. Incydent z zakresu bezpieczeństwa informacyjnego to:

Pytanie 9

Ważne

Punkty: 1,00

▼ Oflaguj pytanie

„Plan bezpieczeństwa informacyjnego dla ....” powinien być dokumentem:

Wybierz jedną odpowiedź:

- a. jawnym
- b. dostępnym zgodnie zasadą wiedzy koniecznej
- c. poufnym (w rozumieniu ustawy o ochronie informacji niejawnych)
- d. do użytku wewnętrznego

[Odnacz mój wybór](#)

Pytanie 10

Odpowiedź zapisana

Punkty: 1,00

▼ Oflaguj pytanie

Incydent z zakresu bezpieczeństwa informacyjnego to:

Wybierz jedną odpowiedź:

- a. stan systemu informacyjnego, który powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji
- b. proces ujawniania podatności w systemie informacyjnym
- c. zdarzenie lub ciąg zdarzeń (składających się na realizację zagrożenia) które powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji
- d. zawsze i tylko rezultat działania cyberprzestępcy

5. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa

6. Produkty klasy SIEM służą do:

Pytanie 5

Odpowiedź zapisana

Punkty: 1,00

Oflaguj pytanie

Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:

Wybierz jedną odpowiedź:

- a. zasadą minimalnego środowiska pracy
- b. zasadą wiedzy koniecznej
- c. zasadą dwóch osób
- d. zasadą rotacji obowiązków

Odnacz mój wybór

Pytanie 6

Odpowiedź zapisana

Punkty: 1,00

Oflaguj pytanie

Produkty klasy SIEM służą do:

Wybierz jedną odpowiedź:

- a. korelowania wyników działania różnych narzędzi z zakresu bezpieczeństwa (IPS, WAF, itd.) oraz automatyzacji prezentacji wybranych zdarzeń i reakcji na te zdarzenia
- b. nadzorowania obiegu informacji w systemie informatycznym i wspomagania przeciwdziałania jej wyciekowi
- c. analizy i korelacji informacji wieloźródłowej o zdarzeniach zachodzących w systemie informatycznym i przedstawiania w czasie zbliżonym do rzeczywistego spójnego, kompleksowego obrazu stanu tego systemu
- d. kontroli tożsamości użytkowników systemu informatycznego

Odnacz mój wybór

Korzystanie z systemu ochrony fizycznej i technicznej obiektów, w ramach metod postępowania z ryzykiem należy do:

Ustalany eksperymentalnie czas przywrócenia działania systemu informatycznego i odtworzenia zbiorów danych określa parametr:

Ustalanie z systemu ochrony fizycznej i technicznej obiektów, w ramach metod postępowania z ryzykiem, dotyczy do:

Wybierz jedną odpowiedź:

- a. retencji ryzyka
- b. unikania ryzyka
- c. kontrolowania ryzyka
- d. transferu ryzyka

Odnacz mój wybór

Ustalany eksperymentalnie czas przywrócenia działania systemu informatycznego i odtworzenia zbiorów danych określa parametr:

Wybierz jedną odpowiedź:

- a. RPO
- b. RTA
- c. RTO

9. Podmiot świadczący usługi hostingu:

10. Zasada Defense-in-depth (obrona w głąb) oznacza, że:

=

**Pytanie 9**

Odpowiedź  
zapisana

Punkty: 1,00

¶ Oflaguj  
pytanie

**Podmiot świadczący usługi hostingu:**

Wybierz jedną odpowiedź:

- a. serwisiuje sprzęt komputerowy w siedzibie klienta
- b. administruje i przetwarza w swoim centrum komputerowym zasoby informacyjne powierzone przez klienta
- c. udostępnia klientowi swoje centrum danych i swój sprzęt komputerowy
- d. udostępnia swoje centrum danych, a klient wstawia tam swój sprzęt komputerowy

[Odznacz mój wybór](#)

**Pytanie 10**

Odpowiedź  
zapisana

Punkty: 1,00

¶ Oflaguj  
pytanie

**Zasada Defense-in-depth (obrona w głąb) oznacza, że:**

Wybierz jedną odpowiedź:

- a. zastosowano implementację zasad polityki bezpieczeństwa z uwzględnieniem ataków na warstwę aplikacyjną (zasada stosowana m.in. przez aplikacyjne zapory sieciowe)
- b. wykorzystano w obrębie jednego urządzenia sieciowego wiele funkcji zabezpieczeń dla różnych usług, np.: poczty elektronicznej, baz danych, serwerów FTP itp.
- c. po przełamaniu jednej warstwy zabezpieczeń zagrożenie natrafia na kolejną, z innymi zabezpieczeniami
- d. następuje zmniejszenie prawdopodobieństwa ukrycia źródła ataku poprzez wdrożenie systemu zabezpieczeń wewnętrz sieci LAN

[Odznacz mój wybór](#)

7. Termin “steganografia” oznacza:

8. Incydent z zakresu bezpieczeństwa informacyjnego to:

---

Pytanie 7

Odpowiedź zapisana

Punkty: 1,00

FLAGA  
pytanie

**Termin „steganografia” oznacza:**

Wybierz jedną odpowiedź:

- a. rysunki stegozaurów wykonywane na ścianach jaskiń przez człowieka pierwotnego
- b. metodę zapewniania integralności informacji
- c. metodę ukrywania informacji
- d. sposób weryfikacji tożsamości użytkownika systemu teleinformatycznego

[Odnacz mój wybór](#)

Pytanie 8

Odpowiedź zapisana

Punkty: 1,00

FLAGA  
pytanie

**Incydent z zakresu bezpieczeństwa informacyjnego to:**

Wybierz jedną odpowiedź:

- a. zawsze i tylko rezultat działania cyberprzestępcy
- b. proces ujawniania podatności w systemie informacyjnym
- c. stan systemu informacyjnego, który powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji
- d. zdarzenie lub ciąg zdarzeń (składających się na realizację zagrożenia) które powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji

[Odnacz mój wybór](#)

5. Atak na system informacyjny i informację w nim przetwarzaną jest:

6. Dokument Polityka bezpieczeństwa informacyjnego powinien być dokumentem zawierającym:

**Pytanie 5**

Odpowiedź zapisana

Punkty: 1,00

Oflaguj pytanie

**Atak na system informacyjny i informację w nim przetwarzaną jest:**

Wybierz jedną odpowiedź:

- a. sposobem realizacji zagrożenia
- b. zagrożeniem
- c. elementem socjotechniki
- d. narzędziem intruza

[Odnacz mój wybór](#)

**Pytanie 6**

Odpowiedź zapisana

Punkty: 1,00

Oflaguj pytanie

**Dokument Polityka bezpieczeństwa informacyjnego powinien być dokumentem zawierającym:**

Wybierz jedną odpowiedź:

- a. zapis najważniejszych, ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnych i powierzonych informacji i jego deklaracje co do zapewniania odpowiedniego poziomu tego bezpieczeństwa
- b. wykaz stosowanych w organizacji podstawowych zabezpieczeń informacji
- c. instrukcje i procedury dla osób korzystających z systemów teleinformatycznych organizacji
- d. szczegółowe plany obiegu informacji i schematy sieci teleinformatycznych

[Odnacz mój wybór](#)

3. Poprawna treść Zasady Kerckhoffsa to:

4. Promieniowanie ujawniające:

**Pytanie 3**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

Poprawna treść **Zasady Kerckhoffsa** to:

Wybierz jedną odpowiedź:

- a. Odporność kryptosystemu powinna zależeć od utrzymania tajności klucza wybierającego konkretne przekształcenie, a nie od tajności przekształceń używanych w tym kryptosystemie
- b. Odporność kryptosystemu powinna zależeć od utrzymania tajności przekształceń używanych w tym kryptosystemie, a nie od tajności klucza wybierającego konkretne przekształcenie

Odnacz mój wybór

**Pytanie 4**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

**Promieniowanie ujawniające:**

Wybierz jedną odpowiedź:

- a. jest promieniowaniem elektromagnetycznym stanowiącym zagrożenie dla tajności informacji przetwarzanej w systemie komputerowym
- b. jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla tajności informacji przetwarzanej w systemie komputerowym
- c. jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla tajności i integralności informacji przetwarzanej w systemie komputerowym
- d. nie stanowi żadnego zagrożenia

Odnacz mój wybór

**1.Do uwierzytelniania danych stosuje się:**

**2.Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informacyjnych obejmuje:**

**Pytanie 1**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

**Do uwierzytelniania danych **stosuje się**:**

Wybierz jedną odpowiedź:

- a. hasła
- b. sumy kontrolne i podpisy cyfrowe
- c. metody biometryczne
- d. tokeny

[Odnacz mój wybór](#)

**Pytanie 2**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

**Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informacyjnych obejmuje:**

Wybierz jedną odpowiedź:

- a. dywersifikację i niesprzecznośc zastosowanych zabezpieczeń
- b. dywersifikację i spójność zastosowanych zabezpieczeń
- c. dywersifikację oraz spójność zastosowanych zabezpieczeń i organizację ochrony "w głęb"
- d. dywersifikację, spójność, niesprzecznośc zastosowanych zabezpieczeń i organizację ochrony "w głęb"

[Odnacz mój wybór](#)

**1.Czy dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi**

**2. Para(Poziom atrybutu, kategoria informacji) wyznacza klasę:**

**Pytanie 1**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

**Czy dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym:**

Wybierz jedną odpowiedź:

- a. NIE
- b. TAK, chyba że przepisy odrębne stanowią inaczej

[Odnacz mój wybór](#)

**Pytanie 2**

Nie udzielono odpowiedzi

Punkty: 1,00

Oflaguj pytanie

**7. Para (poziom atrybutu, kategoria informacji) wyznacza klasę:**

Wybierz jedną odpowiedź:

- a. bezpieczeństwa
- b. sterowania dostępem
- c. uwierzytelniania
- d. autoryzacji

[Odnacz mój wybór](#)

Atak na system informacyjny i informację w nim przetwarzaną jest:  
Zgodnie z ustawą z dn. 05.08.2010 „O ochronie informacji niejawnych” informację niejawą oznacza się klauzulą:

Atak na system informacyjny i informację w nim przetwarzaną jest:

Wybierz jedną odpowiedź:

a. zagrożeniem

b. sposobem realizacji zagrożenia

c. elementem socjotechniki

d. narzędziem intrusa

Odnacz mój wybór

Zgodnie ustawą z dn. 05.08.2010 „O ochronie informacji niejawnych” informację niejawą oznacza się klauzulą:

Wybierz jedną odpowiedź:

a. „ściśle tajne” lub „tajne” lub „poufne” lub „zastrzeżone”

b. „ściśle tajne” lub „tajne” lub „poufne”

c. „tajne” lub „poufne” lub „zastrzeżone”

d. „ściśle tajne” lub „tajne” lub „poufne” lub „do użytku wewnętrznego”

Odnacz mój wybór

Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informacyjnych obejmuje:  
Test penetracyjny to:

Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informacyjnych obejmuje:

Wybierz jedną odpowiedź:

a. dywersyfikację i spójność zastosowanych zabezpieczeń

b. dywersyfikację i niesprzecznośc zastosowanych zabezpieczeń

c. dywersyfikację, spójność, niesprzecznośc zastosowanych zabezpieczeń i organizację ochrony „w głębi”

d. dywersyfikację oraz spójność zastosowanych zabezpieczeń i organizację ochrony w „w głębi”

Odnacz mój wybór

Test penetracyjny to:

Wybierz jedną odpowiedź:

a. metoda oddziaływanie socjotechnicznego

b. metoda zbierania informacji o badanym systemie

c. to samo, co audyt bezpieczeństwa informacyjnego

d. metoda włamywania się do systemu informatycznego

Odnacz mój wybór

Zgodnie z ustawą z dn. 05.08.2010 „O ochronie informacji niejawnych” informację niejawą oznacza się klauzulą:  
Incydent z zakresu bezpieczeństwa informacyjnego to:

**Zgodnie ustawą z dn. 05.08.2010 „O ochronie informacji niejawnych” informację niejawą oznacza się klauzulą:**

Wybierz jedną odpowiedź:

- a. „tajne” lub „poufne” lub „zastrzeżone”
- b. „ścisłe tajne” lub „tajne” lub „poufne” lub „do użytku wewnętrznego”
- c. „ścisłe tajne” lub „tajne” lub „poufne” lub „zastrzeżone”
- d. „ścisłe tajne” lub „tajne” lub „poufne”

Odnacz mój wybór

**Incydent z zakresu bezpieczeństwa informacyjnego to:**

Wybierz jedną odpowiedź:

- a. stan systemu informacyjnego, który powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji
- b. zdarzenie lub ciąg zdarzeń (składających się na realizację zagrożenia) które powoduje lub może spowodować niepożdaną zmianę wartości istotnych kryteriów jakości informacji
- c. zawsze i tylko rezultat działania cyberprzestępcy
- d. proces ujawniania podatności w systemie informacyjnym

Odnacz mój wybór

Norma PN-ISO/IEC – 15408 dotyczy:  
Podpis cyfrowy ma za zadanie zapewnić:

Norma PN-ISO/IEC-15408 dotyczy:

Wybierz jedną odpowiedź:

- a. sposobów archiwizowania informacji
- b. klas metod kryptograficznych
- c. konstrukcji i oceny „bezpiecznych” produktów informatycznych
- d. systemu zarządzania bezpieczeństwem informacji

Odnacz mój wybór

Podpis cyfrowy ma za zadanie zapewnić:

Wybierz jedną odpowiedź:

- a. tylko integralność informacji
- b. tylko poufność i autentyczność informacji
- c. dostępność informacji
- d. niezaprzecalność, autentyczność, integralność informacji

Odnacz mój wybór

---

Podstawowe atrybuty informacji związane z jej bezpieczeństwem to:  
Dokument Polityka bezpieczeństwa informacyjnego powinien być dokumentem zawierającym:

---

Podstawowe atrybuty informacji związane z jej bezpieczeństwem to:

Wybierz jedną odpowiedź:

- a. tajność, integralność, dostępność
- b. integralność, metoda szyfrowania, dostępność
- c. tajność, integralność, długość (w bajtach)
- d. tajność, integralność, długość (w znakach)

Odnacz mój wybór

Dokument Polityka bezpieczeństwa informacyjnego powinien być dokumentem zawierającym:

Wybierz jedną odpowiedź:

- a. szczegółowe plany obiegu informacji i schematy sieci teleinformatycznych
- b. zapis najważniejszych, ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnych i powierzonych informacji i jego deklaracje co do zapewniania odpowiedniego poziomu tego bezpieczeństwa
- c. instrukcje i procedury dla osób korzystających z systemów teleinformatycznych organizacji
- d. wykaz stosowanych w organizacji podstawowych zabezpieczeń informacji

Odnacz mój wybór

---

Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego, gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku, nazywa się:

Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:

Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego, gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku, nazywa się:

Wybierz jedną odpowiedź:

- a. weryfikację uwierzytelnienia
- b. weryfikację autoryzacji
- c. weryfikację poziomu ochrony
- d. weryfikację tożsamości

[Odnacz mój wybór](#)

Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków, nazywa się:

Wybierz jedną odpowiedź:

- a. zasadą dwóch osób
- b. zasadą rotacji obowiązków
- c. zasadą minimalnego środowiska pracy
- d. zasadą wiedzy koniecznej

[Odnacz mój wybór](#)

## **1. Podstawowe atrybuty informacji związane z bezpieczeństwem**

### **- tajność, integralność, dostępność**

- tajność integralność długość (w znakach)
- tajność integralność długość (w bajtach)
- integralność, metoda szyfrowania, dostępność

## **2. Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym**

### **- zapis najważniejszych ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa**

- wykaz stosowanych podstawowych zabezpieczeń informacji
- instrukcje i procedury dla osób korzystających z systemów teleinformatycznych
- szczegółowy plan obiegu informacji i schematu sieci telefonicznych

## **3. Zgodnie z ustawą o ochronie informacji niejawnych informacje nie jawne oznacza się klauzulą**

### **- ścisłe tajne lub tajne lub poufne lub zastrzeżone**

- ścisłe tajna lub tajne
- poufne lub zastrzeżone
- jawne

## **4. Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku nazywa się**

- weryfikacja tożsamości
- **weryfikacja autoryzacji**
- weryfikacja poziomu ochrony
- weryfikacja uwierzytelniania

## **5. Norma 27001 dotyczy**

- klas metod kryptograficznych
- konstrukcji bezpiecznych produktów informatycznych
- sposobów archiwizowania informacji
- **systemów zarządzania bezpieczeństwem informacji**

## **6. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i takie informacje, które wynikają z jego obowiązków nazywa się**

- zasada minimalnego środowiska pracy
- zasada rotacji obowiązków
- zasada dwugłosu

### **- zasada wiedzy koniecznej**

## **7. Za pomocą VPN nie da się zabezpieczyć**

### **- dostępności**

- integralności
- czytelności

## **8. Test penetracyjny to**

- to samo co audyt bezpieczeństwa informacyjnego
- **metoda zbierania informacji o badanym systemie**
- metoda włamywania się do systemu informatycznego
- to samo co atak socjotechniczny

## **9. Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informatycznych obejmuje**

- dywersyfikacja i spójność
- dywersyfikacja, niezaprzeczalność i organizacja wg zasady ochrony "w głab"
- **dywersyfikacja, niezaprzeczalność, spójność i organizacja wg zasady ochrony "w głęb"**

- dywersyfikacja i organizacja wg zasady ochrony "w głąb"

**10. Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową jest równoważne, co do skutków prawnych, użyciu bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem?**

- tak

- nie

**11. Postępowanie i wdrożenie planów zapewniania ciągłości działania w ramach metod postępowania z ryzykiem to**

- retencji ryzyka

- transferu ryzyka

- unikania ryzyka

- **kontrolowania ryzyka**

**12. Podstawowe metody realizacji operacji uwierzytelniania tożsamości użytkownika to:**

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja wiedzy użytkownika, weryfikacja jego uprawnień systemowych

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja komputera z którego loguje się użytkownik

- **weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja wiedzy użytkownika**

**13. Audyt w zakresie bezpieczeństwa informacyjnego**

- wykonuje się przy okazji sporządzania spisu zasobów informacyjnych

- jest tym samym co test penetracyjny

**- wymaga tzw. wzorca audytowego i niezależności podmiotu wykonującego audit**

- polega na sprawdzeniu logów systemowych przez administratora systemu teleinformatycznego

**14. Promieniowanie ujawniające**

- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności i integralności informacji przetwarzanych w systemie komputerowym

- jest promieniowaniem elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanych w systemie komputerowym

**- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanej w systemie komputerowym**

- nie stanowi zagrożenia

**15. Czy obowiązujący w Polsce Kodeks Karny przewiduje sankcje za nieuprawnione, szkodliwe działanie wobec systemu komputerowego i informacji w nich przetwarzanej?**

- tak

- nie

**16. Dokument „Polityka bezpieczeństwa teleinformatycznego dla...” powinien być dokumentem**

- do użytku wewnętrznego

**- jawny**

- nie ma znaczenia

- poufnny

**17. Podpis cyfrowy ma za zadanie zapewnić**

**- niezaprzeczalność, autentyczność i integralność informacji**

**18. Outsourcing**

- transfer ryzyka

**19. Czym jest steganografia**

- utajnianie informacji

**20. RTA (Real Time Actual)**

- Ile czasu schodzi na przywrócenie systemu po awarii

**21. Backup taki ze zapisuje raz pełny a potem tylko to co doszło od ostatniego pełnego**

roznicy

**22. UTM**

**Unified Threat Management - kompleksowy system ochrony wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia**

**23. Ochrona danych osobowych**

tylko dla żyjących

**24. Zasada ochrony w głab**

jak przedostanie się przez zapory to napotyka druga

**25. Ubezpieczenie zalicza się do**

- transferu ryzyka

**26. Co to jest SNORT**

- IDS/IPS... -> Jest to oprogramowanie mające za zadanie identyfikację potencjalnych ataków na sieć lub konkretny komputer (intrusiondetection), powiadamianie o nich oraz ich blokadę (intrusionresponse) np. poprzez dynamiczne przekonfigurowanie reguł współpracującej zapory sieciowej

**27. W którym dokumencie opisano System Zarządzania**

**Bezpieczeństwem Informacji**

- ISO 27001

**28. Zasada, żeby pracownik, do wykonywania pracy, miał tylko dostęp do tych programów i usług, których potrzebuje to**

- zasada minimalnego środowiska pracy

**29. Usługa kolokacji**

- udostępnienie miejsca, własny sprzęt

**30. Co to jest hoax?**

- atak socjotechniczny

**31. Co to jest SandBox?**

**Sandbox (wiki)** – rodzaj piaskownicy, w której wydzielona została część systemu informatycznego przeznaczona, ze względów bezpieczeństwa, do odseparowanego uruchamiania programów, które są nieprzetestowane lub niezaufane lub pochodzą od niezaufanych stron trzecich.

Zwykle jest to ścisłe nadzorowany zestaw zasobów systemu utworzonych w obszarach roboczych pamięci operacyjnej oraz masowej. Uruchamiane w nich programy najczęściej albo nie mają praw na dostęp sieciowy, inspekcję systemu gospodarza i czytanie z urządzeń wejściowych, albo mają je mocno ograniczone. Z tego względu piaskownicę można traktować jako specyficzny przypadek wirtualizacji.

**32. Co to jest Recovery Point Object?**

Dopuszczalny przez organizację czas przywracania systemu

**33. Na czym polega hosting?**

Udostępnianie centrum danych (miejsca) i sprzętu.

**34. Na czym polega personal firewall?**

Filtracja pakietów

**35. Zasada Kerckhoffsa**

System kryptograficzny powinien być bezpieczny nawet wtedy, gdy wszystkie szczegóły jego działania oprócz klucza są znane.

**36. Miara bezpieczeństwa w common criteria**

- jest to poziom uzasadnionego zaufania.

**37. Na czym bazuje autoryzacja dostępu na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.**

**38. Jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa**

**niejawny, dokument do użytku wewnętrznego**

**39. jakie klauzule odpowiadają tajemnicy służbowej  
Poufne, zastrzeżone**

**40. Co nie jest plikiem systemowym NTFS**

\$Sector.

**41. Co się dzieje z plikiem po usunięciu z dysku:**

wpis w \$MFT jest usuwany, dane zostają

**wpis w \$MFT zostaje, dane zostają i zmieniają się dwie flagi**

wpis w \$MFT jest usuwany, dane są usuwane

wpis w \$MFT zostaje, dane zostają

**42. Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania:**

**- minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia**

**43. W których Windowsach domyślnie włączony jest dziennik zdarzeń?**

Odp.: Vista i Windows 7. ok

**44. W którym Windowsie było logowanie zdarzeń?**

Odp.: (Podobno) od 2000 w górę (ME chyba nie bo to jeszcze nie było jądro NT tylko podkolorowane 98) czyli 2000, XP, 2003, 2008, Vista, 7 itd. ok

**45. Ile jest well-known portów?**

Odp.: 1024.

**46. Coś tam o audycie bezpieczeństwa teleinformatycznego:**

Odp.: Zawiera się w audycie informatycznym (jest podzbiorem audytu informatycznego coś takiego).

**47. W Windows XP dzienniki są:**

Odp.: Aplikacji, zabezpieczeń, system (domyślnie wyłączone). ok

**48. Co jest wyposażeniem teleinformatycznym wg PN-EN ISO/IEC 17025:**

Odp.: Nie pamiętam dokładnie, ale najdłuższa odpowiedź (A) w której było oprogramowanie, urządzenia i jeszcze kilka innych rzeczy.

**49. Plan bezpieczeństwa powinien być:**

Odp.: Dostępny zgodnie z zasadą wiedzy koniecznej.

**50. Pytanie o Web Application Firewall**

51. Island hopping

- atakowanie najsłabszego systemu i skakanie na inne

**52. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwową**

- tajność , ścisła tajność

**53. Jaki powinien być dokument "Planowania bezpieczeństwa dla ..."**

- powinien być jawnym.

54. Wymagania na system zarządzania bezpieczeństwa informacji (SZBI) są opisane w normie:

- PN - ISO/IEC - 27001

55. czy w polskim prawie karnym jest paragraf na włamania (?)

**-tak**

56. Cechy podpisu elektronicznego

**- Integralność, Autentyczność, Niezaprzecjalność (Skrypt 124)**

57. Jaka norma jest od Systemu zarządzania bezpieczeństwem?

**- norma ISO27001**

58. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego

- różnica jest taka że pełny audit jest nadzorem auditu bezpieczeństwa.

59. Czym rozni się audit informatyczny od audytu bezpieczeństwa?

- Audit bezpieczeństwa zawiera się w audycie informatycznym.

60. kolejność wykonywania exploita

- : mfsconsole->mfsupdate->use exploit<nazwa>->RHOST<ip ofiary>->LHOST<ip intrusa>->exploit

61. na czym polega weryfikacja tożsamości użytkownika?

- Weryfikacja cech fizycznych użytkownika; Weryfikacja przedmiotu posiadanego przez użytkownika; Weryfikacja wiedzy użytkownika;

62. Co robi forward proxy?

-maskuje klienta przed serwerem

63. Czy zgodnie z prawem Kirchoffa?

-nie

64. Zabezpieczenie przedmiotów I danych to:

-kontrolowanie ryzyka

65. Backup całosciowy jest robiony w każdy piątek o 18. Backupy różnicowe robione są w pozostałe powszednie dni o 18. Które backup różnicowe są potrzebne aby odzyskać dane utracone w czwartek o 17:50?

-środa

66.Jaki jest parametr przywrócenia działania systemu I danych?

-rta

1. Podstawowe atrybuty informacji związane z bezpieczeństwem

- tajność, integralność, dostępność

- tajność integralność długość (w znakach)

- tajność integralność długość (w bajtach)

- integralność, metoda szyfrowania, dostępność

2. Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym

- zapis najważniejszych ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa

- wykaz stosowanych podstawowych zabezpieczeń informacji

- instrukcje i procedury dla osób korzystających z systemów teleinformatycznych

- szczegółowy plan obiegu informacji i schematu sieci telefonicznych

3. Zgodnie z ustawą o ochronie informacji niejawnych informacje nie jawne oznacza się klauzulą

- ścisłe tajne lub tajne lub poufne lub zastrzeżone

- ścisłe tajna lub tajne

- poufne lub zastrzeżone

- jawne

4. Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku nazywa się

- weryfikacja tożsamości

- weryfikacja autoryzacji

- weryfikacja poziomu ochrony

- weryfikacja uwierzytelniania

5. Norma 27001 dotyczy

- klas metod kryptograficznych

- konstrukcji bezpiecznych produktów informatycznych

- sposobów archiwizowania informacji

- systemów zarządzania bezpieczeństwem informacji

6. Podpis cyfrowy ma za zadanie zapewnić

- nieprzeliczalność autentyczność integralność informacji

7. Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i takie informacje, które wynikają z jego obowiązków nazywa się

- zasada minimalnego środowiska pracy

- zasada rotacji obowiązków

- zasada dwugłosu

- zasada wiedzy koniecznej

8. Za pomocą VPN nie da się zabezpieczyć

- dostępności

- integralności

- czytelności

9. Test penetracyjny to

- to samo co audyt bezpieczeństwa informacyjnego

- metoda zbierania informacji o badanym systemie

- metoda włamywania się do systemu informatycznego

- to samo co atak socjotechniczny

10. Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informatycznych obejmuje

- dywersyfikacja i spójność

- dywersyfikacja, niezaprzeczalność i organizacja wg zasady ochrony w głab

- dywersyfikacja, niezaprzeczalność, spójność i organizacja wg zasady ochrony w głab

- dywersyfikacja i organizacja wg zasady ochrony w głab

1. Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową jest równoważne, co do skutków prawnych, użyciu bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem?

- tak

- nie

2. Postępowanie i wdrożenie planów zapewniania ciągłości działania w ramach metod postępowania z ryzykiem to:

- retencji ryzyka

- transferu ryzyka

- unikania ryzyka

- kontrolowania ryzyka

3. Podstawowe atrybuty informacji związane z jej bezpieczeństwem to:

- tajność integralność długość (w znakach)

- tajność integralność długość (w bajtach)

- tajność integralność dostępność

- integralność, metoda szyfrowania, dostępność

4. Podstawowe metody realizacji operacji uwierzytelniania tożsamości użytkownika to:

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja wiedzy użytkownika, weryfikacja jego uprawnień systemowych

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja komputera z którego loguje się użytkownika

- weryfikacja przedmiotu posiadanego przez użytkownika, weryfikacja cech fizycznych użytkownika, weryfikacja wiedzy użytkownika

5. Audyt w zakresie bezpieczeństwa informacyjnego

- wykonuje się przy okazji sporządzania spisu zasobów informacyjnych

- jest tym samym co test penetracyjny

- wymaga tzw wzorca audytowego i niezależności podmiotu wykonującego audit

- polega na sprawdzeniu logów systemowych przez administratora systemu teleinformatycznego

6. Wymagania na system zarządzania bezpieczeństwem informacji (SZBI) są opisane w normie

- PN-ISO/IEC-9001

- PN-ISO/IEC-15408

- PN-ISO/IEC-27001

- nie są opisane w żadnej normie

7. Promieniowanie ujawniające

- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności i integralności informacji przetwarzanych w systemie komputerowym

- jest promieniowaniem elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanych w systemie komputerowym

- jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności informacji przetwarzanej w systemie komputerowym

- nie stanowi zagrożenia

8. Stosowanie określaniu praw dostępu do informacji zasada, że każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji, które wynikają z jego obowiązków nazywa się

- zasada wiedzy koniecznej

- zasada rotacji obowiązków

- zasada minimalnego środowiska pracy

- zasada dwóch osób

9. Czy obowiązuje w Polsce Kodeks Karny przewiduje sankcje za nieuprawnione, szkodliwe działanie wobec systemu komputerowego i informacji w nich przetwarzanej?

- tak

- nie

10. Dokument „Polityka bezpieczeństwa teleinformatycznego dla...” powinien być dokumentem

- do użytku wewnętrznego

- jawnym

- nie ma znaczenia

- poufnym

**Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową TAK**

Przygotowanie i wdrożenie planów zapewnienia ciągłości działania:

**Minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia.**

**Podstawowe atrybuty informacji związane z jej bezpieczeństwem to: Tajność, integralność, dostępność.**

**Podstawowe metody realizacji operacji uwierzytelniania tożsamości użytkownika to:**

**Weryfikacja przedmiotu, weryfikacja cech fizycznych, weryfikacja wiedzy.**

**Audyt w zakresie bezpieczeństwa informacyjnego: Wymaga wzorca audytowego i niezależnego wykonawcy.**

**Wymagania na system zarządzania bezpieczeństwem informacji (SZBI) są opisane w normie: ISO/IEC-27001.**

**Promieniowanie ujawniające: Promieniowanie elektromagnetyczne zagrażające poufności informacji w sieci.**

**Stosowana w określaniu praw dostępu do informacji zasada, że każdy pracownik ma ... Zasada wiedzy koniecznej.**

**Czy obowiązujący w Polsce Kodeks Karny przewiduje sankcje za nieuprawnione, szkodliwe działania wobec systemów komputerowych i informacji w nich przetwarzanych: TAK**

**UTM? co to/co robi (nie rozwinięcie skrótu)**

**Dokument „Polityka bezpieczeństwa teleinformatycznego dla..” powinien być dokumentem: Jawnym.**

**Ubezpieczenie zalicza się do: Transferu ryzyka.**

**Co to jest SNORT ? IDS/IPS... („prewencja przed intruzami”)**

**Atrybuty informacji: Tajność, integralność, dostępność.**

**W którym dokumencie opisano System Zarządzania Bezpieczeństwem Informacji? ISO 27001**

**Podpis cyfrowy zapewnia: Niezaprzeczalność, autentyczność, integralność.**

**Zasada, żeby pracownik, do wykonywania pracy, miał tylko dostęp do tych programów i usług, których potrzebuje to:**

**Zasada minimalnego środowiska pracy.**

**Co to jest RTA? Czas przywrócenia danych ( eksperimentalny ).**

**Minimalny zestaw wymagań na system zabezpieczeń:**

**Dyweryfikacja, niezaprzeczalność, spójność i organizacja wg zasady ochrony "w głąb".**

**Usługa kolokacji: Udostępnienie miejsca, własny sprzęt.**

**Co to jest hoax? Atak socjotechniczny**

**Ubezpieczenie zalicza się do: Transferu ryzyka.**

**Co to jest SandBox? Służy do izolacji /separacji programów. (Testowanie nieznanych?)**

**Co to jest Recovery Point Object? [ 'A' było, jedyna odpowiedź w cudzysłowie.]**

**Co to jest UTM? (Najdłuższa), cały system, wyspecjalizowany sprzęt**

**Na czym polega hosting? Udostępnione centrum danych i sprzętu.**

**Na czym polega personal firewall ? Filtracja pakietów.**

**Zapis plików, przez tydzień itp. Przyrostowe (jeżeli porównanie to różnicowe)**

**Co to jest steganografia? Metoda ukrywania informacji.**

**Chodziło o nazwę czegoś, jakiegoś procesu, który wykonuje się, kiedy użytkownik chce uzyskać dostęp do pliku.**

**Odpowiedź była z autoryzacją.**

**Outsourcing zaliczamy do: Transferu ryzyka.**

**Firewall co robi? Kontrola ruchu pakietów w sieci.**

**Zasada Kerchoffa: (odp. B , klucz jest tajny a nie shaker)**

**Zadanko ze od pon do cz o 18 jest backup niepełny a w piątek o 18 pełny i jak w czwartek o 17 50 sie zepsuje system to ile dysków potrzeba z backupem żeby odnowić system - jeden backup = jeden dysk**

**Za pomocą VPN nie da się zabezpieczyć: Dostępności.**

**Test penetracyjny to Metoda zbierania informacji o danym systemie.**

**Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku nazywa się: Weryfikacja autoryzacji.**

**Zgodnie z ustawą o ochronie informacji niejawnych informacje nie jawne oznacza się klauzulą:**

**Ścisłe tajne, tajne, poufne bądź zastrzeżone,**

**Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym:**

**Zapis najważniejszych ogólnych zamiarów działań kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa.**

**Minimalny zbiór cech skutecznego systemu ochrony informacji przetwarzanej w systemach informatycznych obejmuje**

**Dyweryfikacja, niezaprzeczalność, spójność i organizacja wg zasady ochrony w głąb**

**Coś tam o audycie bezpieczeństwa teleinformatycznego:**

**Zawiera się w audycie informatycznym (jest podziobrem audytu informatycznego)**

**Jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa? Niejawny - do użytku wewnętrznego.**

**Kogo dotyczy Ustawa o ochronie danych osobowych? Tylko żywych.**

**Co to jest RPO ? Był szacowany podczas analizy ryzyka - określa maksymalny, szacowany czas pracy możliwy do zaakceptowania przez kierownictwo organizacji**

**Miara bezpieczeństwa w common criteria (norma iso 15194 czy jakoś tak) Poziom uzasadnionego zaufania.**

**Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania: Minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia.**

**Jakie są klauzule tajemnicy państwownej? Tajność, ścisła tajność.**

**Management a kompleksowy system ochrony - Difens po przelamaniu 1 warstwy**

## Trochę info.

**Informacja** - Byt abstrakcyjny który zwiększa obszar wiedzy bądź zmniejsza obszar niewiedzy.

Przykład:

- dla piszącego kolokwium informacją nie jest – treść pytania, imię nazwisko osoby siedzącej obok, numer Sali w której piszemy kolokwium.
- dla ucznia szkoły pdst informacją jest – wzór na transmitancje Laplacea, przestrzeń Hilberta itp.

**Bezpieczeństwo informacji** - oznacza zachowanie poufności, integralności i dostępności informacji.

**integralność** - jest zdefiniowana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

**dostępność** - jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

**Jakie są skutki zawyżania klauzul tajności:**

Bezpieczeństwo przetwarzania danych (informacji) o zróżnicowanych klauzulach tajności - dane (informacje) o wyższej klauzuli tajności nie mogą „przepływać” do obiektów (aktywnych lub pasywnych) mających niższą klauzulę tajności. **Problem niedoceniany** - nadmierne koszty systemu bezpieczeństwa dla informacji o zawyżonych bez uzasadnienia klauzulach tajności barierą dla wzmacniania innych składników bezpieczeństwa informacyjnego(niegospodarne dysponowanie publicznymi środkami finansowymi)

**Na czym polega problem bliskości:**

Zarówno w świecie realnym , jak i cyberprzestrzeni występuje problem bliskości. Jeśli firma ma siedzibę w biurowcu wraz z innymi instytucjami, dla których ryzyko fizycznego ataku jest większe, firma ta przyjmuje w pewnej części to ryzyko. Takie fizyczne ataki mogą przybierać dowolną formę, od groźby podłożenia bomby do pikietowania, lub może być cokolwiek innego, co ma wpływ na działanie tego przedsiębiorstwa.

**Co to są szkody uboczne:**

Szkoda uboczna to taka, która jest spowodowana przez efekt uboczny towarzyszący danemu incydentowi. Nieraz jest to określane efektami kaskadowymi; zwykle ujawniają się one w systemach uzależnionych od systemów, w których wystąpiły incydenty. Szkoda uboczna jest relatywnie nowym problemem w dziedzinie bezpieczeństwa informacji

**Co to jest polityka nakazowa, co to jest polityka uszczelniająca:**

**Polityka nakazowa** obejmuje zbiór rozwiązań, które wprost wynikają z nakazów prawnych i które muszą być bezwzględnie stosowane.

**Polityka uszczelniająca** obejmuje zbiór rozwiązań, które decyzją kierownika jednostki organizacyjnej stanowią „wzmocnienie” rozwiązań nakazowych.

**Na czym polega sterowanie dostępem:**

- model Lampsona (macierzy dostępu) 1969
- najczęściej stosowany
- zbiór podmiotów, zbiór obiektów, zbiór reguł dostępu

**Rozszerzenia:**

- identyfikacja osoby tworzącej regułę dostępu
- wskaźnik prawa przekazania prawa dostępu
- reguły dodatkowych warunków dostępu

**Reguła ochrony wykorzystująca ten mechanizm** - upoważnienie dowolnego żądania dostępu polega na sprawdzeniu w macierzy dostępu czy istnieje reguła dostępu dopuszczająca jego realizację

**Na czym polega sterowanie przepływem:**

- korporacja MITRE ,1973
- zbiór obiektów pamięciowych
- zbiór procesów powodujących przepływy danych
- zbiór klas tajności
- relacja przepływu

**Reguła ochrony wykorzystująca ten mechanizm** - mechanizm sterowania przepływem powinien zabronić realizacji żądań powodujących przepływy danych niezgodnych z określona relacją przepływu

**Kto wchodzi w skład pionu ochrony danych niejawnych:**

- **Pionem Ochrony Informacji Niejawnych** kieruje **Pełnomocnik do spraw Ochrony Informacji Niejawnych** zwany dalej „Pełnomocnikiem Ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.
- W skład **Pionu Ochrony Informacji Niejawnych** wchodzi **Kancelaria Tajna**, która stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio Pełnomocnikowi Ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie dokumentów zawierających informacje niejawne uprawnionym osobom.

**Kto stoi na straży ochrony danych osobowych:**

GIODO - Generalny Inspektor Ochrony Danych Osobowych

Kompetencje GIODO wyznaczają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.). W ich świetle GIODO jest uprawniony do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- prowadzenia rejestru zbioru danych oraz udzielanie informacji o zarejestrowanych zbiorach,

- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W przypadku naruszenia przepisów o ochronie danych osobowych, Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

- usunięcie uchybień,
- uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
- wstrzymanie przekazywania danych osobowych do państwa trzeciego,
- zabezpieczenie danych lub przekazanie ich innym podmiotom,
- usunięcie danych osobowych.

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

#### **Różnica pomiędzy administratorem danych osobowych a administratorem bezpieczeństwa danych osobowych:**

#### **Podstawowe obowiązki administratora danych osobowych**

- obowiązek informacyjny wypełniany przy zbieraniu danych osobowych (art. 24 i 25 ustawy)
- szczególna staranność przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza (art. 26 ustawy)
- udzielanie informacji o zakresie przetwarzanych danych osobowych (art. 33 ustawy)
- obowiązek uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane przez administratora (art. 35 ustawy)
- obowiązek stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 36 ustawy)
- kontroluje, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane (art. 38 ustawy)
- prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy)
- zgłasza zbiór do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych w przypadkach przewidzianych prawem (art. 40 ustawy)

**Administrator bezpieczeństwa informacji** (skrót ABI) – termin prawniczy, który w prawie polskim został zdefiniowany w ustawie z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Oznacza osobę nadzorującą z upoważnienia administratora danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.

**Co to jest zagrożenie pasywne i aktywne:**

- zagrożenia aktywne - wynikające z działań nieuprawnionego użytkownika np. wirusy, terroryzm, vandalizm, inżynieria społeczna
- zagrożenia pasywne - nie będące skutkiem celowego działania (np. powódź, trzęsienie ziemi, huragan, awaria zasilania, awaria sprzętu)

**Co to jest polityka bezpieczeństwa:**

Zestaw reguł określających wykorzystanie informacji, łącznie z jej przetwarzaniem, przechowywaniem, dystrybucją i prezentacją, niezależnie od wymagań dotyczących bezpieczeństwa i celów bezpieczeństwa

**Zest. 4.****1. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

**2. czego dotyczy norma ISO27001****3. czy w polskim prawie karnym jest paragraf na włamania (?)**

TAK (Włamanie do systemu komputerowego jest aktem vandalizmu: Skrypt 96-99)

**4. jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa**

jawny

**5. jakie klauzule odpowiadają tajemnicy państowej**

tajność , ścisła tajność

**6. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi informacje**

zasada wiedzy koniecznej ((??) Skrypt 113)

**7. hoax - co to jest**

(tu nie wiem jakie były możliwości, wg wikipedii hoax to mistyfikacja ☺)

## **Zest. 5.**

**1. Miara bezpieczeństwa w common criteria (norma iso 15194 czy jakoś tak) - jest to poziom uzasadnionego zaufania.**

### **2. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

### **3. Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzecalność (Skrypt 124)

**4. Zasada dostępu tylko do takich informacji przez pracownika , które mu są w tej chwili potrzebne to:**

zasada wiedzy koniecznej (Skrypt 113)

### **5. Czy w prawie karnym jest paragraf za włamania komputerowe**

Tak (Skrypt 96 – 99)

### **6. Jaka norma jest od Systemu zarządzania bezpieczeństwem**

norma ISO27001

**7. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego**

różnica jest taka że pełny audit jest nadzbiorem audytu bezpieczeństwa.

**8. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwową tajność , ścisła tajność**

### **9. Jaki powinien być dokument "Planowania bezpieczeństwa dla ..."**

powinien być jawnym.

### **10. Na czym bazuje autoryzacja dostępu**

na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.

## **Zest. 5.**

1.Co zapewnia Common Criteria i standard ISO/IEC 15408 ?

Odpowiedni poziom zaufania(odp. Ze slowem „zaufanie”)

2. Do czego wykorzystywany jest outsourcing?

Transfer ryzyka

3. Metody uwierzytelniania pracowników

weryfikacja przedmiotu posiadanego przez użytkownika (przepustka).

weryfikacja cech fizycznych użytkownika (odcisk palca, oko, długość fallusa)

weryfikacja wiedzy użytkownik (piny, hasła)

4.Co zapewnia podpis cyfrowy:

Jednoznaczosc, autentyczność...(odpowiedz z największa liczba wymienionych cech)

5. Czym rozni się audyt informatyczny od audytu bezpieczeństwa

Audyt bezpieczeństwa zawiera się w audycie informatycznym.

6. ) czy w polskim prawie jest paragraf dotyczący sankcji za włamania informatyczne?

tak

7. "polityka bezpieczeństwa" jaka powinna miec klauzule tajnosc?

Jawna

8. w ktorej normie jest mowa o wymaganiach dotyczących bezpieczeństwa teleinformatycznego

norma 27001

9. Pytanie dotyczące podawania pracownikom informacji

Odp. Zgodnie z zasada wiedzy koniecznej

10. Atrybuty informacji związane z jej bezpieczeństwem

Tajność, integralność, dostępność

Troszke zebranych materiałów na ten temat:

## **1. Co to jest outsourcing?**

Jest to wykorzystywanie zasobów zewnętrznych, zlecanie wyspecjalizowanym podmiotom zewnętrznym procesów niezbędnych do funkcjonowania dla funkcjonowania własnego przedsiębiorstwa, które zostaną zrealizowane efektywniej niż byłoby to możliwe we własnym zakresie. Zwykle dotyczy to zadań pomocniczych nie związanych bezpośrednio z uzyskiwaniem dochodu. Współcześnie bardzo często są to usługi ochroniarskie, prawnicze, informatyczne, księgowe, rekrutacyjne, wynajem pracowników, utrzymywanie czystości itp.

## **2. W której normie jest mowa o poziomie bezpieczeństwa teleinformatycznego?**

Common Criteria. ISO/IEC 15408 (?)

## **3. Audyt bezpieczeństwa teleinformatycznego, a audyt informatyczny.**

- Audyt informatyczny jest wykorzystywany w procesach biznesowych organizacji systemów informatycznych oraz projektów takich systemów. Jest to proces zbierania i oceniania dowodów w celu określenia czy system informatyczny i związane z nim zasoby właściwie chronią majątek, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągając efektywnie cele organizacji, oszczędnie wykorzystując zasoby i stosując mechanizmy kontroli wewnętrznej tak aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne oraz, że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane, a ich skutki na czas korygowane.

- Audyt bezpieczeństwa to coś mniejszego niż audyt informatyczny. Jest to proces testowania organizacji pod kątem jej zdolności do ochrony informacji

- Audyt informacyjny jako diagnoza stanu posiadania strategii biznesowej, ocena jej poprawności oraz ocena jej postrzegania istotnej akceptacji wśród pracowników firmy.

## **4. Czy w polskim prawie jest paragraf na włamania**

Tak.

## **5. Co zapewnia podpis cyfrowy?**

Podpis elektroniczny jest ekwiwalentem podpisu ręcznego. Technologia zapewnia niezaprzecalność wystawienia takiego podpisu. Oznacza to jednoznaczna identyfikację transakcji i możliwość kontroli nienaruszalności danych podczas transmisji. Podpis cyfrowy polega na dodawaniu unikatowych danych do dokumentu w taki sposób, że generować je może jedynie właściciel klucza prywatnego, ale każdy kto posiada odpowiedni klucz publiczny może weryfikować autentyczność takiego podpisu.

## **6. Dokument „polityka bezpieczeństwa” jaka powinien mieć klauzulę tajności?**

Jawny i ogólnodostępny.

## **7. Metody uwierzytelnienia pracowników?**

1. weryfikacja przedmiotu posiadanego przez użytkownika (przepustka).
2. weryfikacja cech fizycznych użytkownika (odcisk palca, oko, długość fallusa)
3. weryfikacja wiedzy użytkownika (piny, hasła)

## **8. Pytanie o zasadę wiedzy koniecznej?**

Każdy pracownik ma przydzielone jedynie takie prawa i do tych informacji (danych), które wynikają z jego obowiązków, np. prezes firmy ma prawo dostępu do wszystkich danych i ich zestawień na odczyt, ale nie ma prawa żadnych danych modyfikować.

## **9. Common criteria.**

Trzyczęciowa norma międzynarodowa ISO/IEC 15408.

1. Mają na celu ujednolicenie programu informatycznego pod względem bezpieczeństwa

2. Nie zalecają żadnej z metodyk projektowania i wytwarzania systemów informatycznych
3. Są katalogiem schematów konstrukcji wymagań związań z ochroną wymiany informacji.
4. Mogą być stosowane zarówno do produktów programowych jak i sprzętowych w informatyce
5. Są przeznaczone dla użytkowników projektantów

#### **10. Czego dotyczy norma 27001**

Jest ona specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność, z którą będą wydawane certyfikaty. W normie ISO/IEC 27001 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 teleinformatycznych
10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji
11. Zgodność z wymaganiami prawnymi i własnymi standardami

#### **11. Atrybuty informacji związane z jej bezpieczeństwem**

1. tajność – termin ten oznacza, że dostęp do określonych danych i informacji posiadają wyłącznie uprawnione osoby
2. integralność – termin ten oznacza, że dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji
3. dostępność – termin ten charakteryzuje system informatyczny i oznacza dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika
4. inne atrybuty w literaturze - rozliczalność

## **Zest. 6.**

### **1. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

### **2. czego dotyczy norma ISO27001**

Jest specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność z którą mogą być prowadzone audyty, na podstawie których są wydawane certyfikaty.

W normie ISO/IEC 27001 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.

### **3. Czy w polskim prawie karnym jest paragraf na włamania (?)**

TAK (Włamanie do systemu komputerowego jest aktem vandalizmu: Skrypt 96-99)

### **4. Jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa niejawnny, dokument do użytku wewnętrznego**

„Instrukcja bezpieczeństwa teleinformatycznego ... zawiera zasady postępowania w zakresie bezpieczeństwa teleinformatycznego dla osób korzystających z systemów teleinformatycznych; dokument do użytku wewnętrznego.”

#### **5. Jaki poziom ochrony powinien mieć dokument polityka bezpieczeństwa**

jawny

„Zawiera najważniejsze ogólne ustalenia dotyczące działania firmy/instytucji w zakresie ochrony informacji”

#### **6. jakie klauzule odpowiadają tajemnicy państowe.**

Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę państową oznacza się klauzulą:

ścisłe tajne - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych Rzeczypospolitej Polskiej albo zagrażać nieodwracalnymi lub wielkimi stratami dla interesów obronności, bezpieczeństwa państwa i obywateli lub innych istotnych interesów państwa, albo narazić je na szkodę w wielkich rozmiarach,

tajne - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę.

#### **7. jakie klauzule odpowiadają tajemnicy służbowej**

Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą:

poufne - w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli,

zastrzeżone - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

#### **8. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi**

## **informacje**

zasada wiedzy koniecznej (Skrypt 113)???

### **9. hoax - co to jest**

Z ang: głupi żart; głupi kawał; głupi dowcip

Fałszywka (hoax) to wykorzystanie ludzkiej niewiedzy do rozprzestrzenienia podanej informacji. Polega to na tym, że użytkownik otrzymuje wiadomość (poprzez sieć, telefonicznie czy podczas rozmowy) o pewnym zdarzeniu powodującą podjęcie przez niego określonego działania. Może to być np. otrzymanie maila z wiadomością, że plik o podanej nazwie jest wirusem i można się go pozbyć jedynie poprzez usunięcie tego pliku. W rzeczywistości plik nie jest wirusem i może być nawet częścią systemu operacyjnego, a jego usunięcie może spowodować nieprzewidziane skutki. Użytkownik najczęściej zastosuje się do wskazówek zawartych w otrzymanej wiadomości i w dobrej wierze rozpowszechni ją dalej (w przypadku maili spowoduje to niepotrzebny wzrost generowanego w sieci ruchu). Oprócz wywołania zamieszania fałszywki mogą również przyczynić się do poniesienia szkód (np. otrzymanie wiadomości o awarii serwera i prośbie o wysłanie hasła do konta na podany adres). Walczyć z takimi fałszywymi alarmami jest szczególnie trudno gdyż nigdy nie ma 100% pewności czy są one prawdziwe czy nie. Najlepiej jest mieć ograniczone zaufanie do podejrzanych i pochodzących z niepewnych źródeł wiadomości i sprawdzać ich wiarygodność w serwisach antywirusowych.

### **10. Miara bezpieczeństwa w common criteria.**

Common Criteria (norma ISO 15408) - norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych.

CC udostępnia procedury pozwalające na zdefiniowanie zagrożeń oraz zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania w produkcie. Certyfikacją według normy CC zajmują się niezależne, akredytowane laboratoria badawcze na całym świecie.

Wynikiem procesu certyfikacji jest tzw. "profil ochrony" (PP - *protection profile*), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat, potwierdzający ich faktyczną skuteczność. Proces certyfikacji może być prowadzony według różnych poziomów szczegółowości i weryfikacji formalnej (EAL - *Evaluation Assurance Level*), począwszy od EAL1 (tylko testy funkcjonalne) aż do EAL7 (formalna weryfikacja projektu oraz testy).

Posiadanie certyfikatu CC *nie gwarantuje* że produkt jest bezpieczny pod każdym względem - zapewnia jedynie o działaniu wszystkich *zadeklarowanych* przez producenta zabezpieczeń. Sam certyfikat niewiele więc mówi bez profilu ochrony opisującego zastosowane

zabezpieczenia. Dla popularnych produktów (np. bezpieczne urządzenie do składania podpisu elektronicznego) istnieją ustandaryzowane profile ochrony.

Starszą, ale nadal stosowaną w certyfikacji normą tego typu jest ITSEC.

#### **10b. Co zapewnia Common Criteria i standard ISO/IEC 15408 ?**

Odpowiedni poziom zaufania.

### **11. Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzecjalność (Skrypt 124)

**W szerszym rozumieniu podpis elektroniczny posiada cztery główne cechy:**

autentykacja – uniemożliwienie podszywania się pod daną osobę i wysłania w jej imieniu przesyłki, np. zlecenia dokonania przez bank operacji;

integralność – zapewnienie wykrywalności wszelkiej zmiany w danych przesyłki, zlecenia na drodze od nadawcy do odbiorcy i podczas przechowywania jej u odbiorcy;

autoryzacja – zapewnienie niemożliwości wyparcia się podpisu i treści przesyłki (zlecenia) przez autora;

umożliwienie weryfikacji podpisu przez osobę niezależną.

### **12. Czy w prawie karnym jest paragraf za włamania komputerowe**

Tak (Skrypt 96 – 99)

### **12. Jaka norma jest od Systemu zarządzania bezpieczeństwem**

Pytanie 2 - norma ISO27001

### **13. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego**

Audyt – ocena danej osoby, organizacji, systemu, procesu, projektu lub produktu. Audyt jest przeprowadzany w celu upewnienia się co do prawdziwości i rzetelności informacji, a także oceny systemu kontroli wewnętrznej.

Standard COBIT (Control Objectives for Information and Related Technology) opracowany i rozwijany w ramach ISACA (Information Systems Audit and Control Association). Standard ten zawiera "Control Objectives", czyli tak zwane Punkty Kontrolne, gdzie określone są 302 szczegółowe wymagania przypisane do 34 procesów przebiegających w systemie informatycznym. Jeżeli audyt będzie dotyczył wszystkich procesów, ocenionych zarówno przez pryzmat pierwszo jak i drugorzędnych kryteriów, będzie to pełny audit informatyczny.

Jeżeli procesy będą oceniane tylko wg wybranych kryteriów, np. poufności, integralności i dostępności to możemy mówić o audycie bezpieczeństwa informatycznego. Audit bezpieczeństwa inf. jest tylko częścią audytu informatycznego

Pełny audit informatyczny jest nadzorem audytu bezpieczeństwa teleinformatycznego

#### **14. Na czym bazuje autoryzacja dostępu**

- na przedmiocie posiadanym przez osobę autoryzowaną (przepustka)
- cechach fizycznych (odcisk palca, skan siatkówki oka)
- jego wiedzy (PIN, hasło)

#### **15. Do czego wykorzystywany jest outsourcing?**

##### Transfer ryzyka

Outsourcing – wykorzystywanie zasobów zewnętrznych, zlecanie wyspecjalizowanym podmiotom zewnętrznym procesów niezbędnych dla funkcjonowania własnego przedsiębiorstwa, które zostaną tam zrealizowane efektywniej niż byłoby to możliwe we własnym zakresie. Outsourcing jest częścią szerszego zagadnienia - strategii przedsiębiorstwa w obszarze sourcingu.

Zwykle dotyczy to zadań pomocniczych, nie związanych bezpośrednio z uzyskiwaniem dochodu. Współcześnie bardzo często outsource'owane są usługi ochroniarskie, prawnicze, informatyczne, księgowe, rekrutacyjne, wynajem pracowników (outsourcing personalny), utrzymywanie czystości itd. Niektóre firmy idą znacznie dalej, outsource'uając np. support lub część produkci. Wśród dużych zachodnich koncernów rozpowszechniła się praktyka outsource'owania znacznej części produkcji do krajów o tańszej sile roboczej, zwłaszcza do krajów azjatyckich – szczególną popularnością cieszą się usługi firm hinduskich.

Najczęstszą przyczyną wprowadzania praktyk outsourcingowych jest chęć obniżenia kosztów i uniknięcia sytuacji korupcjognnych.

### **16. Metody uwierzytelniania pracowników**

Weryfikacja z elem. z pytania 14

### **17. Co nie jest plikiem systemowym NTFS**

\$Sector.

## **Zest. 7.**

### **1. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

### **2. czego dotyczy norma ISO27001**

Jest specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność z którą mogą być prowadzone audyty, na podstawie których są wydawane certyfikaty.

W normie ISO/IEC 27001 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.

### **3. Czy w polskim prawie karnym jest paragraf na włamania (?)**

TAK (Włamanie do systemu komputerowego jest aktem vandalizmu: Skrypt 96-99)

### **4. Jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa niejawnny, dokument do użytku wewnętrznego**

„Instrukcja bezpieczeństwa teleinformatycznego ... zawiera zasady postępowania w zakresie bezpieczeństwa teleinformatycznego dla osób korzystających z systemów teleinformatycznych; dokument do użytku wewnętrznego.”

#### **5. Jaki poziom ochrony powinien mieć dokument polityka bezpieczeństwa**

jawny

„Zawiera najważniejsze ogólne ustalenia dotyczące działania firmy/instytucji w zakresie ochrony informacji”

#### **6. jakie klauzule odpowiadają tajemnicy państowe.**

Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę państową oznacza się klauzulą:

ścisłe tajne - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych Rzeczypospolitej Polskiej albo zagrażać nieodwracalnymi lub wielkimi stratami dla interesów obronności, bezpieczeństwa państwa i obywateli lub innych istotnych interesów państwa, albo narazić je na szkodę w wielkich rozmiarach,

tajne - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę.

#### **7. jakie klauzule odpowiadają tajemnicy służbowej**

Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą:

poufne - w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli,

zastrzeżone - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

#### **8. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi**

## **informacje**

zasada wiedzy koniecznej (Skrypt 113)???

### **9. hoax - co to jest**

Z ang: głupi żart; głupi kawał; głupi dowcip

Fałszywka (hoax) to wykorzystanie ludzkiej niewiedzy do rozprzestrzenienia podanej informacji. Polega to na tym, że użytkownik otrzymuje wiadomość (poprzez sieć, telefonicznie czy podczas rozmowy) o pewnym zdarzeniu powodującą podjęcie przez niego określonego działania. Może to być np. otrzymanie maila z wiadomością, że plik o podanej nazwie jest wirusem i można się go pozbyć jedynie poprzez usunięcie tego pliku. W rzeczywistości plik nie jest wirusem i może być nawet częścią systemu operacyjnego, a jego usunięcie może spowodować nieprzewidziane skutki. Użytkownik najczęściej zastosuje się do wskazówek zawartych w otrzymanej wiadomości i w dobrej wierze rozpowszechni ją dalej (w przypadku maili spowoduje to niepotrzebny wzrost generowanego w sieci ruchu). Oprócz wywołania zamieszania fałszywki mogą również przyczynić się do poniesienia szkód (np. otrzymanie wiadomości o awarii serwera i prośbie o wysłanie hasła do konta na podany adres). Walczyć z takimi fałszywymi alarmami jest szczególnie trudno gdyż nigdy nie ma 100% pewności czy są one prawdziwe czy nie. Najlepiej jest mieć ograniczone zaufanie do podejrzanych i pochodzących z niepewnych źródeł wiadomości i sprawdzać ich wiarygodność w serwisach antywirusowych.

### **10. Miara bezpieczeństwa w common criteria.**

Common Criteria (norma ISO 15408) - norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych.

CC udostępnia procedury pozwalające na zdefiniowanie zagrożeń oraz zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania w produkcie. Certyfikacją według normy CC zajmują się niezależne, akredytowane laboratoria badawcze na całym świecie.

Wynikiem procesu certyfikacji jest tzw. "profil ochrony" (PP - *protection profile*), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat, potwierdzający ich faktyczną skuteczność. Proces certyfikacji może być prowadzony według różnych poziomów szczegółowości i weryfikacji formalnej (EAL - *Evaluation Assurance Level*), począwszy od EAL1 (tylko testy funkcjonalne) aż do EAL7 (formalna weryfikacja projektu oraz testy).

Posiadanie certyfikatu CC *nie gwarantuje* że produkt jest bezpieczny pod każdym względem - zapewnia jedynie o działaniu wszystkich *zadeklarowanych* przez producenta zabezpieczeń. Sam certyfikat niewiele więc mówi bez profilu ochrony opisującego zastosowane

zabezpieczenia. Dla popularnych produktów (np. bezpieczne urządzenie do składania podpisu elektronicznego) istnieją ustandaryzowane profile ochrony.

Starszą, ale nadal stosowaną w certyfikacji normą tego typu jest ITSEC.

#### **10b. Co zapewnia Common Criteria i standard ISO/IEC 15408 ?**

Odpowiedni poziom zaufania.

### **11. Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzecjalność (Skrypt 124)

**W szerszym rozumieniu podpis elektroniczny posiada cztery główne cechy:**

autentykacja – uniemożliwienie podszywania się pod daną osobę i wysłania w jej imieniu przesyłki, np. zlecenia dokonania przez bank operacji;

integralność – zapewnienie wykrywalności wszelkiej zmiany w danych przesyłki, zlecenia na drodze od nadawcy do odbiorcy i podczas przechowywania jej u odbiorcy;

autoryzacja – zapewnienie niemożliwości wyparcia się podpisu i treści przesyłki (zlecenia) przez autora;

umożliwienie weryfikacji podpisu przez osobę niezależną.

### **12. Czy w prawie karnym jest paragraf za włamania komputerowe**

Tak (Skrypt 96 – 99)

### **12. Jaka norma jest od Systemu zarządzania bezpieczeństwem**

Pytanie 2 - norma ISO27001

### **13. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego**

Audyt – ocena danej osoby, organizacji, systemu, procesu, projektu lub produktu. Audyt jest przeprowadzany w celu upewnienia się co do prawdziwości i rzetelności informacji, a także oceny systemu kontroli wewnętrznej.

Standard COBIT (Control Objectives for Information and Related Technology) opracowany i rozwijany w ramach ISACA (Information Systems Audit and Control Association). Standard ten zawiera "Control Objectives", czyli tak zwane Punkty Kontrolne, gdzie określone są 302 szczegółowe wymagania przypisane do 34 procesów przebiegających w systemie informatycznym. Jeżeli audyt będzie dotyczył wszystkich procesów, ocenionych zarówno przez pryzmat pierwszo jak i drugorzędnych kryteriów, będzie to pełny audit informatyczny.

Jeżeli procesy będą oceniane tylko wg wybranych kryteriów, np. poufności, integralności i dostępności to możemy mówić o audycie bezpieczeństwa informatycznego. Audit bezpieczeństwa inf. jest tylko częścią audytu informatycznego

Pełny audit informatyczny jest nadzorem audytu bezpieczeństwa teleinformatycznego

#### **14. Na czym bazuje autoryzacja dostępu**

- na przedmiocie posiadanym przez osobę autoryzowaną (przepustka)
- cechach fizycznych (odcisk palca, skan siatkówki oka)
- jego wiedzy (PIN, hasło)

#### **15. Do czego wykorzystywany jest outsourcing?**

##### Transfer ryzyka

Outsourcing – wykorzystywanie zasobów zewnętrznych, zlecanie wyspecjalizowanym podmiotom zewnętrznym procesów niezbędnych dla funkcjonowania własnego przedsiębiorstwa, które zostaną tam zrealizowane efektywniej niż byłoby to możliwe we własnym zakresie. Outsourcing jest częścią szerszego zagadnienia - strategii przedsiębiorstwa w obszarze sourcingu.

Zwykle dotyczy to zadań pomocniczych, nie związanych bezpośrednio z uzyskiwaniem dochodu. Współcześnie bardzo często outsource'owane są usługi ochroniarskie, prawnicze, informatyczne, księgowe, rekrutacyjne, wynajem pracowników (outsourcing personalny), utrzymywanie czystości itd. Niektóre firmy idą znacznie dalej, outsource'uając np. support lub część produkci. Wśród dużych zachodnich koncernów rozpowszechniła się praktyka outsource'owania znacznej części produkcji do krajów o tańszej sile roboczej, zwłaszcza do krajów azjatyckich – szczególną popularnością cieszą się usługi firm hinduskich.

Najczęstszą przyczyną wprowadzania praktyk outsourcingowych jest chęć obniżenia kosztów i uniknięcia sytuacji korupcjognnych.

### **16. Metody uwierzytelniania pracowników**

Weryfikacja z elem. z pytania 14

### **17. Co nie jest plikiem systemowym NTFS**

\$Sector.

## **Zest. 8.**

### **1. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

### **2. czego dotyczy norma ISO27001**

#### **>3. czy w polskim prawie karnym jest paragraf na włamania (?)**

TAK (Włamanie do systemu komputerowego jest aktem vandalizmu: Skrypt 96-99)

### **4. jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa**

jawny

### **5. jakie klauzule odpowiadają tajemnicy państowej**

tajność , ścisła tajność

### **6. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi**

**informacje**

zasada wiedzy koniecznej ((??) Skrypt 113)

### **7. hoax - co to jest**

(tu nie wiem jakie były możliwości, wg wikipedii hoax to mistyfikacja ☺)

**1. Miara bezpieczeństwa w common criteria (norma iso 15194 czy jakoś tak) - jest to poziom uzasadnionego zaufania.**

**2. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

**3. Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzeczalność (Skrypt 124)

**4. Zasada dostępu tylko do takich informacji przez pracownika , które mu są w tej chwili potrzebne to:**

zasada wiedzy koniecznej (Skrypt 113)

**5. Czy w prawie karnym jest paragraf za włamania komputerowe**

Tak (Skrypt 96 – 99)

**6. Jaka norma jest od Systemu zarządzania bezpieczeństwem**

norma ISO27001

**7. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego**

Różnica jest taka że pełny audit jest nadzorem audytu bezpieczeństwa.

**8. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwową tajność , ścisła tajność**

**9. Jaki powinien być dokument "Planowania bezpieczeństwa dla ..."**

powinien być jawnym.

**10. Na czym bazuje autoryzacja dostępu**

na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.

Dla testu B

1. atrybuty informacji: **(tajność, integralność, dostępność)**
2. czy w polskim prawie karnym jest paragraf na włamania **(tak)** (chyba par. 255k.k. <- poza konkurem)
3. jaki poziom ochrony powinien mieć dokument polityka bezpieczeństwa **(jawny)**
4. w teście B zad 1 coś z normą PN/ISO xxxx45 odpowiedź **a)** (najmniej pasująca)
5. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi informacje **(zasada wiedzy koniecznej)**
6. weryfikacja tożsamości użytkownika na podstawie **rzeczy** (np klucz), **cech fizycznych** (np odcisk palca, zdjęcie), **wiedzy** (np hasło)
7. było coś z normą PN/ISO 27001 ale nie pamiętam już co.
8. Nie pamiętam pytania, to jest konkluzja -> **Pełny audit informatyczny jest nadzorem audytu bezpieczeństwa teleinformatycznego**

## **Zest. 9.**

### **1. Co to jest informacja**

Informacja – obiekt abstrakcyjny, który może zwiększyć obszar wiedzy.

Z teorii informacji to miara niepewności zajścia pewnego zdarzenia ze zbioru skońzonego zdarzeń prawdziwych.

### **2. Co to jest bezpieczeństwo informacji**

slajd 94 +

W obecnych czasach, instytucje niezależnie od profilu działalności wytwarzają, przechowują, przetwarzają i przesyłają informacje wrażliwe, których nieuprawnione ujawnienie lub zniszczenie może spowodować poważne szkody dla osoby fizycznej lub instytucji.

Przykładem informacji wrażliwej mogą być informacje stanowiące tajemnicę państwową lub służbową, dane osobowe, hasła użytkowników systemów informatycznych oraz informacje dotyczące działań instytucji. W odniesieniu do bezpieczeństwa systemów teleinformatycznych informacja jest przedmiotem, którym należy właściwie zarządzać i chronić go.

Ochrona danych przed nieuprawnionym, przypadkowym, umyślnym ujawnieniem, modyfikacją lub zniszczeniem opiera się na spełnieniu aspektów bezpieczeństwa, jakimi są:

- poufność,
- integralność,
- dostępność,
- spójność danych.

Poufność oznacza stan w którym informacje wrażliwe mogą zostać odczytane tylko przez uprawnione osoby.

Integralność danych oznacza, że pochodzą one z wiarygodnego źródła, są kompletne i poprawne, ich modyfikacji dokonują osoby upoważnione.

Dostępność to zapewnienie, że uprawnieni użytkownicy mają dostęp do zasobów systemu informatycznego, kiedy zachodzi taka potrzeba.

Spójność danych dotyczy poprawności baz danych i wiąże się z właściwym ich zarządzaniem oraz odpornością na awarie środowiska sprzętowo-programowego oraz anomalie wynikające z rozproszenia baz danych.

Powszechnie bezpieczeństwo kojarzy się z niezakłóconą pracą systemów, jednak należy przy tym pamiętać, że zakłócić może ją wiele czynników. Źródłem zagrożenia może być niepowołany dostęp do zasobów nie tylko z zewnątrz, ale i od wewnętrz sieci korporacyjnej. Ze względu na rodzaj zagrożenia, wyróżniamy ataki aktywne i pasywne. Ataki aktywne dążą do modyfikacji strumienia informacji lub tworzenia fałszywych informacji, np. podszywanie się pod osobę uprawnioną i blokowanie działania. Ataki pasywne polegają na podsłuchiwaniu i monitorowaniu przesyłanych informacji, np. dążenie do ujawnienia treści wiadomości.

Utrzymanie wysokiego poziomu bezpieczeństwa strategicznych zasobów systemu informatycznego wymaga między innymi:

- dokonania klasyfikacji zasobów poprzez określenie stopnia ich wrażliwości;
- stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów systemu;
- doboru i wdrożenia odpowiednich sprzętowo-programowych rozwiązań, takich jak system zaporowy, systemy wykrywania włamań, system antywirusowy;
- zastosowania środków ochrony mających wpływ na zwiększenie niezawodności sprzętu oraz umożliwiających odtworzenie stanu systemu po awarii;
- przeszkolenia użytkowników sieci korporacyjnej w zakresie przeciwdziałania i wykrywania naruszeń bezpieczeństwa informatycznego;
- podnoszenia kwalifikacji administratorów systemów poprzez specjalistyczne szkolenia z zakresu bezpieczeństwa teleinformatycznego.

W celu zapewnienia niezawodności w działaniu wdrożonego systemu bezpieczeństwa i stworzenia możliwości spełnienia powierzonej roli, należy go systematycznie aktualizować. Wdrożone systemy zaporowy lub antywirusowy, które nie posiadają uaktualnień wersji i latek, stają się podatne na wszelkiego rodzaju ataki ze strony hakerów. Sytuacja taka powoduje naruszenie aspektów bezpieczeństwa, jakimi są: poufność, integralność, dostępność i spójność danych znajdujących się w sieci.

Ventus Communications kładzie szczególny nacisk na bezpieczeństwo danych w projektowanych przez siebie sieciach. Opracowujemy kompleksową politykę bezpieczeństwa systemów teleinformatycznych przedsiębiorstwa obejmującą podstawowe założenia bezpieczeństwa oraz szczegółowe procedury dla każdego z użytkowników. W naszej ofercie posiadamy produkty pozwalające na stworzenie kompleksowego systemu zabezpieczeń każdego przedsiębiorstwa. Z dostępnych na rynku rozwiązań wybraliśmy te o najlepszych referencjach tak, aby realizowane przez nas systemy były niezawodne i funkcjonalne.

### **3. Jakie są skutki zawyżania klauzuli tajności**

Nieuzasadnione podwyższanie klauzul tajności powoduje:

- utrudnienia w przetwarzaniu danych,
- zwiększone koszty budowy systemu bezpieczeństwa informacyjnego, znacznie zwiększone koszty eksploatacyjne, szkoleniowe, itd.,
- ograniczone możliwości współdziałania z innymi systemami informatycznymi,
- niemożliwość wykonania wielu uzasadnionych zadań przetwarzania bez naruszenia ustawy,
- narażenie pracowników na świadome lub nieświadome (przy braku odpowiednich mechanizmów) naruszenie ustawy,

### **4. Co to jest zagrożenie pasywne i zagrożenie aktywne**

**Zagrożenie aktywne** - dowolne zagrożenie związane z zamierzoną, nieuprawnioną zmianą stanu systemu przetwarzania danych.

**Zagrożenia zamierzone:**

- a. nielegalne , świadome działania własnych pracowników
- b. działania użytkowników wykraczające poza ich obowiązki
- c. działania przestępcości komputerowych
- d. szpiegostwo gospodarcze i wojskowe
- e. vandalizm , terroryzm , sabotaż

**Zagrożenie pasywne** - nie będące skutkiem celowego działania.

**Zagrożenia niezamierzone:**

- a. zagrożenia losowe
- b. zagrożenia związane z niedostatkami organizacyjnymi
- c. zagrożenia związane z błędem człowieka
- d. Zagrożenia techniczne (awarie)

**Źródła zagrożeń**

- użytkownicy:
  - wewnętrzni:
    - akty wewnętrznego sabotażu
    - kradzież informacji
    - kradzież usług
    - błędy użytkowników
    - niedbalstwo
    - nieprawidłowe stosowanie mechanizmów bezpieczeństwa
  - zewnętrzni
- ataki na systemy informatyczne
- wirusy komputerowe
- awarie sprzętu

**Przyczyny występowania luk**

- błędy na etapie projektowania systemu
  - asymetria polityki bezpieczeństwa i zabezpieczeń
- brak lub wady polityki bezpieczeństwa
  - asymetria polityki bezpieczeństwa i brak kontroli
- błędy w konfiguracji
  - prymat funkcjonalności systemu
- niewłaściwe stosowanie narzędzi
  - Nadmierne zaufanie do narzędzi (ulubionych)
- błędy w oprogramowaniu
  - nie ma oprogramowanie bez błędów
- zaufanie do „uznanych producentów”
  - producent implementuje technologie

## 5. Co to jest problem bliskości i szkody uboczne

### Problem bliskości

Zarówno w świecie realnym , jak i cyberprzestrzeni występuje problem bliskości. Jeśli firma ma siedzibę w biurowcu wraz z innymi instytucjami, dla których ryzyko fizycznego ataku jest większe, firma ta przyjmuje w pewnej części to ryzyko. Takie fizyczne ataki mogą przybierać dowolną formę, od groźby podłożenia bomby do pikietowania, lub może być cokolwiek innego, co ma wpływ na działanie tego przedsiębiorstwa.

### Szkody uboczne

Szkoda uboczna to taka, która jest spowodowana przez efekt uboczny towarzyszący danemu incydentowi. Nieraz jest to określane efektami kaskadowymi; zwykle ujawniają się one w systemach uzależnionych od systemów, w których wystąpiły incydenty. Szkoda uboczna jest relatywnie nowym problemem w dziedzinie bezpieczeństwa informacji.

## 6. Co to jest polityka nakazowa i polityka uszczelniająca

**Polityka nakazowa** obejmuje zbiór rozwiązań, które wprost wynikają z nakazów prawnych i które muszą być bezwzględnie stosowane.

**Polityka uszczelniająca** obejmuje zbiór rozwiązań, które decyzją kierownika jednostki organizacyjnej stanowią „wzmocnienie” rozwiązań nakazowych.

## **7. Na czym polega sterowanie dostępem i sterowanie przepływem, wraz z regułami ochrony**

**kontrola dostępu / sterowanie dostępem** - jest ochroną zasobów przed nieupoważnionymi użytkownikami.

- model Lampsona (macierzy dostępu) 1969
- najczęściej stosowany
- zbiór podmiotów, zbiór obiektów, zbiór reguł dostępu

**rozszerzenia:**

- identyfikacja osoby tworzącej regułę dostępu
- wskaźnik prawa przekazania prawa dostępu
- reguły dodatkowych warunków dostępu

**reguła ochrony** - upoważnienie dowolnego żądania dostępu polega na sprawdzeniu w macierzy dostępu czy istnieje reguła dostępu dopuszczająca jego realizację.

- sterowanie przepływem
- korporacja MITRE ,1973
- zbiór obiektów pamięciowych
- zbiór procesów powodujących przepływ danych
- zbiór klas tajności
- relacja przepływu

**reguła ochrony** - mechanizm sterowania przepływem powinien zabronić realizacji żądań powodujących przepływ danych niezgodnych z określona relacją przepływu

## **8. Co to jest polityka bezpieczeństwa**

**Polityka bezpieczeństwa** (ang. *security policy*) jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby i w jaki sposób mają być chronione.

Polityka powinna obejmować wskazanie możliwych rodzajów naruszenia bezpieczeństwa (jak np. utrata danych, nieautoryzowany dostęp), scenariusze postępowania w takich

sytuacjach i działania, które pozwolą uniknąć powtórzenia się danego incydentu. Polityka bezpieczeństwa definiuje ponadto poprawne i niepoprawne korzystanie z zasobów (np. kont użytkowników, danych, oprogramowania).

Istotne jest, aby polityka bezpieczeństwa była dokumentem spisanym i znany oraz zrozumianym przez pracowników organizacji korzystających z zasobów informatycznych. Dotyczy to także klientów organizacji (użytkowników jej zasobów).

Przy projektowaniu polityki należy rozważyć, czy organizacja będzie w stanie ponieść koszty wprowadzania tej polityki w życie. Podwyższanie poziomu bezpieczeństwa organizacji/systemu odbywa się najczęściej kosztem wygody i efektywności działania. Dlatego, opierając się na zalecanych modelach czy standardach w tej dziedzinie, należy pamiętać o dostosowaniu rozwiązania do specyfiki organizacji, tak aby nadać jej cechy ułatwiające zastosowanie w praktyce. Podstawowym zadaniem jest przeprowadzenie analizy ryzyka i ustalenie akceptowalnego poziomu ryzyka - bo tylko wtedy możemy zacząć myśleć o tworzeniu polityki bezpieczeństwa.

Polityka powinna adresować następujące zagadnienia:

- co podlega ochronie ?
  - informacja (dane)
  - systemy teleinformatyczne ( sprzęt )
- jak chronimy krytyczne zasoby ?

Projektując mechanizmy ochrony informacji należy określić następujące elementy:

- model bezpieczeństwa
- mechanizmy kontroli dostępu
- poziomy uprawnień (jakie poziomy uprawnień istnieją i jakie są zasady ich przyznawania)
- mechanizmy identyfikacji i zapewnienie autentyczności (na poziomie fizycznym i systemów)
- śledzenie zdarzeń w systemie (jakie mechanizmy/programy/procedury stosowane są do śledzenia zmian w systemach)

## **9. Kto wchodzi w skład pionu ochrony danych osobowych**

W celu realizacji zadań związanych z ochroną informacji niejawnych kierownicy jednostek organizacyjnych tworzą stanowiska pełnomocników ochrony informacji niejawnych, którym podlegają piony ochrony lub wytypowani do tych zadań pracownicy.

Pion ochrony informacji niejawnych jest komórką organizacyjną właściwą do określania i zapewniania przestrzegania zasad ochrony informacji niejawnych, a także ich eksploatacji, jak również bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony fizycznej obiektów w danej jednostce organizacyjnej, które wymagają ochrony przed nieuprawnionym dostępem osób postronnych /nieupoważnionych/.

Tworzenia pionu ochrony informacji niejawnych w jednostce organizacyjnej:

- Kierownik jednostki organizacyjnej powołuje na pełnomocnika ochrony osobę, która spełnia następujące wymagania:
  - posiada obywatelstwo polskie,
  - posiada co najmniej średnie wykształcenie,
  - posiada odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa po przeprowadzeniu postępowania sprawdzającego,
  - odbyła przeszkolenie w zakresie ochrony informacji niejawnych.
- Na wniosek pełnomocnika ochrony kierownik jednostki organizacyjnej wyznacza kierownika kancelarii tajnej oraz w razie potrzeby pozostałych pracowników pionu ochrony, którzy spełniają następujące wymagania:
  - posiadają obywatelstwo polskie,
  - posiadają odpowiednie poświadczenie bezpieczeństwa wydane po przeprowadzeniu postępowania sprawdzającego,
  - odbyły przeszkolenie w zakresie ochrony informacji niejawnych.
- Kierownik jednostki organizacyjnej w oparciu o wydzielone środki finansowe tworzy tajną kancelarię w wyodrębnionym pomieszczeniu, zabezpieczonym zgodnie z przepisami o środkach ochrony fizycznej informacji niejawnych (zlokalizowanym w strefie bezpieczeństwa, z wydzieloną wokół strefy bezpieczeństwa strefą administracyjną służącą do kontroli osób i pojazdów, z systemem określającym uprawnienia do wejścia, przebywania i wyjścia ze strefy bezpieczeństwa oraz wyposażeniem i urządzeniami, którym na podstawie odrębnych przepisów przyznano certyfikaty i świadectwa kwalifikacyjne) i obsługiwana przez pracowników pionu ochrony.
- Pełnomocnik opracowuje instrukcje pracy kancelarii tajnej.
- Kierownik jednostki organizacyjnej określa w zarządzeniu stanowiska oraz rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności dla osób zatrudnionych w podległych komórkach organizacyjnych.
- Pełnomocnik ochrony prowadzi w jednostce organizacyjnej "Wykaz stanowisk i prac zleconych oraz osób dopuszczonych do pracy lub służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności" w oparciu o:

- zwykłe postępowanie sprawdzające przeprowadzone przez pełnomocnika ochrony na pisemne polecenie kierownika jednostki organizacyjnej wobec osób zatrudnionych w podległych komórkach organizacyjnych,
  - postępowanie sprawdzające przeprowadzone przez służby ochrony państwa na pisemny wniosek kierownika jednostki organizacyjnej wobec osób zatrudnionych w podległych komórkach organizacyjnych.
- Kierownik jednostki organizacyjnej zatwierdza opracowane przez pełnomocnika ochrony, szczegółowe wymagania w zakresie ochrony informacji niejawnych oznaczonych klauzulą "zastrzeżone" w podległych komórkach organizacyjnych.
- Opracowanie przez pion ochrony planu ochrony informacji niejawnych w jednostce organizacyjnej i nadzorowanie jego realizacji.

Do podstawowych zadań pionu ochrony należy:

- organizowanie ochrony informacji niejawnych;
- klasyfikowanie informacji niejawnych;
- udostępnianie informacji niejawnych;
- organizowanie szkolenia na temat ochrony informacji niejawnych;
- ochrona informacji niejawnych w systemach i sieciach teleinformatycznych;
- prowadzenie zwykłych postępowań sprawdzających przed wydaniem poświadczzeń bezpieczeństwa do klauzuli "Zastrzeżone" i "Poufne";
- ewidencjonowanie, przechowywanie, przetwarzanie i udostępnianie danych uzyskiwanych w związku z prowadzonym postępowaniem o ustalenie rękojmi zachowania tajemnicy w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w ankiecie bezpieczeństwa przemysłowego;
- organizowanie kontroli przestrzegania zasad ochrony informacji niejawnych w jednostce organizacyjnej;
- opracowywanie i opiniowanie planów postępowania z informacjami niejawnymi w razie wprowadzenia stanu nadzwyczajnego;
- organizowanie systemu kontroli dostępu do obiektów i poszczególnych stref bezpieczeństwa oraz nadzorowanie przechowywania i wykorzystywania kluczy i kodów do zamków szyfrowych;
- monitorowanie pomieszczeń objętych specjalną strefą bezpieczeństwa podczas narad, konferencji i odpraw prowadzonych w obiektach jednostki organizacyjnej;
- uczestniczenie w opiniowaniu projektów rozporządzeń oraz projektów programów, analiz i innych dokumentów opracowywanych w jednostce organizacyjnej, a dotyczących ochrony informacji niejawnych;
- nadzorowanie rozdziału środków finansowych przeznaczonych na realizację wspomagania ochrony i obrony obiektów jednostki organizacyjnej;

**Generalny Inspektor Ochrony Danych Osobowych** (skr. **GIODO**) - organ do spraw ochrony danych osobowych powoływany na 4-letnią kadencję (liczoną od dnia złożenia przysięgi) przez Sejm RP za zgodą Senatu.

Działa na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. W zakresie wykonywania swoich zadań podlega tylko ustawie. Przysługuje mu immunitet. Kontroluje zgodność przetwarzania danych z przepisami o ochronie danych osobowych, wydaje decyzje administracyjne i rozpatruje skargi w sprawach wykonania przepisów o ochronie danych osobowych, prowadzi rejestr zbiorów danych, opiniuje akty prawne dotyczące ochrony danych osobowych, inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych, uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych (np. Grupy roboczej art. 29).

W celu wykonania swoich zadań ma do pomocy Biuro Generalnego Inspektora Ochrony Danych Osobowych. Siedziba Biura znajduje się w Warszawie.

Generalni Inspektorzy Ochrony Danych Osobowych:

- I kadencja (4 kwietnia 1998 - 26 kwietnia 2002) - Ewa Kulesza
- II kadencja (26 kwietnia 2002 - 13 lipca 2006) - Ewa Kulesza
- III kadencja od 13 lipca 2006 - Michał Serzycki

#### **Zest. 10.**

1. atrybuty informacji: (**tajność, integralność, dostępność**)
2. czy w polskim prawie karnym jest paragraf na włamania (**tak**) (chyba par. 255k.k. <- poza konkurem)
3. jaki poziom ochrony powinien mieć dokument polityka bezpieczeństwa (**jawny**)
4. w teście B zad 1 coś z normą PN/ISO xxxx45 odpowiedź **a)** (najmniej pasująca)
5. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi informacje (**zasada wiedzy koniecznej**)
6. weryfikacja tożsamości użytkownika na podstawie **rzeczy** (np klucz), **cech fizycznych** (np odcisk palca, zdjęcie), **wiedzy** (np hasło)
7. było coś z normą PN/ISO 27001 ale nie pamiętam juz co.
- 8.Nie pamiętam pytania, to jest konkluzja -> **Pełny audyt informatyczny jest nadzbiorem audytu bezpieczeństwa teleinformatycznego**  
wiecej nie pamiętam

Ad.1

Atrybuty informacji:

**Bezpieczeństwo informacji** - oznacza zachowanie poufności, integralności i dostępności informacji.

**integralność** - jest zdefiniowana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

**dostępność** - jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

Ad.2

TAK (Art. 267)

Ad.3

Dokument powinien być **jawny**.

Ad.4

- a) cokolwiek to było:P
- b)

Ad.5

**zasada wiedzy koniecznej:** Pracownik powinien mieć dostęp w określonym zakresie tylko do tych zasobów, których potrzebuje do zakończenia zadania. Ograniczenie dostępności zasobów zgodnie z zasadą wiedzy koniecznej umożliwia zmniejszenie negatywnych skutków działania procesów błędnych.

Ad.6

Weryfikacja tożsamości użytkownika:

- **rzeczy** (np klucz)
- **cech fizycznych** (np odcisk palca, zdjęcie),
- **wiedzy** (np hasło)

Ad.7

**SO/IEC 27001** to norma, która została opracowana 14 października 2005 r. Jest ona specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność z którą będą wydawane certyfikaty.

W normie ISO/IEC 27001 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;

Ad.8

różnica jest taka że pełny audyt jest nadzbiorem audytu bezpieczeństwa.

Ad...

**klauzule tajemnicy państowej:**

tajność , ścisła tajność

Ad...

**Hoax**

jeden z kilku rodzajów *łańcuszków email*. Fałszywki to głupie żarty, przesyłane przez dowcipniów w formie ważnego ostrzeżenia przed groźnym, rozprzestrzeniającym się błyskawicznie wirusem, mającym, według opisu, bardzo destrukcyjne działanie, a informacja ta rzekomo pochodzi od producentów oprogramowania.

Ad...

**Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzecjalność

Ad...

**Na czym bazuje autoryzacja dostępu**

na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.

Add..

**Miara bezpieczeństwa w common criteria** (norma iso 15194 czy jakoś tak) - jest to poziom uzasadnionego zaufania.

## Zest. 11.

Zestaw C:

1. Ubezpieczenie zalicza sie do....

- kontroli ryzyka
- retencji ryzyka
- **transferu ryzyka**

2. Co sie dzieje z plikiem po usunieciu z dysku:

- wpis w \$MFT jest usuwany, dane zostaja
- **wpis w \$MFT zostaje, dane zostaja i zmieniaja sie dwie flagi**
- wpis w \$MFT jest usuwany, dane sa usuwane
- wpis w \$MFT zostaje, dane zostaja

3. W ktorym dokumencie opisano System zarzadzania bezpieczenstwem informacji:

- **ISO 27001**
- ISO 15408

4. Podpis cyfrowy zapewnia:

- **niezaprzecjalnosc, autentycznosc i integralnosc**

5. Minimalny zestaw wymagan na system zabezpieczeń:

- dywersyfikacja i spojnosc
- dywersyfikacja, niezaprzecjalnosc i organizacja wg zasady ochrony "w glab"
- **dywersyfikacja, niezaprzecjalnosc, spojnosc i organizacja wg zasady ochrony "w glab"**
- dywersyfikacja i organizacja wg zasady ochory "w glab" (chyba)

6. Zasada, zeby pracownik do wykonywania pracy mial tylko dostep do tych programow i uslug, ktorych potrzebuje, to:

- **zasada minimalnego srodowiska pracy**

- zasada wiedzy koniecznej
- zasada dwóch ludzi

7. Atrybuty informacji w kontekście bezpieczeństwa:

- **poufnosc, integralnosc, dostepnosc**

8. Costam o audycie bezpieczeństwa teleinformatycznego:

- **zawiera sie w audycie informatycznym**

9. Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania:

- minimalizujemy ryzyko
- minimalizujemy zagrożenia
- minimalizujemy podatności
- **minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia**

10. Dokument "Polityka bezpieczeństwa dla ..." powinien być:

- **jawny**

1. (dokładniej treści nie pamiętam, ale była dużo dłuższa) Jeśli wyślemy sygnał na port 80 sprawdzający czy jest otwarty i odpowiedź dostaniemy z flagą RST to znaczy, że port jest:  
- zamknięty
2. Jeśli uwierzytelniony użytkownik chce dostać się do pliku to proces logicznego sprawdzania czy użytkownik czegoś tam coś tam nazywa się:  
- Proces autoryzacji.

Rok 2009

1. Miara bezpieczeństwa w common criteria (norma iso 15194 czy jakoś tak) - jest to poziom uzasadnionego zaufania.
2. Atrybuty informacji - tajność , dostępność, integralność
3. Cechy podpisu elektronicznego - niesprzeczny, integralny i autentyczny
4. Zasada dostępu tylko do takich informacji przez pracownika , które mu są w tej chwili potrzebne to - zasada wiedzy koniecznej

5. Czy w prawie karnym jest paragraf za włamania komputerowe - Tak
  6. Jaka norma jest od Systemu zarządzania bezpieczeństwem - norma 270001 lub 27001 nie pamiętam
  7. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego - różnica jest taka że pełny audit jest nadzorem audytu bezpieczeństwa.
  8. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwa - tajność , ścisła tajność
  9. Jaki powinien być dokument "Planowania bezpieczeństwa dla ..." - powinien być jawnym.
  10. Na czym bazuje autoryzacja dostępu - na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.
- 
- 

1. Co zapewnia Common Criteria i standard ISO/IEC 15408 ?  
Odpowiedni poziom zaufania(odp. Ze słowem „zaufanie”)
2. Do czego wykorzystywany jest outsourcing?  
Transfer ryzyka
3. Metody uwierzytelniania pracowników  
weryfikacja przedmiotu posiadanego przez użytkownika (przepustka).  
weryfikacja cech fizycznych użytkownika (odcisk palca, oko, długość fallusa)  
weryfikacja wiedzy użytkownik (piny, hasła)
4. Co zapewnia podpis cyfrowy:  
Jednoznaczosc, autentycznoś...(odpowiedź z największa liczba wymienionych cech)
5. Czym rozni się audit informatyczny od audytu bezpieczeństwa  
Audyt bezpieczeństwa zawiera się w audycie informatycznym.
6. ) czy w polskim prawie jest paragraf dotyczący sankcji za włamania informatyczne?  
tak
7. "polityka bezpieczeństwa" jaka powinna mieć klauzule tajności?  
Jawna
8. w której normie jest mowa o wymaganiach dotyczących bezpieczeństwa teleinformatycznego  
norma 27001
9. Pytanie dotyczące podawania pracownikom informacji  
Odp. Zgodnie z zasadą wiedzy koniecznej
10. Atrybuty informacji związane z jej bezpieczeństwem  
Tajność, integralność, dostępność

### **1. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

**2. czego dotyczy norma ISO27001**

**>3. czy w polskim prawie karnym jest paragraf na włamania (?)**

TAK (Włamanie do systemu komputerowego jest aktem vandalizmu: Skrypt 96-99)

**4. jaki poziom ochrony powinien mieć dokument instrukcja bezpieczeństwa**

jawny

**5. jakie klauzule odpowiadają tajemnicy państowej**

tajność , ścisła tajność

**6. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi**

**informacje**

zasada wiedzy koniecznej ((??) Skrypt 113)

**7. hoax - co to jest**

(tu nie wiem jakie były możliwości, wg wikipedii hoax to mistyfikacja ☺)

**1. Miara bezpieczeństwa w common criteria (norma iso 15194 czy jakość tak) - jest to poziom uzasadnionego zaufania.**

**2. atrybuty informacji (Skrypt 12)**

Tajność – dostęp do określonych danych i informacji posiadają tylko uprawnione osoby

Integralność – dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji

Dostępność – dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika

**3. Cechy podpisu elektronicznego**

Integralność, Autentyczność, Niezaprzeczalność (Skrypt 124)

**4. Zasada dostępu tylko do takich informacji przez pracownika , które**

**mu są w tej chwili potrzebne to:**

zasada wiedzy koniecznej (Skrypt 113)

**5. Czy w prawie karnym jest paragraf za włamania komputerowe**

Tak (Skrypt 96 – 99)

**6. Jaka norma jest od Systemu zarządzania bezpieczeństwem**

norma ISO27001

**7. Różnica pomiędzy pełnym audytem informatycznym , a audytem bezpieczeństwa teleinformatycznego**

różnica jest taka że pełny audit jest nadzorem audytu bezpieczeństwa.

**8. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwową tajność , ścisła tajność**

**9. Jaki powinien być dokument "Planowania bezpieczeństwa dla ..."**

powinien być jawnym.

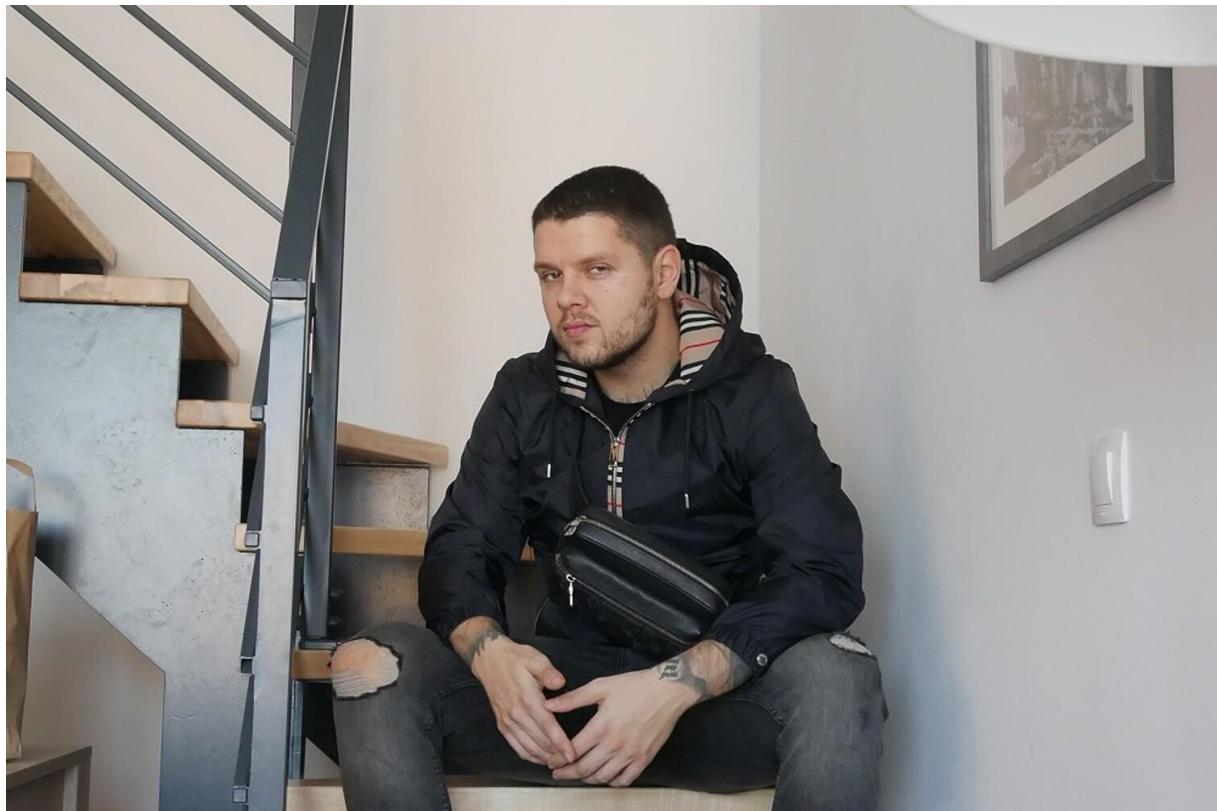
**10. Na czym bazuje autoryzacja dostępu**

na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy.

Dla testu B

1. atrybuty informacji: **(tajność, integralność, dostępność)**
2. czy w polskim prawie karnym jest paragraf na włamania **(tak)** (chyba par. 255k.k. <- poza konkurem)
3. jaki poziom ochrony powinien mieć dokument polityka bezpieczeństwa **(jawny)**
4. w teście B zad 1 coś z normą PN/ISO xxxx45 odpowiedź **a)** (najmniej pasująca)
5. jak nazywa się zasada zgodnie z którą ujawnia się pracownikowi informacje **(zasada wiedzy koniecznej)**
6. weryfikacja tożsamości użytkownika na podstawie **rzeczy** (np klucz), **cech fizycznych** (np odcisk palca, zdjęcie), **wiedzy** (np hasło)
7. było coś z normą PN/ISO 27001 ale nie pamiętam już co.
8. Nie pamiętam pytania, to jest konkluzja -> **Pełny audit informatyczny jest nadzorem audytu bezpieczeństwa teleinformatycznego**

## **BAZUNIA BETONIK PBI**



*Obraz 1. Największy bandit w Polsce*

*„Pa, jakie jaja; Manchester City*

*B do G znowu pije wódę, wyjebane mam na jakieś siki*

*Biggie mówił, nie ćpaj swojego tematu, chłopcze*

*Jestem hip-hop, a nie hiphopowcem”*

1. Miara bezpieczeństwa w common criteria: **jest to poziom uzasadnionego zaufania**
2. Atrybuty informacji: **tajność, dostępność, integralność**
3. Cechy podpisu elektronicznego: **niesprzeczny, integralny, autentyczny**
4. Zasada dostępu tylko do takich informacji przez pracownika, które mu są w danej chwili potrzebne to: **zasada wiedzy koniecznej**
5. Czy w prawie karnym jest paragraf za włamania komputerowe/informatyczne: **tak**
6. Jaka norma jest od systemu zarządzania bezpieczeństwem: **27001**
7. W której normie mowa jest o wymaganiach dot. bezp. teleinf.: **norma 27001**
8. Różnica między pełnym audytem informatycznym a audytem bezpieczeństwa teleinformatycznego: **pełny jest nadzorem audytu bezp. teleinformatycznego/audyt bezpieczeństwa teleinf. zawiera się w audycie pełnym**
9. Jakie etykiety ma wiadomość sklasyfikowana jako tajemnica państwową: **tajność, ścisła tajność**
10. Jakie klauzule odpowiadają tajemnicy służbowej: **poufne, zastrzeżone**
11. Jaki powinien być dokument „Polityka bezpieczeństwa dla...”: **jawny**
12. Jaki powinien być dokument instrukcja bezpieczeństwa: **niejawny/zastrzeżony/do użytku wewnętrznego**
13. Na czym bazuje autoryzacja dostępu: **na przedmiocie posiadanym przez osobę autoryzowaną, cechach fizycznych oraz jego wiedzy**
14. Co zapewnia Common Criteria i standard ISO/IEC 15408: **odpowiedni poziom zaufania**
15. Do czego wykorzystywany jest outsourcing: **transfer ryzyka**
16. Metody uwierzytelniania pracowników: **weryfikacja przedmiotu (przepustka), weryfikacja cech fizycznych (odcisk, oko, kutas), wiedza (hasło, pin)**
17. Co zapewnia podpis cyfrowy: **niezaprzecjalność, autentyczność, integralność (najwięcej odpowiedzi)**
18. W których systemach Windows domyślnie włączony jest dziennik zdarzeń: **vista + win7**
19. W którym systemie Windows było logowanie zdarzeń: **od 2000 w góre (2000, xp, 2003, 2008, vista, 7, itd.)**
20. Ile jest ‘well known’ portów: **1024**
21. Ubezpieczenie jest...: transferem ryzyka
22. Czy pliki są usuwane całkowicie z dysku: **wpis w \$MFT zostaje, dane zostają i zmieniają się dwie flagi**
23. Minimalny zestaw wymagań na system zabezpieczeń: **dywersyfikacja, niezaprzecjalność, spójność i organizacja według zasady ochrony „w głąb”**
24. Co nie jest plikiem systemowym NTFS: **\$Sector**

25. Czym jest hoax: **atak socjotechniczny/mistyfikacja/fałszywa informacja podana przez sieć, telefon, rozmowę mająca na celu zmuszenie odbierającego do konkretnego działania na korzyść osoby przekazującej fałszywą informację**
26. Co to jest SNORT: **IDS, IPS...**
27. Usługa kolokacji: **udostępnianie miejsca, własny sprzęt**
28. Czy zastosowanie profilu zaufanego ePUAP w kontaktach z administracją państwową jest równoważne, co do skutków prawnych, użyciu bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem: **tak**
29. Przygotowanie i wdrożenie planów zapewniania ciągłości działania w ramach postępowania z ryzykiem należy do: **kontrolowania ryzyka**
30. Audyt w zakresie bezpieczeństwa informacyjnego: **wymaga tzw. wzorca audytowego i niezależności podmiotu wykonującego audit**
31. Promieniowanie ujawniające: **jest promieniowaniem akustycznym i/lub elektromagnetycznym stanowiącym zagrożenie dla poufności i integralności informacji przetwarzanej w systemie komputerowym**
32. Steneografia: **metoda utajniania informacji**
33. RTA time actual: **chodziło o eksperymenty do wyznaczania czasu**
34. Backup w którym do jednego pełnego dopisuje się nowe dane/usuwa niepotrzebne: **różnicowy**
35. Czym jest UTM: **wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia**
36. Personal firewall: **aplikacja kontrolująca ruch z i do urządzenia (komputera)/filtracja pakietów**
37. Ochrona danych osobowych: **tylko dla żyjących**
38. Zasada ochrony w głęb: **jak przedostanie się przez zapory to napotyka kolejną**
39. Na czym polega hosting: **udostępnianie centrum danych i sprzętu**
40. Backup polegający na zapisie plików przez tydzień itp./klonowanie plików: **przyrostowy**
41. Zasada Kerchoffa: **klucz jest tajny a nie shaker**
42. „Zadanko ze od pon do cz o 18 jest backup niepełny a w piątek o 18 pełny i jak w czwartek o 17 50 sie zepsuje system to ile dysków potrzeba z backupem żeby odnowić system - **jeden backup = jeden dysk**”
43. Dokument polityka bezpieczeństwa powinien być dokumentem zawierającym: **zapis najważniejszych ogólnych zamiarów kierownictwa organizacji w zakresie bezpieczeństwa własnym i powierzonych informacji i jego deklaracje w stosunku do zapewnienia bezpieczeństwa**
44. Zgodnie z ustawą o ochronie informacji niejawnych informacje niejawne oznaczone są klauzulą: **ściśle tajne lub tajne lub poufne lub zastrzeżone**

45. Proces realizowany przez podsystem kontroli dostępu logicznego systemu komputerowego gdy uwierzytelniony użytkownik próbuje uzyskać dostęp do pliku nazywa się: **weryfikacja autoryzacji**
46. Za pomocą VPN nie da się zabezpieczyć: **dostępności**
47. Test penetracyjny to: **metoda zbierania informacji o badanym systemie**
48. Co to jest Recovery Point Object: **(jedyna odpowiedź w cudzysłowie)**
49. Na czym polega hosting: **udostępnianie danych i sprzętu**
50. Zasada, że pracownik do wykonywania pracy miał dostęp tylko do potrzebnych programów i usług: **zasada minimalnego środowiska pracy**
51. Poprzez sporządzenie i w razie potrzeby wdrożenie planu odzyskiwania: **minimalizujemy straty wynikłe z wykorzystania podatności przez zagrożenia**
52. W windows xp dzienniki są: **aplikacji, zabezpieczeń, system (domyślnie wyłączone)**
53. Kolejność wykonywania exploitu: **mfsconsole->mfsupdate->use exploit<nazwa>->RHOST<ip ofiary>->LHOST<ip intruza>->exploit**
54. Island hopping: atakowanie najsłabszego systemu i skakanie na inne