

Spis treści

<b>Przedmowa</b>	<b>9</b>
<b>Wprowadzenie</b>	<b>11</b>
<b>1. INFORMACJE</b>	<b>14</b>
1.1. Zasady przetwarzania informacji	14
1.2. Klasyfikacja informacji	15
1.3. Postępowanie z informacjami	17
<b>2. OGÓLNY MODEL BEZPIECZEŃSTWA INFORMACJI</b>	<b>20</b>
2.1. Model znormalizowany	20
2.2. Podstawy metodyczne	21
2.3. Klasy bezpieczeństwa systemów informatycznych	23
<b>3. ZARZĄDZANIE RYZYKIEM</b>	<b>25</b>
3.1. Ryzyko	25
3.2. Proces zarządzania ryzykiem	25
3.3. Ustanowienie kontekstu	28
3.4. Zakres procesu zarządzania ryzykiem	30
3.5. Szacowanie ryzyka	32
3.6. Postępowanie z ryzykiem	38
3.7. Akceptowanie ryzyka	40
3.8. Monitoring i przegląd ryzyka	41
<b>4. ZAGROŻENIA</b>	<b>43</b>
4.1. Identyfikacja zagrożeń	43
4.2. Nieobliczalne oprogramowanie	45
4.3. Ewolucja zagrożeń	47
4.3.1. Ataki ukierunkowane	47
4.3.2. Podatność Internetu Rzeczy (IoT)	50
4.3.3. Oprogramowanie ransomware	52
<b>5. BEZPIECZEŃSTWO SYSTEMÓW OPERACYJNYCH</b>	<b>55</b>
5.1. Podstawy systemów operacyjnych	55
5.2. Zagrożenia dla systemów operacyjnych i sposoby ochrony	57
5.2.1. Ataki na systemy WINDOWS i metody przeciwdziałania	57
5.2.2. Ataki na systemy UNIX	59
<b>6. BEZPIECZEŃSTWO SIECI</b>	<b>67</b>
6.1. Sieć informatyczna	67

6.2. Mechanizmy bezpieczeństwa usług sieciowych	67
6.3. Detekcja	68
6.4. Podatności w zabezpieczeniach sieci	69
6.5. Zarządzanie bezpieczeństwem sieci	72
<b>7. ZAGROŻENIA DLA APLIKACJI WEBOWYCH I ŚRODKI PRZECIWDZIAŁANIA</b>	<b>76</b>
7.1. Ataki na serwery aplikacji	76
7.2. Ataki na aplikacje webowe	78
<b>8. KONTROLA DOSTĘPU</b>	<b>82</b>
8.1. Kryteria dostępu	82
8.2. Usługi sieciowe	83
8.3. Dane wrażliwe	86
8.4. Urządzenia mobilne	86
8.5. System kontroli dostępu	87
<b>9. KRYPTOGRAFIA</b>	<b>89</b>
<b>10. ZARZĄDZANIE BEZPIECZEŃSTWEM EKSPLOATACJI</b>	<b>93</b>
10.1. Zasady bezpiecznej eksploatacji	93
10.2. Integralność oprogramowania	94
10.3. Kopie zapasowe	95
10.4. Ujawnianie informacji	96
10.5. Transakcje elektroniczne	97
10.6. Nowe protokoły komunikacyjne	99
10.7. Monitorowanie zdarzeń	100
10.8. Zarządzanie podatnościami technicznymi	101
10.9. Serwis systemów informatycznych	102
<b>11. ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA</b>	<b>104</b>
11.1. Zasady podstawowe	104
11.2. Obsługa zdarzeń i incydentów bezpieczeństwa	105
11.3. Metodologia zarządzania incydentami bezpieczeństwa	108
<b>12. KRYTERIA WYBORU ZABEZPIECZEŃ</b>	<b>111</b>
12.1. Zasady ogólne	111
12.2. Polityka dotycząca haseł	112
12.3. Wytyczne dotyczące różnych platform technologicznych	115
12.4. Przetwarzanie transakcyjne	117
12.5. Technologie biometryczne	118
<b>13. WDRAŻANIE SYSTEMÓW INFORMATYCZNYCH</b>	<b>121</b>
13.1. Metodologia projektowania systemów informatycznych	121
13.2. Błędy programistyczne	122
13.3. Projektowanie zabezpieczeń	128
13.4. Zasady bezpiecznego programowania	129

<b>14. POMIARY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH</b>	<b>132</b>
14.1. Problem badawczy	132
14.2. Procesy pomiarowe	132
14.3. Model pomiarowy	134
14.4. Wskaźniki pomiarowe	135
14.5. Ocena skuteczności zabezpieczeń	136
<b>15. METODOLOGIA TESTÓW BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH</b>	<b>138</b>
15.1. Testy bezpieczeństwa	138
15.2. Testy penetracyjne	139
15.3. Zakres przeprowadzenia testu penetracyjnego	140
15.4. Etapy testów penetracyjnych	142
15.5. Metodyka OWASP Top 10	144
15.6. Inne metodyki	147
15.7. Narzędzia do prowadzenie testów	150
<b>16. AUDYT BEZPIECZEŃSTWA</b>	<b>155</b>
16.1. Zasady ogólne	155
16.2. Metodyka audytu według norm międzynarodowych	156
16.3. Oprogramowanie klasy SIEM	157
16.4. Raport z audytu bezpieczeństwa	159
<b>17. PODSUMOWANIE</b>	<b>161</b>
<b>BIBLIOGRAFIA</b>	<b>164</b>
<b>Załącznik A. RAPORT Z TESTU PENETRACYJNEGO</b>	<b>168</b>
<b>Załącznik B. METODY TESTOWANIA ZABEZPIECZEŃ</b>	<b>183</b>