Markov model of the Smart Business Center wired network considering attacks on software and hardware components

Vyacheslav Kharchenko
Department of Computer Systems and Networks
National Aerospace University "KhAI"
Kharkiv, Ukraine

Maryna Kolisnyk
Department of automation and control in the technical systems
National Technical University " KPI",
Kharkiv, Ukraine

Iryna Piskachova
Department of Computer Science and Control System, Ukrainian State University of the Railway Transport,
Kharkiv, Ukraine

Nikolaos Bardis
Department of Mathematics & Engineering Sciences
Hellenic Military Academy
Vari - 16673, Greece

Abstract— Internet of Things covers the increasing number spheres of human activity. Create protected from malicious impacts smart business centers (SBC) is a challenge, and includes aspects of safety at every level of SBC architecture. The article analyzes some of the problems arising from the creation and operation of SBC wireline networks. In the analysis of dependability IoT system must take into account the reliability and security of the system at several levels SBC architecture: sensors level, connection level (link, router, switch), the level of software / hardware components of the server as a network management device, the level of the entire SBC system. To account for the impact of malicious actions on major hardware and software components of the SBC system is represented by a Markov model, which takes into account the specifications of typical network components SBC with the presence of software vulnerabilities when exposed to hacker attacks, which takes into account the attacks rate on software vulnerabilities and the hardware and as the values of the rate of their recovery after the attacks derived from the analysis of statistical data. The analysis of the simulation results gives the opportunity to identify ways to improve the reliability and safety of the SBC.

Keywords—Internet of Things; smart business center; network; security; reliability; availability function.

I. INTRODUCTION

IoT is a paradigm that involves ubiquitous presence in the environment of different things / objects that are using wireless and wire networks and unique addressing scheme are able to interact with each other and with other things / objects to create new applications / services to achieve purposes [1, 2]. They are becoming more diverse, and embedding in the micro- and nano-scale physical systems, not only to create a distributed cybernetic system, but also a new concept for computing and communications paradigm of creative self-organized spaces that may occur in real time. IoT technology - a concept combining sensor networks, of machine-to-machine solutions (M2M, applications to process data from sensors, mobile electronic devices, and cloud infrastructure).

IoT represents the next wave of the Internet: Internet of Content (Distribution/Access) include Email; Information; Entertainment; Internet of Service (Participation/Trade) include E-commerce; Productivity tools; Integrated chains Internet of People (Collaboration/Share); Voice and video collaboration; Social media and docs; Web logs/boards; Internet of Things (Integration/Control) unites Indexing and tracking; Control and connectivity; Autonomous operations [1]. The purpose of IoT is that things have always been in touch (anytime, anywhere). Smart home and smart offices must learn and find new ways to communicate the things/objects. This is a new revolution of the Internet [2,3]. IoT widens the internet's scope from people-operated computers towards autonomous intelligent smart devices [4]. Typically, these devices are connected to the Internet for remote monitoring and diagnosis, leading to significant cost savings. IoT can be divided into three parts: mobile; domestic; industrial [5].

According to [1], new concepts of IoT must to reduce complexity through pre-integrated modules for data acquisition, validation, and analysis; reduce risk due to compliance with the one M2M standard; must have faster time-to-value through as-a-Service (AAS) hosted models; lower total cost of ownership (TCO) by reducing capital expenses, providing scalability. Modern IoT technologies have been created under a totally different scenario [6,7]: 1) Internet and cellular networks have become the world standard, with very high levels of coverage, reliability and availability; 2) smaller and smarter devices are constantly hit the industrial and consumer markets, to better understand and present the new after-sales and remote-controlled services; 3) software development and system interoperability standards such as XML, web services and SOA are converging to create fertile ground for M2M communications technologies, that makes it easier to use them in a variety of industries.

The development of IoT is accompanied with the receipt, storage, processing and distribution of large amounts of data. More precisely, with data acquisition, processing and release of information from them, the formation and distribution on the basis of this information, knowledge, adoption and

implementation of solutions based on information and knowledge. Those, we can talk about yet another paradigm DIKS: "data-information-knowledge-solution".

The model of IoT currently includes over fifty use cases, covering many service categories such as [6, 7]: Smart metering (electricity, gas and water); Facility management services; Intruder alarms& fire alarms for homes & commercial properties; Connected personal appliances measuring health parameters; Tracking of persons, animals or objects Agriculture; Health Care / E-Health; Retail Safety and Security Automotive & Logistics Energy & Utilities Manufacturing; Smart City; Smart Home; Smart city infrastructure such as street lamps or dustbins; Smart office; Smart hotel; Connected industrial appliances such as welding machines or air compressors.

The goal of the paper is to analyze and develop on the basis of this analysis, architectural important from a safety standpoint IoT subsystem - SBC. The second section describes the architecture of the standard SBC, an analysis of possible types of software vulnerabilities objects of this system, as well as the means to ensure the safety of SBC network components. The third section is devoted to the development of Markov network model and researching system's SBC reliability indicators - availability function. Last section is a conclusion and discusses future research steps.

II. Analysis of SBC network reliability and security

1. Architecture of network of the SBC

IoT solutions for the office is a network of automated and user devices, allowing staff to solve their business problems using the latest technological capabilities. Network nodes are able to receive and transmit information; can interact with other objects or be independent; may have different levels of access to its settings, depending on the security level, etc. To install SBC it is necessary as to automate some specific functions (control of lighting, ventilation and air conditioning, etc.) and introduce the virtual integration of any equipment, of SBC in the single system, which works by the algorithm which will set by the installer and designer SBC. Based on the analysis of standard solutions for the implementation of IoT system is proposed the wired architecture of the network SBC. Using for IoT SBC Internet wire network devices are: router with Ethernet-ports and wireless access ability, softswitch the second or third layer, firewall, power block, server with control software, IP-camera, sensors, cables (fig. 1). The system can operate as a standalone or with Internet connection.

Work wired network SBC depends entirely on the power source. For the smooth functioning of the UPS is used a redundancy as of its blocks and their batteries, also alternative power sources (solar panels, etc.). The basic system is an intelligent home security, the ability to backup data, the ability to software improvements, a rate recovery in the event of a malfunction or failure. All actions must interact with the subsystems of a smart home, and therefore should be focused on start-up and adjustment of the system smart home. In this case, fixing any one subsystem does not affect the operation of other subsystems.

Router is the central subsystem of SBC, that connected Internet network by ISP and LAN, includes switch, server, interconnected cables, and also can to plug tablets, smartphones over IEEE 802.11 or 802.15.4 standards. Switch the second or third layer with PoE technology connect all Ethernet-sensors and IP-cameras in office. Server - it is the control subsystem in the SBC, it keeps control and diagnostics programs that poll the Ethernet-sensors, and keeps and treated statistics. Additional software with security policies are installed on the server. On the server undertaken the largest number of DOS- and distributed denial-of-service (DDOS) – attacks, brute-force attacks, Phishing attacks. Some types of attacks aimed at disabling Server, Router and Switch, resulting in malfunction of computers, tablets, smartphones and various gadgets connected to the system, as well as the sensors. All actions must interact with the subsystems of a SBC, and therefore should be focused on start-up and adjustment of the system smart home. In this case, fixing any one subsystem does not affect the operation of other subsystems.

2. Analysis of Security Aspects

But there is problem with security in SBC: these are the unknown or unreported vulnerabilities in the software that's being used. They could be bugs, or entirely new types of attacks [8]. Each device of the SBC is a potential entry point for a network attack by insiders, hackers, or criminals. When security is insufficient in even seemingly harmless household appliances, or other IoT products, it presents endemic vulnerabilities and risks [9]. IoT is based on using a variety of sensors and control units. SBC system gives staff complete control over their offices, but, at the same time, there are new dangers and threats due to the fact that the new computer technology with an internet connection, provide possibility of hackers to connect to the system. The IoActive IoT Security Survey revealed that nearly half (47%) of all respondents felt that less than 10% of all IoT products on the market are designed with adequate security [10].

As written at [11], the IoT facilities, available by the Internet, may disclose personal user data to another people. Lack of data security IoT brings to detection of vulnerable devices by criminals to gain access to him or other IoT facilities. The attacks report by Kaspersky Lab shows, that IP-cameras are connected wirelessly to the Internet are not necessarily secure: here is the potential for cybercriminals to passively monitor the cameras for the implementation of the code in the network, thereby replacing the image in the camera channel communication to fake shots, or put the system in offline mode. If the data packets are transmitted via a data network, it has not been encrypted, an attacker can create their own version of the software and data processing for controlling the IoT [12]. Physical security - notification of suspicious activity at the moment, which is found near the IoT-device. Alerts come with surveillance cameras, physical access control, and other sensors to detect movement and other [7, 12]. With the increasing variety and scale of apps running on the network, they need a common policy framework to move beyond the perimeter-based security

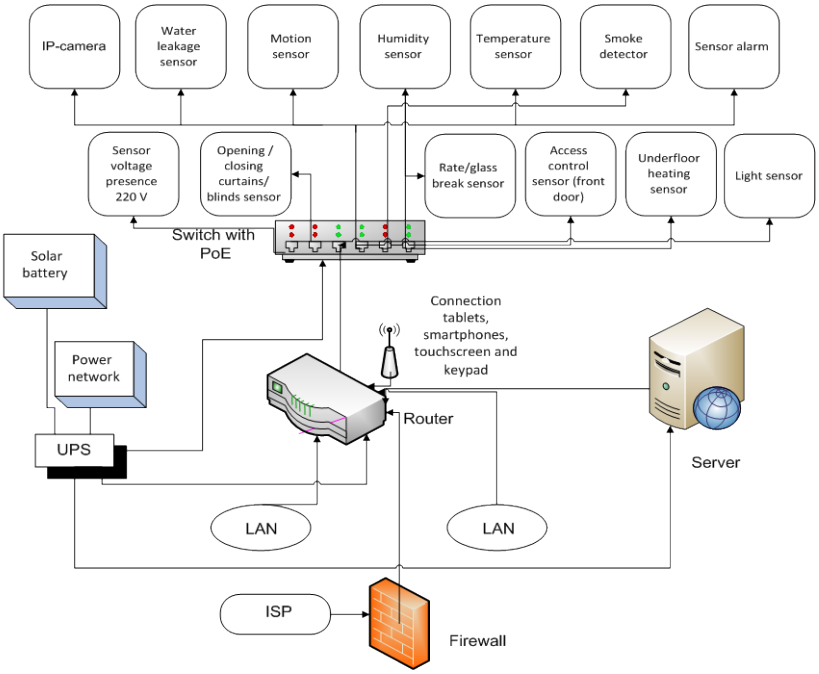

Fig. 1. The architecture of the SBC network

model for all things connected [13]. Security and privacy are important requirements for the IoT due to the inherent heterogeneity of the Internet connected objects and the ability to monitor and control physical objects [14]. Last week was carried out a series of powerful DDoS attacks aimed to kill multiple targets. For DDoS attacks had been used malware to infect the largest number of IoT devices, connected to the Internet [15].

Analysis is shown, that large manufacturers of network equipment, which should be used in the organization of the wired network SBC, complement its routers, switches, additional measures to protect against possible attacks from the Internet. However, Security reports the major antivirus companies (Kaspersky Lab, McAfee, Symantec), CERT, Security lab Cisco, HP, indicates that periodically occurring attacks on the routers and other network equipment, that lead to the failure of hardware and software components of the device as a result of the availability of its software vulnerabilities [15-24]. Attack methods include the use of zero-day management target phishing attacks, as well as keylogger kernel mode, which is when you press downloads data from infected computers. They also manage to crack the weak digital signature keys to generate certificates for signing malware to malicious files presented as legitimate software.

As the use of IoT business and IT - technology security experts, entrusted with the installation of IoT - applications and solutions must take into account the significant paradigm shift, as well as operational, strategic and business objectives. When faced with a variety of internal and external security issues, such as network attacks, malicious software, malware, external hackers, the decision makers should be aware that the statistics of threats from external hackers (37%), malware (33 %), internal hackers (30%), and denial of service attacks. List of types of malicious actions performed by the attacker: illegal use of user accounts; theft software; running the executable code for the damage to the systems, for the destruction or corruption of data; modification data; identity theft; execution of actions that do not allow users to access network services and resources; execution of actions that absorb network resources and bandwidth.

III. SBC Dependability Modeling

1. Rationale of Markov Model for Describing of Technical Condition of SBC Network's Components

IoT systems combined with their high-availability requirements means that these systems are more at risk of unintended, non-malicious downtime. When designing SBC, it is necessary to provide the security of the operation and the reliability of hardware and software components of the system. Understanding new communication protocols, hardware types, and obscure operating systems is difficult, making IoT security an incredible challenge [23, 24].

In the network equipment that used for the organization of systems SBC, according to statistics, more and more vulnerabilities found in software code. When exposed to hacker attacks via these vulnerabilities can be stolen proprietary information of the company, and making failure of the software and hardware components of network devices and servers. Manufacturers proposes decisions on the release of patch, redundancy of components to reduce the risks of vulnerabilities of network equipment in IoT. However, vulnerabilities are discovered again and again, and the attacks translates them inoperable technical condition. In order to provide network Dependability of IoT, which includes providing a high reliability and high safety at the required level, it is necessary to develop a mathematical model for a more accurate

quantification.

Assumptions in the development of the model:

- stream hardware failures of the system obeys Poisson distribution;
- the flow of failures of subsystems obeys Poisson distribution, as the results of monitoring and diagnostics. The software testing corrected secondary error (the result of the accumulation of the effects of primary errors and defects, bookmarks), and to fix a malfunction or failure of software, eliminating or the consequences of software bookmarks and code vulnerabilities, DDOS - attacks. The number of primary software defects permanently. Therefore, the assumption is true, that the flow of software failures obeys Poisson distribution, the failure rate is constant;
- the model does not take into account that eliminating software vulnerabilities and design faults changes the parameters of the flow of failures (and recovering). To investigate the dependability SBC had been used the theory of Markov models, as the failure rates of hardware and software and the availability of software vulnerabilities is constant. Availability of software vulnerabilities is constant.

2. Graph of States Markov Model

Fig. 2 shows a Markov graph of functioning of the main subsystems SBC, λ - the failure rate or attack, μ - the recovery rate. The basic state of the system: 1) Normal condition (up-state) system; 2) Failure due to faulty feeder from the stationary power supply (220 V); 3) Failure due to a malfunction of the second feeder (a solar battery); 4) Failure of the battery in the UPS; 5) Reconfigure the power subsystem; 6) Failure of the cable connecting the router and server; 7) Failure of the cable connecting the ups and switch, and / or the router, and / or server; 8) Failure of the cable connecting the router and switch; 9) Firewall denial; 10) Refusal server due to a fault server components, or exposure to attacks on the code server system software with vulnerabilities; 11) Failure router as a result of failure of the router components, or the impact of the attacks on the code of the router operating system vulnerabilities; 12) Switch failure due to a fault switch components, or exposure to an attack on the system software code switch with the presence of vulnerabilities; 13) Partial failure of the system due to the failure of cable connecting any or multiple sensors and IP cameras; 14) Partial failure of the system due to the failure of any one or more sensors and IP cameras; 15) Failure of the system SBC; 16) DDoS-attack; 17) Failure of the server hardware; 18) Failure of the router hardware; 19) Failure of the switch hardware; 20) Brute-force attack; 21) Phishing-attack; 22) Special attack on the power subsystem UPS; 23) Failure of the software of server or router.

3. Research Results of Modelling

At the model, shown in the fig. 2, there are circles with numbers of states of the SBC system, arrows with rate transitions from one to another state and the recovery rate of SBC system components after failures.

As an index of reliability SBC we choose availability function AC(t), that is defined as the sum of the probabilities of staying the system in an up-states:

$$AC(t) = P_1(t) + P_5(t).$$

Solving the system of Kolmogorov-Chapmen equations, we can get the value of the availability function components and SBC network, the number of network failures due to software vulnerabilities, and how and with what recovery rate the system restored after such failures. It follows that service availability, service continuity, cyber security, data integrity, resilience and high dependability of software and hardware should be inherent in IoT networks. Initial data for simulation of the Markov's model is shown in Fig. 2: $\lambda 12=2{,}28\cdot10^{-4}$ 1/h; $\lambda 13=1{,}14\cdot10^{-5}$ 1/h; $\lambda 14=1{,}94\cdot10^{-3}$ 1/h; $\lambda 16=1{,}14\cdot10^{-4}$ 1/h; $\lambda 17=2{,}28\cdot10^{-5}$ 1/h; $\lambda 18=5{,}7\cdot10^{-5}$ 1/h; $\lambda 19=5{,}7\cdot10^{-4}$ 1/h; $\lambda 110=1{,}1\cdot10^{-5}$ 1/h; $\lambda 111=1{,}4\cdot10^{-5}$ 1/h; $\lambda 112=2{,}28\cdot10^{-4}$ 1/h; $\lambda 113=5{,}7\cdot10^{-5}$ 1/h; $\lambda 114=5{,}7\cdot10^{-5}$ 1/h; $\lambda 117=1{,}1\cdot10^{4}$ 1/h; $\lambda 119=4{,}56\cdot10^{-5}$ 1/h; $\lambda 123=1\cdot10^{-5}$ 1/h; $\lambda 25=0{,}25$ 1/h; $\lambda 35=0{,}2$ 1/h; $\lambda 45=0{,}913$ 1/h; $\lambda 615=1\cdot10^{-8}$ 1/h; $\lambda 715=1\cdot10^{-8}$ 1/h; $\lambda 815=1\cdot10^{-8}$ 1/h; $\lambda 915=1\cdot10^{-8}$ 1/h; $\lambda 916=4\cdot10^{-5}$ 1/h; $\lambda 920=9{,}89\cdot10^{-4}$ 1/h; $\lambda 921=1{,}71\cdot10^{-5}$ 1/h; $\lambda 922=1{,}37\cdot10^{-4}$ 1/h; $\lambda 910=4{,}79\cdot10^{-3}$ 1/h; $\lambda 911=1\cdot10^{-8}$ 1/h; $\lambda 912=1\cdot10^{-4}$ 1/h; $\lambda 1015=5{,}4795\cdot10^{-3}$ 1/h; $\lambda 1115=1{,}7123\cdot10^{-3}$ 1/h; $\lambda 1215=9{,}1324\cdot10^{-4}$ 1/h; $\lambda 1315=2{,}2831\cdot10^{-4}$ 1/h; $\lambda 1615=2{,}28\cdot10^{-4}$ 1/h; $\lambda 1617=1{,}826\cdot10^{-3}$ 1/h; $\lambda 1618=9{,}13\cdot10^{-4}$ 1/h; $\lambda 1619=2{,}28\cdot10^{-4}$ 1/h; $\lambda 2023=9{,}9\cdot10^{-2}$ 1/h; $\lambda 2123=1\cdot10^{-3}$ 1/h; $\lambda 224=1{,}14\cdot10^{-4}$ 1/h; $\lambda 2310=9{,}14\cdot10^{-4}$ 1/h; $\lambda 2311=1{,}826\cdot10^{-3}$ 1/h; $\mu 51=250$ 1/h; $\mu 61=2$ 1/h; $\mu 71=2$ 1/h; $\mu 81=0{,}25$ 1/h; $\mu 91=4$ 1/h; $\mu 101=1$ 1/h; $\mu 111=1$ 1/h; $\mu 121=1$ 1/h; $\mu 131=1$ 1/h; $\mu 141=1$ 1/h; $\mu 151=1$ 1/h; $\mu 171=2$ 1/h; $\mu 191=2$ 1/h; $\mu 221=4$ 1/h; $\mu 231=2$ 1/h; $\lambda 118=2{,}28\cdot10^{-5}$ 1/h; $\mu 181=2$ 1/h; $\lambda 2110=1\cdot10^{-6}$ 1/h; $\lambda 1610=3{,}424658\cdot10^{-2}$ 1/h; $\lambda 1611=5{,}13699\cdot10^{-3}$ 1/h; $\lambda 1612=3{,}42466\cdot10^{-3}$ 1/h; $\lambda 1623=0{,}171233$ 1/h.

At figures 3-6 is shown the changing of AC from changing the rate of the transition from one state to another in the Markov's model. Obtained probabilities of finding the SBC system in each state of Markov model (fig.2):

P1(t)=0,995502297364980; P2(t)=0,000907898095197;
P3(t)=0,000567436309498; P4(t)=0,002115306087011;
P5(t)=0,000009086944973; P6(t)=0,000056743630666;
P7(t)=0,000011348726133; P8(t)=0,000226974514720;
P9(t)=0,000141647345048; P10(t)=0,000011567185530;
P11(t)=0,000013914403890; P12(t)=0,000226767534296;
P13(t)=0,00005673067874; P14(t)=0,00005674363095;
P15(t)=0,000000307264927; P16(t)=0,000000029993993;
P17(t)=0,000056743658334; P18(t)=0,000011348739882;
P19(t)=0,000022697455799; P20(t)=0,000001415042669;
P21(t)=0,000002419749850; P22(t)=0,000000004851283;
P23(t)=0,000000570791630.

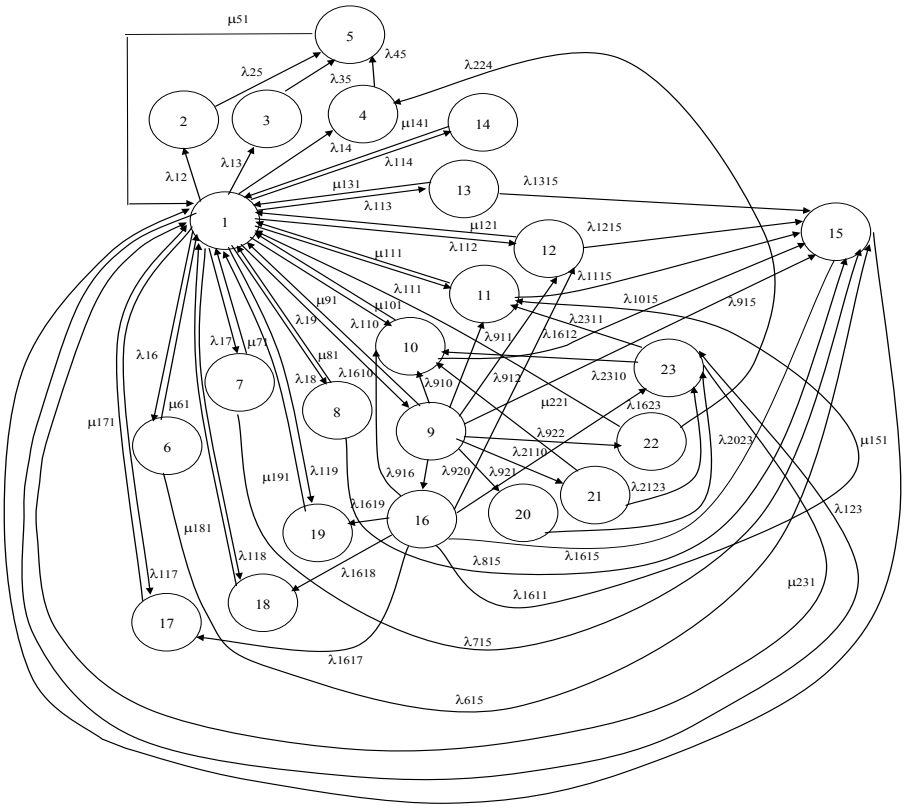

Fig. 2. Markov's graph of system SBC states

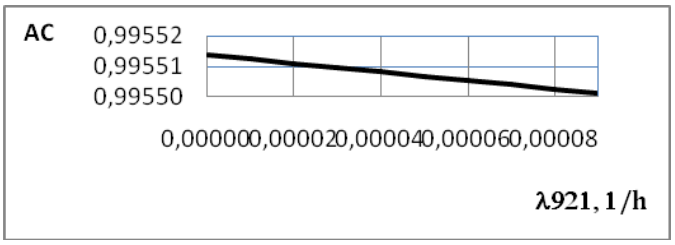

Fig 3. Graph of dependence of AC of SBC and the rate of transition to a state of Phishing-attack - λ921

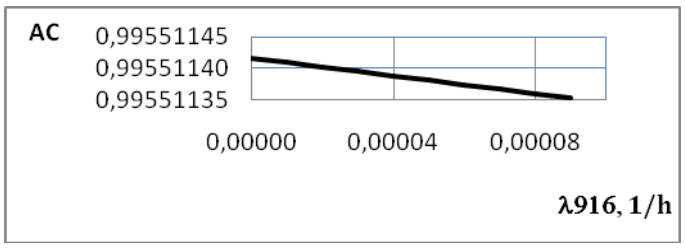

Fig 4. Graph of dependence of AC of SBC and the rate of transition to a state of DDoS-attacks - λ916

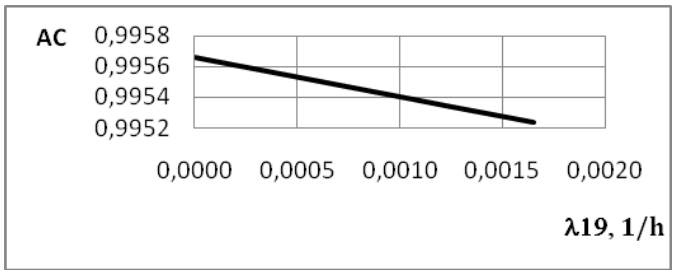

Fig 5. Graph of dependence of AC of SBC and the rate of transition to a state of denial Firewall - λ19

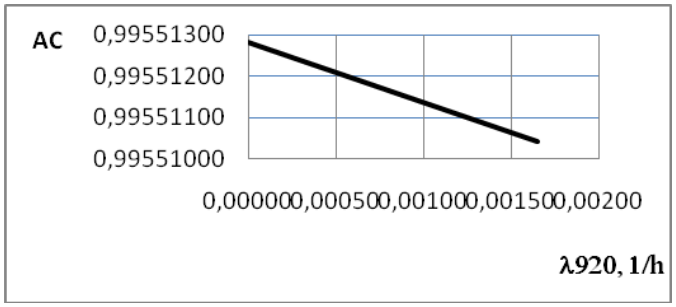

Fig 6. Graph of dependence of AC of SBC and the rate of transition to a state of Brute-force attacks - λ920

The analysis of the Markov model simulation results showed that by increasing the rate of the transition to a state of denial firewall λ19 decreases the value of SBC availability function. In case of refusal the firewall different kinds of attacks can freely influence the vulnerability of the server software, router, switch. Increase the rate of the transition from a state to a state of denial firewall Brute-force attack - λ920, Phishing-attacks - λ921, DDoS-attacks - λ916 reduces the value of availability function of SBC.

IV. Conclusion

Analysis of the safety and reliability of the proposed in the paper system SBC based on the statistics of failures of hardware, software components, communication lines, router, firewall, some existing attacks that are included in the constructed Markov model, showed that the studied system is stable, the availability function quite high and not much changing with an increase in the intensities of the attacks. Recently, however, increasing number of malicious attacks and their types, that will lead to a sharp decrease in system reliability and security of SBC. It is therefore necessary to look for more advanced security techniques researched systems that suppose purpose of further research.

References

[1] O. Vermesan, p. Friess, P. Guillemin, et.al. Internet of things – from research and innovation to market deployment. river publishers series in communication, 2014. Available at: http://www.internet-of-things-research.eu/pdf /IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf (accepted at 3.08.2016). 141 p.

[2] Ljubomir Lazic, and Nikos Mastorakis, "Orthogonal Array application for optimal combination of software defect detection techniques choices", WSEAS Transactions on Computers, pp.1319-1336, Issue 8, Volume 7, August 2008

[3] NB-IOT – Enabling new business opportunities. Building a better connection. Huawei Technologies CO., LTD. Available at: http://www.huawei.com/minisite/4-5g/img/NB-IOT.pdf (accepted at 3.08.2016).

[4] Matat D. Internet rechey I tehnotrendi yak oznaki evolyutsIYi suspIlstva. Osvita Ukrayini. Available at: http://pedpresa.ua/136666-internet-rechej-i-tehnotrendy-yak-oznaky-evolyutsiyi-suspilstva.html (accepted at 3.08.2016).

[5] Cisco IoT System Brochure Cisco IoT System Deploy. Accelerate. Innovate. 2015.

[6] Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust White Paper. 2015. http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/iot-system-security-wp.pdf. 4 p.

[7] No stars for Internet of Things security. At this week's AusCERT 2016 conference, an embedded device security specialist proposed a 'Security Star' rating for consumer IoT devices. It's a great idea, but it'll never happen. Available at: http://www.zdnet.com/article/no-stars-for-internet-of-things-security/(accepted at 3.08.2016).

[8] IoTSF Guest Blog. Available at: https: //iotsecurityfoundation org/survey-less-than-10-of-iot-devices-keep-data-secure/(accepted at 3.08.2016).

[9] PRESS RELEASE. ioactive. Available at: http://www.ioactive.com/news-events/iot-products-have-inadequate-security-according-to-practitioner-survey.html (accepted at 3.08.2016).Internet of Things security is dreadful: Here's what to do to protect yourself. Consumers still aren't doing their homework before buying and deploying internet-connected baby monitors and other products. Available at: http://www.zdnet.com/article/internet-of-things-security-it-dreadful-heres-what-to-do-to-protect-yourself (accepted at 3.08.2016).

[10] Kaspersky security bulletin 2015. Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. Available at: https://securelist.com/files/2015/12/ Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. (accepted at 3.08.2016). 85 p.

[11] Internet of things. Hewlett Packard Enterprise. Available at: http://www.arubanetworks.com/solutions/internet-of-things/. (accepted at 3.08.2016).

[12] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015. P. 2347-2376. Available at: *http://www.comsoc.org/files/Publications/Tech%20Focus/2016/iot/ 3.pdf* (accepted at 3.08.2016).

[13] Delivering on the IoT customer experience. Business white paper. Hewlett Packard Enterprise. Available at: http://h20195.www2.hpe.com /v2/GetDocument.aspx?docname=4AA6-5128ENW (accepted at 3.08.2016). 8 p.

[14] Cisco IOS Firewall Common Deployment Common Deployment Scenarios. Available at: http://www.cisco.com/ c/dam/en/us/products/collateral/security/ios-firewall/prod_presentation0900aecd804e1307.pdf (accepted at 3.08.2016). 10 p.

[15] Cisco IOS XR Software Command Injection Vulnerability. Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-ios-xr (accepted at 3.08.2016).

[16] Cyber Risk Report 2016 Executive summary. Hewlett Packard Enterprise. Available at: http://www8.hp.com/fi/fi/software-solutions/cyber-risk-report-security-vulnerability/ (accepted at 1.08.2016).

[17] McAfee Labs Threats Report June 2016. Intel security. Available at: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf (accepted at 1.08.2016). 53 p.

[18] Internet Security Threat Report VOLUME 21, APRIL 2016. Symantec.

[19] Executive report: SMART CITIES. Transformational 'smart cities': cyber security and resilience. Transformational Smart Cities - Symantec Executive Report.pdf Available at: https://eu-smartcities.eu/sites /all/files/blog/files/Transformational%20Smart%20Cities %20-%20 Symantec%20Executive%20Report.pdf. (accepted at 1.08.2016). 20 p.

[20] Support Communication - Security Bulletin. Support Center Hewlett Packard Enterprise. Available at: http://h20566.www2.hpe.com/hpsc/doc/public/display?sp4ts.oid=4282347&docLocale=ru_RU&docId=emr_na-c04453311. (accepted at 1.08.2016). 1 p.

[21] Bulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available. Sign up to receive these security bulletins in your inbox or subscribe to our RSS feed. Available at: https://www.us-cert.gov/ncas/bulletins/SB16-200,%20https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1426. (accepted at 1.08.2016).

[22] Cisco IOS XR for NCS 6000 Packet Timer Leak Denial of Service Vulnerability. Available at: https://tools.cisco.com/security/ center/content/CiscoSecurityAdvisory/cisco-sa-20160713-ncs6k. (accepted at 3.08.2016).

[23] A Forrester Consulting Thought Leadership Paper Commissioned By Cisco. March 2015. Security: The Vital Element Of The Internet Of Things. http://www.cisco.com/c/dam/en_us/solutions/trends/iot/vital-element.pdf. 11 p.

[24] Powerful DDoS attacks leveraging IoT devices hit several companies. http://searchsecurity.techtarget.com/news/450305010/Powerful-DDoS-attacks-leveraging-IoT-devices-hit-several-companies?utm_medium=EM&asrc=EM_NLN_65279070&utm_campaign=20160928_Record-setting%20DDoS%20attacks%20leverage%20IoT%20devices,%20strike%20several%20targets_mbacon&utm_source=NLN&track=NL1820&ad=910227&src=910227.

[25] Ljubomir Lazic, Nikos Mastorakis, "Cost effective software test metrics", WSEAS Transactions on Computers, pp. 599-619, Issue 6, Volume 7, June 2008