

**Obsah:**

<b>PREDSLOV</b> .....	<b>9</b>
ZOZNAM POUŽÍVANÝCH SKRATIEK .....	11
ZOZNAM OBRÁZKOV .....	13
ZOZNAM TABULIEK.....	13
<b>1 ÚVOD</b> .....	<b>15</b>
1.1 POUŽITÉ MATERIÁLY .....	17
1.11 Právne predpisy .....	17
1.12 Medzinárodné normy.....	17
1.13 Publikácie a monografie .....	17
1.14 Príspevky na semináre a konferencie.....	17
1.15 Firemné metodiky a výskumné správy.....	18
1.2 VYSVETLENIE VYBRANÝCH POJMOV.....	22
<b>2 VZŤAHY MEDZI BEZPEČNOSTNÝMI PRVKAMI</b> .....	<b>29</b>
2.1 AKTÍVA.....	31
2.11 Výpočet odvodených hodnôt aktív .....	32
2.2 HROZBY .....	33
2.21 Najčastejšie hrozby pre informačnú bezpečnosť .....	38
2.22 Hrozby pre dôvernosť.....	39
2.23 Hrozby pre dostupnosť.....	42
2.24 Hrozby pre integritu.....	51
2.25 Hrozby pre počítačové siete.....	57
2.3 ZRANITEĽNOSŤ.....	61
2.31 Príklady zraniteľností vybraných typov aktív.....	61
2.4 DOPAD.....	66
2.41 Príklady dopadov.....	66
2.5 RIZIKO .....	69
2.51 Zostatkové riziko .....	69
2.6 BEZPEČNOSTNÉ OPATRENIA.....	70
2.61 Všeobecne použiteľné opatrenia.....	73
2.62 Príklady bezpečnostných opatrení pre počítače.....	74
2.63 Príklady bezpečnostných opatrení pre servery.....	76
2.64 Príklady bezpečnostných opatrení pre aktívne sieťové prvky.....	78
2.65 Príklady bezpečnostných opatrení pre lokalitu .....	81
2.66 Príklady bezpečnostných opatrení pre budovu.....	83
2.67 Príklady bezpečnostných opatrení pre kanceláriu .....	85
2.68 Príklady bezpečnostných opatrení pre ošetrovanie bezpečnostných incidentov .....	87
2.69 Príklady bezpečnostných opatrení pre antivírusovú ochranu .....	88
2.6.10 Príklady bezpečnostných opatrení pre udržanie kontinuity činnosti .....	89
2.6.11 Typ účinku a sila bezpečnostných opatrení .....	91
2.7 OBMEDZENIA.....	95
<b>3 ANALÝZA A RIADENIE RIZÍK INFORMAČNEJ BEZPEČNOSTI</b> .....	<b>97</b>
3.1 ANALÝZA RIZÍK .....	97
3.1.1 Stratégie analýzy rizík.....	97
3.2 ZÁKLADNÝ PRÍSTUP.....	99
3.2.1 Neformálny prístup.....	100
3.2.2 Detailná analýza rizík .....	101
3.2.3 Kombinovaný prístup .....	102
3.2.4 Riadenie rizík .....	103
3.2.5 Opatrenia pre bezpečnosť .....	106
3.2.6 Akceptácia zostatkových rizík.....	106
<b>4 METODIKA ANALÝZY RIZÍK INFORMAČNEJ BEZPEČNOSTI</b> .....	<b>107</b>
4.1 PONÍMANIE METODIKY ANALÝZY A RIADENIA RIZÍK.....	107
4.2 MATICA S PREDDEFINOVANÝMI HODNOTAMI .....	109
4.3 ZORADENIE HROZIEB PODĽA MIER RIZIKA .....	113

4.4	STANOVENIE HODNÔT FREKVENCIE A MOŽNEJ ŠKODY VYPLÝVAJUJEJ Z RIZÍK .....	114
4.5	ROZLIŠENIE MEDZI TOLEROVATEĽNÝMI A NETOLEROVATEĽNÝMI RIZIKAMI .....	116
4.6	ZHRNUTIE K UVÁDZANÝM METODIKÁM.....	117
<b>5</b>	<b>NORMA ISO/IEC 27005.....</b>	<b>119</b>
5.1	ZÁKLADNÉ INFORMÁCIE .....	121
5.2	ZLOŽENIE PROCESU RIADENIA RIZÍK INFORMAČNEJ BEZPEČNOSTI .....	121
5.3	VYTvoreNIE KONTEXTU PROCESU RIADENIA RIZÍK INFORMAČNEJ BEZPEČNOSTI.....	123
5.3.1	<i>Pristup k riadeniu rizík.....</i>	<i>123</i>
5.3.2	<i>Organizačné predpoklady na riadenie rizík.....</i>	<i>125</i>
5.4	OHODNOCOVANIE RIZIKA INFORMAČNEJ BEZPEČNOSTI .....	125
5.4.1	<i>Metodiky odhadu rizika.....</i>	<i>125</i>
5.4.1.1	<i>Kvalitatívny odhad rizika.....</i>	<i>126</i>
5.4.1.2	<i>Kvantitatívny odhad rizika.....</i>	<i>126</i>
5.5	OŠETROVANIE RIZIKA INFORMAČNEJ BEZPEČNOSTI .....	127
5.6	AKCEPTÁCIA RIZIKA INFORMAČNEJ BEZPEČNOSTI .....	128
5.7	OZNAMOVANIE RIZIKA INFORMAČNEJ BEZPEČNOSTI .....	128
5.8	MONITOROVANIE A PRESKÚVANIE RIZIKA INFORMAČNEJ BEZPEČNOSTI.....	129
5.9	POSÚDENIE PRÍNOSU NOVEJ NORMY .....	129
<b>6</b>	<b>NÁSTROJE NA PODPORU ANALÝZY RIZÍK.....</b>	<b>131</b>
6.1	ENISA – INVENTÁR NÁSTROJOV.....	131
6.2	CALLIO SECURA 17799 .....	136
6.3	CRAMM.....	137
6.4	COBRA.....	138
6.5	RISKWATCH .....	140
<b>7</b>	<b>VZŤAH ANALÝZY RIZÍK IS A ISMS .....</b>	<b>141</b>
<b>8</b>	<b>ANALÝZA A RIADENIE RIZÍK PODĽA NORMY ISO/IEC 27001.....</b>	<b>143</b>
8.1	POŽIADAVKY NA ANALÝZU A RIADENIE RIZÍK INFORMAČNEJ BEZPEČNOSTI .....	143
8.2	ZHRNUTIE A INTERPRETOVANIE POŽIADAVIEK .....	148
8.3	URČENIE KRITÉRIÁ NA AKCEPTOVANIE ZOSTATKOVÝCH RIZÍK.....	160
8.4	PRESKÚVANIE A OHODNOCOVANIE ZOSTATKOVÝCH RIZÍK .....	161
8.4.1	<i>Vstupné zostatkové riziká.....</i>	<i>162</i>
8.4.2	<i>Požadované zostatkové riziká.....</i>	<i>162</i>
8.4.3	<i>Reálne zostatkové riziká po implementácii bezpečnostných opatrení.....</i>	<i>166</i>
8.4.4	<i>Preskúvanie zostatkových rizík.....</i>	<i>167</i>
8.4.5	<i>Zostatkové riziká ako súčasť prevádzkových a strategických rizík organizácie.....</i>	<i>175</i>
8.5	OPAKOVANÁ AR SO ZOHLEDNENÍM VPLYVU BEZPEČNOSTNÝCH OPATRENÍ REALIZOVANÝCH V PRAXI 177	
8.6	MERANIE EFEKTIVNOSTI A ÚČINNOSTI OPATRENÍ .....	177
8.6.1	<i>Meranie efektívnosti a účinnosti opatrení prostredníctvom dosahovaných zostatkových rizík ...</i>	<i>177</i>
8.6.2	<i>Meranie efektívnosti a účinnosti fungovania bezpečnostných opatrení v praxi .....</i>	<i>178</i>
8.7	MERANIE PROCESOV ISMS.....	178
8.8	MERANIE CIEĽOV RIADENIA INFORMAČNEJ BEZPEČNOSTI.....	179
<b>9</b>	<b>ANALÝZA A RIADENIE RIZÍK PODĽA BEZPEČNOSTNÝCH ŠTANDARDOV PRE ISVS....</b>	<b>181</b>
9.1	VYBRANÉ PRÁVNE PREDPISY SR PRE RIADENIE INFORMAČNEJ BEZPEČNOSTI .....	181
9.1.1	<i>Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy ...</i>	<i>182</i>
9.1.2	<i>Zákon č. 275 / 2006 Z.z. o informačných systémoch verejnej správy.....</i>	<i>183</i>
9.1.3	<i>Výnos MF SR o štandardoch pre ISVS.....</i>	<i>186</i>
9.1.4	<i>Zákon č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov 190</i>	
9.1.5	<i>Zákon č. 300/2005 Z.z. Trestný zákon.....</i>	<i>192</i>
9.1.6	<i>Zhrnutie k spomínaným právnym predpisom .....</i>	<i>196</i>
9.2	POŽIADAVKY NA ANALÝZU A RIADENIE RIZÍK POVINNÝCH OSÔB.....	198
9.3	ZHRNUTIE A INTERPRETOVANIE POŽIADAVIEK .....	198
9.4	POROVNANIE POŽIADAVIEK NA ANALÝZU A RIADENIE RIZÍK PODĽA BEZPEČNOSTNÝCH STANDARDOV PRE ISVS A NORMY ISO/IEC 27001 .....	202

<b>10</b>	<b>ZÁRUKY ZA INFORMAČNÚ BEZPEČNOSŤ.....</b>	<b>219</b>
10.1	POŽADOVANÁ INFORMAČNÁ BEZPEČNOSŤ.....	219
10.2	ZÍSKANIE A OVEROVANIE ZÁRUK.....	222
<b>11</b>	<b>ZÁVER.....</b>	<b>229</b>
<b>12</b>	<b>LITERATÚRA.....</b>	<b>231</b>
12.1	MONOGRAFIE A PUBLIKÁCIE.....	231
12.2	ČLÁNKY.....	233
12.3	FIREMNÉ METODIKY.....	234
12.4	ZÁKONY A VYHLÁŠKY.....	234
12.5	ISO NORMY.....	235
12.6	ISO/IEC NORMY.....	235
12.7	STN NORMY.....	236
<b>13</b>	<b>SUMMARY.....</b>	<b>237</b>