Na podstawie dostarczonych prezentacji, poniżej znajdują się opracowane odpowiedzi na zagadnienia zawarte w PDF "Zagadnienia_na_zaliczenie_BSK":

---

1. Wymień co najmniej 3 zasady cyberhigieny

- **Regularne aktualizacje**: Regularne aktualizowanie systemów i aplikacji w celu zabezpieczenia przed znanymi lukami bezpieczeństwa (źródło: W3 Basic security.ppt).

- **Silne hasła**: Tworzenie i używanie silnych, unikalnych haseł oraz ich regularna zmiana (źródło: W3 Basic security.ppt).

- **Używanie programów antywirusowych**: Instalacja i regularne aktualizowanie oprogramowania antywirusowego (źródło: W3 Basic security.ppt).

2. Co oznacza skrót TRANSEC?

TRANSEC (Transmission Security) to zabezpieczenie transmisji danych przed przechwyceniem i nieautoryzowanym dostępem za pomocą metod takich jak skokowe zmiany częstotliwości (Frequency Hopping) i rozpraszanie widma (Direct Sequence) (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

3. Co oznacza skrót COMSEC?

COMSEC (Communications Security) obejmuje metody ochrony poufności, integralności i dostępności komunikacji, w tym bezpieczeństwo kryptograficzne, bezpieczeństwo transmisji, bezpieczeństwo emisji i fizyczne bezpieczeństwo sprzętu oraz oprogramowania (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

4. Opisz AAA

AAA (Authentication, Authorization, and Accounting) to ramy dla inteligentnego kontrolowania dostępu do zasobów komputerowych, egzekwowania zasad, audytowania użytkowania oraz dostarczania informacji niezbędnych do wystawiania rachunków za usługi. Składa się z trzech komponentów:

- **Authentication (Uwierzytelnianie)**: Proces weryfikacji tożsamości użytkownika.

- **Authorization (Autoryzacja)**: Proces przyznawania uprawnień dostępu do zasobów.

- **Accounting (Rozliczalność)**: Monitorowanie i rejestrowanie aktywności użytkownika w systemie (źródło: W3 Basic security.ppt).

5. Opisz NAT

NAT (Network Address Translation) to technika, która umożliwia zmianę adresów IP w pakietach sieciowych. NAT jest używany do mapowania prywatnych adresów IP na publiczne adresy IP, co pozwala na ukrywanie prywatnej sieci przed publiczną siecią oraz na lepsze wykorzystanie dostępnych adresów IP. Dwa główne typy NAT to:

- **SNAT (Source NAT)**: Zmienia adres źródłowy pakietu.

- **DNAT (Destination NAT)**: Zmienia adres docelowy pakietu (źródło: W5 DHCP i NAT.ppt).

6. Do czego służy bit parzystości?

Bit parzystości jest używany do wykrywania błędów w transmisji danych. Jest dodawany do danych w celu umożliwienia prostego sprawdzenia, czy liczba bitów ustawionych na 1 w danym zbiorze jest parzysta czy nieparzysta (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

7. Jak działa CRC?

CRC (Cyclic Redundancy Check) to metoda wykrywania błędów w danych, która polega na obliczeniu wartości kontrolnej (CRC) na podstawie danych wejściowych i dołączeniu jej do danych. Przy odbiorze danych obliczana jest nowa wartość CRC i porównywana z wartością dołączoną do danych, co pozwala na wykrycie błędów (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

8. Do czego służy funkcja skrótu?

Funkcja skrótu przekształca dane wejściowe dowolnej długości w stałej długości skrót. Jest używana do zapewnienia integralności danych, ponieważ nawet najmniejsza zmiana w danych wejściowych powoduje dużą zmianę w skrócie (źródło: W6 Funkcja skrótu.pptx).

9. Jaką rolę odgrywa funkcja skrótu w podpisie elektronicznym?

W podpisie elektronicznym **funkcja skrótu** służy do wygenerowania unikalnego skrótu dokumentu, który jest następnie szyfrowany kluczem prywatnym nadawcy, tworząc podpis cyfrowy. Odbiorca może odszyfrować skrót kluczem publicznym nadawcy i porównać go z wygenerowanym skrótem dokumentu, aby zweryfikować integralność i autentyczność dokumentu (źródło: W6 Funkcja skrótu.pptx).

10. Jak się zabezpiecza login i hasło?

Loginy i hasła zabezpiecza się poprzez:

- **Hashowanie haseł**: Przechowywanie haseł w formie zaszyfrowanych skrótów zamiast tekstu jawnego.

- **Sól (Salt)**: Dodawanie losowej wartości do haseł przed ich hashowaniem, aby zwiększyć bezpieczeństwo.

- **Wieloczynnikowe uwierzytelnianie**: Używanie dodatkowych metod uwierzytelniania, takich jak SMS czy aplikacje uwierzytelniające (źródło: W3 Basic security.ppt).

11. Jaka długość hasła jest zalecana?

Zalecana długość hasła to co najmniej 12 znaków, zawierających kombinację liter, cyfr i znaków specjalnych (źródło: W3 Basic security.ppt).

12. Jaka długość skrótu jest zalecana?

Zalecana długość skrótu to co najmniej 256 bitów dla nowoczesnych zastosowań kryptograficznych (źródło: W6 Funkcja skrótu.pptx).

13. Opisz MD5

MD5 (Message-Digest Algorithm 5) to funkcja skrótu generująca 128-bitowy skrót. Jest obecnie uznawana za niebezpieczną ze względu na podatność na kolizje, co oznacza, że różne dane mogą generować ten sam skrót (źródło: W6 Funkcja skrótu.pptx).

14. Opisz SHA1

SHA1 (Secure Hash Algorithm 1) to funkcja skrótu generująca 160-bitowy skrót. Podobnie jak MD5, SHA1 jest uznawana za niewystarczająco bezpieczną, ponieważ możliwe jest znalezienie kolizji (źródło: W6 Funkcja skrótu.pptx).

15. Opisz SHA2

SHA2 to rodzina funkcji skrótu, która obejmuje SHA-224, SHA-256, SHA-384 i SHA-512. Funkcje te są bardziej bezpieczne niż MD5 i SHA1, oferując skróty o długościach odpowiednio 224, 256, 384 i 512 bitów (źródło: W6 Funkcja skrótu.pptx).

16. Opisz szyfrowanie symetryczne

Szyfrowanie symetryczne używa tego samego klucza do szyfrowania i deszyfrowania danych. Przykłady algorytmów symetrycznych to DES, 3DES i AES. Szyfrowanie symetryczne jest szybkie i efektywne, ale wymaga bezpiecznego zarządzania i dystrybucji kluczy (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

17. Opisz szyfrowanie asymetryczne

Szyfrowanie asymetryczne używa pary kluczy: publicznego do szyfrowania i prywatnego do deszyfrowania. Przykłady algorytmów asymetrycznych to RSA i DSA. Szyfrowanie asymetryczne eliminuje problem dystrybucji kluczy, ale jest wolniejsze niż symetryczne (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

18. Wyjaśnij różnice pomiędzy DES a AES

- **DES** (Data Encryption Standard): Stary algorytm szyfrowania symetrycznego używający 56-bitowego klucza. Ze względu na krótki klucz uznawany jest za niebezpieczny.

- **AES** (Advanced Encryption Standard): Nowszy algorytm szyfrowania symetrycznego używający kluczy o długościach 128, 192 i 256

bitów, oferujący wysoki poziom bezpieczeństwa i wydajność (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

19. Opisz RSA

RSA (Rivest-Shamir-Adleman) to algorytm szyfrowania asymetrycznego oparty na trudności faktoryzacji dużych liczb pierwszych. Jest szeroko stosowany do bezpiecznej wymiany kluczy i podpisów cyfrowych (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

20. Jakie są różnice w długości klucza pomiędzy szyfrowaniem symetrycznym a asymetrycznym?

Klucze w szyfrowaniu asymetrycznym muszą być znacznie dłuższe niż w szyfrowaniu symetrycznym, aby zapewnić podobny poziom bezpieczeństwa. Na przykład, klucz RSA 2048-bitowy jest uważany za bezpieczny w porównaniu do 256-bitowego klucza AES (źródło: W7 Szyfrowanie symetryczne a asymetryczne.pptx).

21. Do czego służy steganografia?

Steganografia to technika ukrywania tajnych informacji w innych, nieszkodliwych danych, takich jak obrazy, pliki audio czy tekst. Celem steganografii jest niewidoczne przesyłanie danych, tak aby nie wzbudzały one podejrzeń (źródło: W9 Steganografia.ppt).

22. Opisz blockchain

Blockchain to zdecentralizowana i rozproszona baza danych, w której dane są zapisywane w blokach połączonych kryptograficznie. Blockchain zapewnia wysoki poziom bezpieczeństwa, transparentności i niezmienności zapisanych danych (źródło: W11 blockchain.ppt).

23. Jakie są zastosowania blockchain'a?

Blockchain znajduje zastosowanie w wielu dziedzinach, takich jak:

- Kryptowaluty (np. Bitcoin)

- Inteligentne kontrakty

- Zarządzanie tożsamością

- Logistyka i łańcuch dostaw

- Głosowanie elektroniczne (źródło: W11 blockchain.ppt).

24. Opisz VPN

VPN (Virtual Private Network) to technologia umożliwiająca bezpieczne i szyfrowane połączenie tunelowe przez publiczne sieci, takie jak internet. VPN chroni prywatność użytkowników i zabezpiecza przesyłane dane (źródło: W3 Basic security.ppt).

25. Jak się zabezpiecza Bluetooth?

Bluetooth zabezpiecza się poprzez:

- Używanie kodów PIN do parowania urządzeń

- Wyłączanie Bluetooth, gdy nie jest używany

- Regularne aktualizacje oprogramowania urządzeń Bluetooth (źródło: Wykład 14-15 Układy bezprzewodowe.ppt).

26. Jak się zabezpiecza Wifi?

Zabezpieczenia WiFi obejmują:

- Używanie silnych haseł i najnowszych protokołów bezpieczeństwa, takich jak WPA3

- Ukrywanie SSID sieci

- Filtracja MAC, ograniczająca dostęp tylko do autoryzowanych urządzeń (źródło: Wykład 14-15 Układy bezprzewodowe.ppt).

27. Jak się zabezpiecza sieci 5G?

Zabezpieczenia sieci 5G obejmują zaawansowane metody szyfrowania, uwierzytelniania oraz segmentację sieci w celu minimalizacji ryzyka cyberataków (źródło: Wykład 14-15 Układy bezprzewodowe.ppt).

28. Jak się zabezpiecza sieci 6G?

Sieci 6G będą wymagały zaawansowanych zabezpieczeń, w tym sztucznej inteligencji do wykrywania zagrożeń, rozszerzonych mechanizmów kryptograficznych i fizycznych zabezpieczeń na poziomie sprzętowym (źródło: Wykład 14-15 Układy bezprzewodowe.ppt).

29. Co obejmuje bezpieczeństwo strony WWW od strony projektanta?

Bezpieczeństwo od strony projektanta obejmuje:

- Walidację danych wejściowych w celu zapobiegania atakom typu SQL Injection i XSS

- Używanie bezpiecznych protokołów komunikacyjnych, takich jak HTTPS

- Ochronę przed atakami CSRF (Cross-Site Request Forgery) (źródło: W8 Powtórzenie o szyfrowaniu.pptx).

30. Co obejmuje bezpieczeństwo strony WWW od strony administratora?

Bezpieczeństwo od strony administratora obejmuje:

- Regularne aktualizacje oprogramowania serwera i aplikacji

- Monitorowanie logów serwera w celu wykrywania podejrzanej aktywności

- Zarządzanie uprawnieniami użytkowników, aby zapewnić dostęp tylko autoryzowanym osobom (źródło: W8 Powtórzenie o szyfrowaniu.pptx).

Generated by GPT-4o