

# CONTENT

<b>Introduction</b> .....	<b>5</b>
<b>1 The State of Affairs of the Analyzed Issue at Home and Abroad</b> .....	<b>7</b>
1.1 The Delineation of the Basic Terminological Apparatus and the Terminological Interrelationships .....	7
1.1.1 Definition of the Term “Security” .....	8
1.2 Information Security (IS) .....	9
1.2.1 Information System, Security of Information Systems .....	13
1.2.2 Communication System (CS), the Security of Communication Systems .....	15
1.3 Small and Medium-sized Enterprises (SMEs) .....	27
1.4 Information Security in the SR.....	30
1.5 Information Security in the World .....	35
1.6 Development of Norms and Standards for the Security of Information and Communication Systems.....	38
1.7 Standards of the ISO / IEC 27000 Series Valid and Issued in the SR .....	42
1.8 Basic Principles of Information Security Solutions .....	44
1.8.1 Information Security Study .....	45
1.8.2 Security Policy .....	45
1.8.3 Security Project .....	47
1.8.4 Risk Analysis.....	48
1.9 Threats to the Information System .....	48
1.9.1 Human Factor .....	48
1.9.2 Classification of Cybercrime.....	49
1.9.3 Types of Cybercrime .....	50
1.9.4 Criminal Liability in Cybercrime .....	53
1.9.5 Non-influenceable Natural Threats .....	54
1.9.6 Technical Failure of the Information System.....	56
1.10 Selected Security Tools of the Information System.....	56
1.10.1 Firewall.....	56
1.10.2 Antivirus Programs .....	58
1.10.3 Penetration Testing.....	58
1.10.4 E-mail Content Monitoring .....	59
1.10.5 Employee Internet Monitoring .....	60
1.10.6 Personnel Policy of an Organization as an Information Security Tool.....	61
1.10.7 Other Measures .....	61
<b>2 Aims of the Research and Methods Used</b> .....	<b>62</b>
<b>3 Methodology and Research Methods</b> .....	<b>64</b>
<b>4 Results of the Survey</b> .....	<b>66</b>
4.1 Sample of Respondents .....	66
4.2 The Importance of Information Security.....	69
4.3 Circumstances Influencing the Enforcement of Information Security.....	70
4.3.1 Internet and E-communications .....	73
4.3.2 Antivirus Measures .....	78

4.4	Personnel Security .....	79
4.5	Security Policy and the Use of IS / IT Standards and Norms .....	81
4.6	Security Incidents and their Consequences .....	83
4.7	Electronic Signature .....	86
4.8	Security Solutions .....	87
	4.8.1 Physical Security .....	90
	4.8.2 Backup of Documentation.....	92
	4.8.3 Access Rights and Passwords .....	93
	4.8.4 Protection of Personal Data and Classified Information.....	96
	4.8.5 Recovery and Functionality Plan .....	98
4.9	Information Security in Slovakia from the Point of View of Enterprises .....	100
<b>5</b>	<b>Factors Influencing Information Security in Enterprises in the Slovak Republic</b> .....	<b>102</b>
5.1	Comparison of the State of Information Security of Small and Medium-Sized Enterprises with the State of Information Security in Large Enterprises.....	102
5.2	Comparison of the State of Information Security According to another Characteristic of the Enterprise .....	107
5.3	Security Management Models.....	108
	5.3.1 Security Assessment Model Based on Potential Threats .....	108
	5.3.2 Model of Security Assessment Based on Weaknesses of the Information System .....	109
	5.3.3 Impact-based Safety Assessment Model.....	110
5.4	Security Categories Based on Impacts - Proposal.....	111
	<b>Conclusion.....</b>	<b>114</b>
	<b>Resources.....</b>	<b>117</b>