

Contents

1	Introduction.....	1
	References.....	4
2	Fields of Application, Methods of and Current Trends in Information Management	5
2.1	Concept of Information: Development	5
2.2	Information Management Process in a Commercial Organisation	7
2.3	Role of the Organisational Structure in the Information Management Process Within a Business Organisation.....	10
	References.....	12
3	Types of Information Splitting and Sharing Techniques	15
3.1	Mathematical Fundamentals of Information Sharing Techniques	17
3.1.1	Mathematical Arithmetic and Congruencies.....	17
3.1.2	Calculating the Converse in Modular Arithmetic	19
3.2	Simple Information Splitting Methods	21
3.2.1	Shamir's Algorithm.....	21
3.2.2	Tang's Algorithm.....	22
3.3	Cryptographic Threshold Schemes	24
3.3.1	Vector Algorithm.....	25
3.3.2	Asmuth-Bloom Algorithm	27
3.3.3	Karnin-Greene-Hellman Algorithm	29
3.4	Protocols of Information Sharing for Secret Distribution.....	29
3.4.1	Information Sharing Without the Involvement of a Trusted Person.....	29
3.4.2	Message Sharing Without Disclosing Own Parts.....	30
3.4.3	Message Sharing with Disclosure Prevention.....	30
3.4.4	Message Sharing with Cheaters	30

3.4.5	Sharing Messages with Verification	32
3.4.6	Sharing a Message with a Share Withdrawn.....	33
3.5	Examples of Secret Sharing and Systems Executing It	34
3.5.1	An Example System Running Secret Sharing Algorithms	34
3.5.2	Example of Sharing a Secret in the Form of an Image.....	36
	References.....	37
4	Model of Multilevel Information Splitting and Management in an Organization	39
4.1	Description of Algorithms for Multilevel Information Splitting in Layered and Hierarchical Structures.....	39
4.1.1	Layered Splitting	40
4.1.2	Hierarchical Splitting	42
4.2	Presentation of Organisational Structure Types.....	43
4.3	Application of Information Sharing Methods in Particular Organizational Structures	45
4.4	An Illustrative Example of Information Sharing in Layered and Hierarchical Structures.....	48
	References.....	51
5	Proposition of Sharing Techniques Based on the Mathematical Linguistic Approach	53
5.1	Description of Mathematical Linguistic Methods	53
5.2	Idea of Linguistic Threshold Schemes.....	56
5.2.1	Multilayer Information Splitting Based on Bits Notation	57
5.2.2	A Multi-level Information Splitting Algorithm Based on Two-bit Notation	60
5.2.3	Multilayer Information Splitting Based on n-Bit Block Notation	61
5.3	An Example of Using Linguistic Threshold Schemes	64
5.3.1	Secret Sharing	64
5.3.2	Secret Restoration	68
	References.....	69
6	Methodological Aspects of Information Sharing and Management in Organizations	71
6.1	Designing Information Flow in Management Information Systems	71
6.2	Methods of Information Sharing in a Commercial Organization.....	77
6.2.1	Information Division in Linear Structures	78
6.2.2	Information Division in Functional Structures.....	81
6.2.3	Information Division in Line-and-Staff Structures	84

6.2.4	Information Splitting in Integrated Division Structures	87
6.2.5	Information Division in Divisional Structures	90
6.2.6	Information Division in Collective Structures	93
6.2.7	Information Division in Complex Structures	96
6.2.8	Information Division in Project Structures	100
6.2.9	Information Division in Matrix Structures	102
6.2.10	Information Division in Mixed Structures	106
6.2.11	Information Division in Process Structures	109
6.2.12	Information Division in Network Structures	112
6.2.13	Information Division in Virtual Structures	112
6.3	Universal and Specific Models of Information Sharing Systems	116
6.4	An Illustrative Example of Information Sharing in Layered and Hierarchical Structures Using the Linguistic Approach	119
	References	121
7	Features of Linguistic Threshold Schemes	125
	References	128
8	Summary	131
	References	133
	Index	135

Secure Information Management Using Linguistic
Threshold Approach

Ogiela, M.R.; Ogiela, U.

2014, XIII, 136 p.,

ISBN: 978-1-4471-5016-9