

Spis treści

Wstęp	5
1. Podstawowe informacje o bezpieczeństwie IT	11
1.1. Co to jest bezpieczeństwo IT?	13
1.2. Komputery typu desktop	15
1.2.1. Windows	15
1.2.2. OS X	19
1.2.3. Linux	20
1.3. Smartfony i tablety	21
1.3.1. iOS	22
1.3.2. Android	23
1.3.3. Windows Phone	23
1.4. Zadania do rozwiązania	24
2. Bezpieczeństwo komputera osobistego	27
2.1. Rodzaje złośliwego oprogramowania	29
2.1.1. Wirusy	30
2.1.2. Robaki	34
2.1.3. Trojany	35
2.1.4. Rootkity	36
2.2. Zagrożenia w sieci, konsekwencje niedostatecznych zabezpieczeń	37
2.3. Zdroworozsądkowe zapobieganie atakom złośliwego oprogramowania	40
2.4. Popularne programy antywirusowe i ich konfiguracja na potrzeby komputera osobistego	41
2.4.1. Co to są programy antywirusowe?	41
2.4.2. Konfiguracja popularnych programów antywirusowych	43
2.4.3. Popularne programy antywirusowe	43
2.5. Zadania do rozwiązania	48
3. Bezpieczeństwo w sieci	49
3.1. Sieci komputerowe	51
3.1.1. Przesyłanie danych w sieciach komputerowych	52
3.1.2. Zabezpieczenie przesyłania danych protokołem TLS	54
3.1.3. VPN	55
3.2. Sprzęt służący bezpieczeństwu	57
3.2.1. Routery	57
3.2.2. Sprzętowe moduły bezpieczeństwa	59

3.3. Bezpieczeństwo elementów sieci.....	61
3.3.1. Włamania i inne ataki.....	61
3.3.2. Konfigurowanie bezpiecznej sieci.....	62
3.3.3. Zapora sieciowa.....	65
3.4. Zadania do rozwiązania.....	68
4. Backup podstawą bezpieczeństwa.....	69
4.1. Zagrożenia utratą danych.....	71
4.2. Przechowywanie i archiwizowanie danych.....	72
4.2.1. Kompresja i deduplikacja.....	73
4.2.2. Sprzęt używany do archiwizacji.....	75
4.3. Podstawowa wiedza o backupie.....	77
4.4. Modele przechowywania danych.....	78
4.4.1. Okno backupowe, przepustowość i inne ograniczenia w procesie tworzenia kopii zapasowych danych.....	79
4.4.2. Nośniki dla backupu danych.....	79
4.5. Zadania do rozwiązania.....	82
5. Bezpieczeństwo IT a praca w województwie wielkopolskim.....	83
Zakończenie.....	87
Bibliografia.....	91
Źródła internetowe.....	93