

Contents

Nomenclature	5
List of figures.....	7
List of tables.....	9
Introduction.....	11
1 Analysis and issues of the current state.....	13
1.1 Issues of Security of IoT Devices	14
1.2 Attacks on industrial production systems.....	14
1.3 Vulnerability statistics of IoT devices.....	16
1.4 Overview of cyber security measures research	18
2 Design Theory and Technology	20
2.1 Industry 4.0.....	20
2.1.1 <i>Technological assumptions</i>	21
2.1.2 <i>Requirements of safety and reliability</i>	22
2.1.3 <i>Standards of Industry 4.0</i>	23
2.2 Internet of Things (IoT)	25
2.2.1 <i>Origin and current state</i>	25
2.2.2 <i>Requirements on IoT</i>	26
2.2.3 <i>Environment characteristics</i>	26
2.2.4 <i>The use of IoT</i>	27
2.2.5 <i>The Industrial IoT (IIoT)</i>	28
2.2.6 <i>The consumer IoT</i>	29
2.2.7 <i>Ways of communication within the IoT</i>	30
2.3 The IoT security	31
2.3.1 <i>Threats of the Internet</i>	31
2.3.2 <i>Cyber threats</i>	32
2.3.3 <i>DDoS and DRDoS attacks</i>	33
2.3.4 <i>The types of DDoS and DRDoS attacks</i>	34
2.3.5 <i>General principles of security against DDoS attacks</i>	36
3 Testing security of real production infrastructure with integrated IoT devices.....	41
3.1 Real production infrastructure.....	41
3.1.1 <i>Production line</i>	43

3.1.2	<i>Communication of the production line</i>	44
3.1.3	<i>IoT Fibaro security system</i>	46
3.1.4	<i>IoT Honeywell thermostat</i>	47
3.2	Testing of production infrastructure in the form of DDoS attacks.....	47
3.2.1	<i>Scenarios of attacks</i>	48
3.2.2	<i>The first attack scenario</i>	48
3.2.3	<i>The second attack scenario</i>	50
3.2.4	<i>The third attack scenario</i>	51
3.2.5	<i>The fourth attack scenario</i>	53
3.2.6	<i>The fifth attack scenario</i>	54
3.2.7	<i>Overview of attack scenarios</i>	56
3.3	Impacts of DDoS and DRDoS attacks on the production process....	57
4	Design of security solutions for production infrastructures with integrated IoT devices	64
4.1	Basic recommendations for securing IoT devices.....	64
4.2	Suggested solutions to mitigate the effects of DDoS attacks.....	65
4.3	Static security strategy using a transparent firewall bridge.....	65
4.3.1	<i>Monitoring of network traffic by using a NetFlow</i>	68
4.4	Dynamic security strategy.....	71
4.4.1	<i>Acquisition of data communication</i>	72
4.4.2	<i>Machine learning</i>	74
4.4.3	<i>Data transformation for machine learning</i>	75
4.4.4	<i>Neural network</i>	75
4.4.5	<i>Firewall security</i>	80
5	Verification and evaluation of proposed solutions	82
5.1	Verification and evaluation of static security.....	83
5.2	Verification and evaluation of dynamic security	85
5.3	Overall summary and comparison of the proposed solutions	91
	Summary	94
	References	95
	About the Author	106
	Subject Index	107