SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL6 No1
MARCH 2022

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 1-14 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

RESOURCE ORCHESTRATION IN 5G TECHNOLOGIES

Ajit Kumar Singh Department of Computer Science Patna Women's College, Bihar, India

Prof G. P. Gadkar Department of Physics College of Commerce, Arts & Science Patliputra University, Bihar, India

ABSTRACT: Heterogeneous architecture is an underlining feature of 5G, however deployment and management of HetNets in 5G scenarios is yet to be explored. Given the need to satisfy overwhelming capacity demands in 5G, mm-wave spectrum (3-300 GHz) is expected to offer a very compelling long term solution by providing additional spectrum to 5G networks. Hence, the challenge is the integration of mm-wave in heterogeneous and dense networks as well as the backward compatibility and integration with legacy 4G/3G networks. Furthermore, Cloud radio access networks (C-RAN) contribution to 5G is considered as a cost effective and energy efficient solution for dense 5G deployment. From an energy point of view, cost and energy consumption are major considerations for 5G. C-RAN and energy efficiency techniques could help in performance improvements.

Although HetNets were introduced in 4G networks, their complexity has increased in 5G networks. In this paper, we will try to build a clear image of HetNets in 5G cellular networks. We consider different technologies with a special focus on mm-wave networks given its important role in 5G networks. We then address the available standards in HetNets that allow interworking and multihoming between different radio access technologies. Afterwards, we consider the virtualization of 5G HetNets and its benefits. Different resource allocation strategies in the literature are also presented for single-resource as well as for multi-resources. Finally, we give an overview of existing works addressing energy efficiency strategies in 5G networks.

Keyword: *5G, HetNets, 5G Energy Efficiency, Resource Allocation, Radio Access Network*

1. INTRODUCTION

Fifth generation (5G) is not as previous generations, an evolution of the existing, but it is rather considered as a cellular network revolution that builds on the evolution of existing technologies. These technologies are complemented by new radio concepts that are designed to meet the new and challenging requirements of some use cases today's radio access networks cannot support [2] [3].

This revolution is necessary to offer new services to 5G users with good quality of service (QoS). These services include:

- Good service even in very crowded places.
- Similar user experience for end-users on the move as for static users.
- The Internet of Things (IoT). Basically, anything that profits from being connected will be connected.

- Machine-to-machine (M2M) or device-to-device (D2D) communication with real-time constraints, enabling new functionalities for traffic safety, traffic efficiency, smart grid, and e-health.
- Huge capacity increase that could be achieved by having more spectrum, better spectrum efficiency and a large number of small cells.

In parallel to the data starving services, several technological concepts that were not supported in previous cellular generations are now potential 5G scenarios to answer users demands. We mainly note: D2D communications, ultra-reliable communications, massive machine communications, IoT, Cloud computing, and hybrid networks. On the other hand, ultra high data rates, extremely low latency, anywhere anytime coverage, huge energy saving – most of the promises made by 5G are associated with their respective challenges. Among these challenges we address in this paper network densification in the form of heterogeneous networks (HetNets).

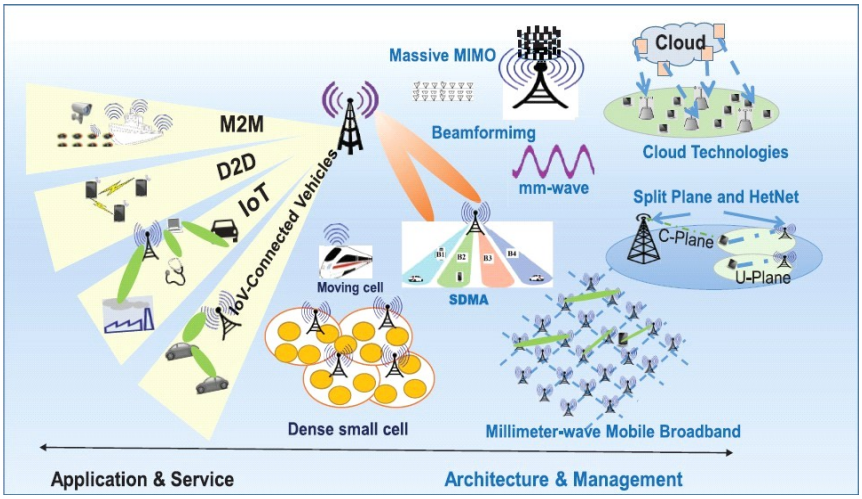

Figure 1.1: Next Generation 5G Wireless Networks (Source: [3]).

2. Heterogeneous networks/Multi-RAT

Today's 3G and 4G networks are designed primarily with a focus on peak rate and spectral efficiency improvements. In the 5G era, we will see a shift towards network efficiency with 5G systems based on dense heterogeneous networks architectures. HetNets are among the most promising low-cost approaches to meet the industry's capacity growth needs and deliver a uniform connectivity experience. A HetNet comprises a group of small cells that support aggressive spectrum spatial reuse coexisting within macro cells as shown in Fig. 1.2. However, HetNets will be architected to incorporate an increasingly diverse set of frequency bands within a range of network topologies, including macro cells in licensed bands (e.g., long term evolution network or LTE) and small cells in licensed or unlicensed bands (e.g., WiFi). New higher frequency spectrum (e.g., millimeter-wave or mm-wave) may also be deployed in small cells to enable ultra-high-data-rate services.

Architecture

HetNets are formed of macro cells and small cells. A macro cell is generally divided into several sectors in order to increase the spatial frequency reuse which increases the network capacity. Typically, a macro cell is implemented as a tri-sectorial base station (BS) with each sector of 120 ◦ . However, different definitions are considered for choosing the cell type, it can consider the radius of the cell, the number of connected users and the deployment options.

As their name indicates, small cells provide a smaller coverage area than a macro cell. As shown in Fig. 1.2 , a macro cell overlaps several small cells. There are several types of small cells such as micro, pico, femto and relay cells, ordered in decreasing order of coverage and transmission power. These small cells can be managed by the same operator as a macro cell or by a different operator and require a lower installation cost. In addition, it is worth to note that small cells are mainly deployed in order to support the increasing rates of data services but can also support voice services.

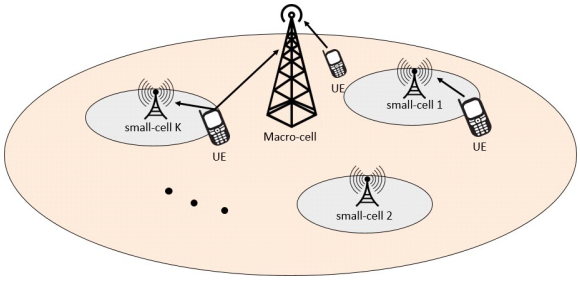

Figure 1.2: Heterogeneous network model.

WiFi small cells

Widely deployed WiFi systems are playing an increasingly important role in offloading data traffic from the heavily loaded cellular network, especially in indoor traffic hotspots and in poor cellular coverage areas. Very recently, the Federal Communications Commission (FCC) voted to make 100 MHz of spectrum in the 5 GHz band available for unlicensed WiFi use based on the IEEE 802.11ac standard [9], giving carriers and operators more opportunities to push data traffic to WiFi. WiFi access points have even been regarded as a distinct tier of small cells in heterogeneous cellular networks. Wireless local access networks (WLAN) technology evolution is mainly carried out within the WLAN IEEE 802.11 working group which released multiple set of standards for various operating frequencies and ranges specification.

LTE Small Cells

LTE small cell networks are highly dense networks constituting of home eNodeBs, indoor enterprise eNodeBs as well as outdoor deployed eNodeBs. Some of the major challenges of the LTE small cell networks are:

1) Maintaining the desired QoS with respect to downlink and uplink packet data transmission.

2) Efficient handover.

3) Interference co-ordination with neighbors. Especially in the uplink direction, i.e., from UE to small cell eNodeB, the task of delivering a wide variety of application layer packets is complicated due to limited transmission power of the UE, limited battery resources at UE and time-varying nature of wireless channels.

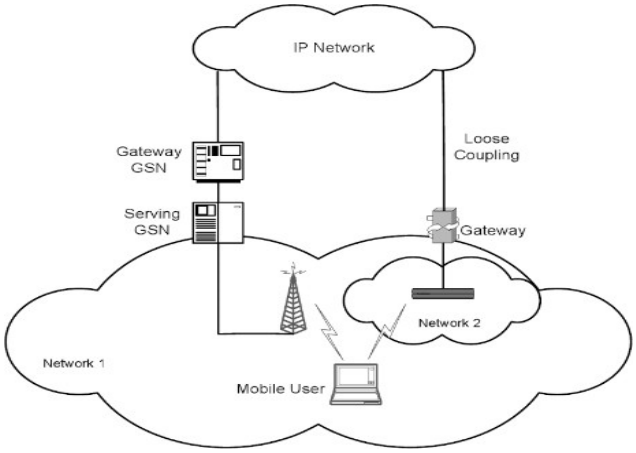

Figure 1.3: HetNet architecture with loose coupling (Source: [19]).

From an architectural point of view, two deployment scenarios were identified in [21], namely small cells co-existing with macro cells,known as Hot Spot, and small cells without macro cells known as Not spot. In such areas, only basic network coverage is needed, which can be adequately supported by lower cost small cells rather than more expensive resource from the macro site. Not-spot small cells are perfect for network coverage extension to reach the rural areas, both indoors and outdoors. The Not-spot scenario may potentially suffer however from high volume of handover signaling load, which may impact the users Quality-of-Experience (QoE).

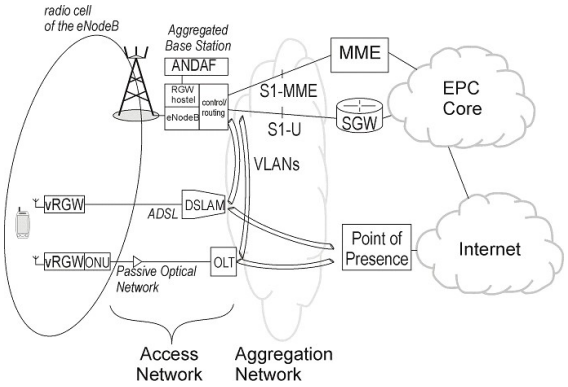

Figure 1.4: HetNet architecture with tight coupling (Source: [19]).

Mm-Wave Small Cells

Capacity for wireless communication depends on spectral efficiency and bandwidth. It is also related to cell size. Cell sizes are becoming small and physical layer technology is already at the boundary of Shannon capacity [24]. It is the system bandwidth that remains unexplored. Presently, almost all wireless communications use spectrum in 300 MHz to 3 GHz band, often termed as "sweet spot" or "beachfront spectrum" [25]. In order to increase capacity, wireless communications cannot help facing the new challenges of high frequency bandwidth. The key essence of next generation 5G wire-less networks lies in exploring this unused, high frequency mm-wave band, ranging from 3 ∼ 300 GHz. Even a small fraction of available mm-wave spectrum can support hundreds of times of more data rate and capacity over the current cellular spectrum [26]. Thus, the availability of a big chunk of mm-wave spectrum is opening up a new horizon for spectrum constrained future wireless communications [26].

Beamforming in mm-wave

The main objective of adaptive beamforming is to shape the beam patterns (e.g., by beamsteering) so that the received signal-to-noise ratio (SNR) is maximized. Full control of beam pattern shaping requires changing both the amplitude and phase of transmitted signals. The need for low-cost and lowpower hardware, however, has pushed mm-wave towards a simpler analog architecture that contains only digitally controlled constant modulus phase shifters. Hybrid precoding proposed in [27] divides the required precoding processing between the analog and digital domains, and hence allows better control of the beam shape.

Mm-wave Mobile Boradband Frame Structure

As in 4G systems, mm-wave uses also OFDM and single-carrier waveform as multiplexing schemes. We show in Fig. 1.5 a mm-wave frame structure as described in [28]. The basic transmission time interval (TTI) is a solt of 62.5μs duration. Subframe, frame and superframe's duration are chosen equal to those in LTE systems (1 ms, 10 ms and 40 ms, respectively) in order to facilitate the interworking between both technologies. The cyclic prefix (CP) is chosen to be 520 ns, which gives sufficient margin to accommodate the longest path, different deployment scenarios, and the potential increase of delay spread in the case of small antenna arrays or wider beams. The subcarrier spacing is chosen to be 480 kHz, small enough to stay within the coherent bandwidth of most multipath channels expected in mm-wave.

Interworking between mm-wave and LTE

A hybrid LTE/mm-wave system can improve coverage and ensure seamless user experience in mobile applications. In a hybrid LTE/mm-wave system, system information, control channel, and feedback are transmitted in the LTE system, making the entire millimeter-wave spectrum available for data communication. Compared with millimeter waves, the radio waves at < 3 GHz frequencies can better penetrate obstacles and are less sensitive to non-line-of-sight (NLOS) communication link or other impairments such as absorption by foliage, rain, and other particles in the air. Therefore, it is advantageous to transmit important control channels and signals via cellular radio frequencies, while utilizing the millimeter waves for high data rate communication

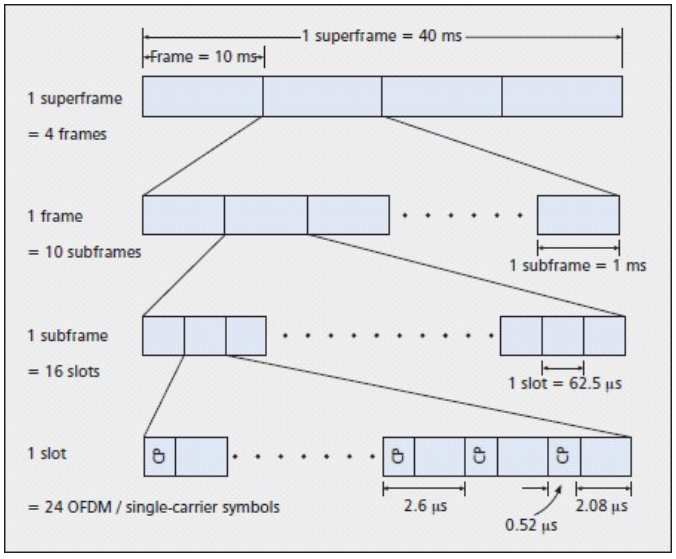

Figure 1.5: Mm-Wave frame structure [28].

Multihoming

HetNets were designed such that traffic can be offloaded between available access networks. However, concurrent multiple access to more than one network in wireless networks has recently been standardized in Release 12 under the name of "Dual Connectivity" [15]. In this section, we introduce the aspects and standards enabling multihoming's concept implementation with focus on the dual connectivity standard. We also present a literature overview on interworking and network selection strategies in this context.

Multihoming aspects

Multihoming was first proposed as a redundancy solution for wired networks. Recently, the coexistence of different wireless access network technologies has renewed this concept and became an attractive topic for study during the past years. Wireless networks multihoming concept started with offloading [31, 32, 33], passing by load balancing [34], optimal distribution [35] [36] [37], as well as concurrent multiple access [38, 39, 40].

Load balancing concept was introduced in wired networks [31]. Such load balancing system must determine the available bandwidth through an access link, assign incoming and outgoing traffic, and detect access links failure. For this aim, a reliable routing protocol must be considered [32]. Similarly, load balancing management could be obtained in heterogeneous wireless networks by dynamically optimizing the packets' split ratio between multiple access networks as shown in [34]. Such strategy might be based on the load information and channel quality information at each access network.

Multihoming Technology Enablers

Throughout the past years, 3GPP and IETF worked hard in order to standardize different HetNets interwoking schemes. Their main interest was to standardize the users mobility between accesses, the transport layer support of multihoming, and frequency resource scheduling known as "Dual Connectivity" (DC).

Mobility in Heterogneous Networks

Non-seamless offloading between LTE and WiFi is disturbing, especially for real-time applications that require the continuity of service (e.g., VoIP, Video Conference, HTTP page). It is highly desirable that mobile operators provide seamless service continuity between cellular and WiFi accesses with involving both user plane routing and control plane functions. This seamless continuity can be first supported by ensuring a service layer continuity even when the IP address has changed which is not supported in TCP/IP. In this section, we present some of the seamless continuity standardized technologies. Several mechanisms are proposed by 3GPP describing the offload management in 3GPP networks. I-WLAN is the first approach allowing local area network access to the 3GPP core.

Multihoming at Transport Layer

In addition to the mobility described above and maintaining the IP connection of a user when offloading, static multihoming of a user connected simultaneously to multiple access networks has multiple IP addresses. However, regular TCP can support only one flow which mean only one IP address. For this reason, several transport protocols were proposed, we will present here an overview of multihoming-capable protocols.

Transport layer multihoming started with node multihoming which is an old concept defined as a device having more than one wired access interface. Two main standards were proposed: Stream Control Transport Protocol (SCTP) in 2000 [39, 40] and Multi-Path Transport Control Protocol (MPTCP) in 2010 [51]. SCTP uses only one path for transfer and keeps the other available paths for packet retransmission or for backup in case of handover or link failure. SCTP suffered however from the middleboxes blocking problem for SCTP packets.

Frequency Resources Aggregation

Since the operator's first choice is to add more capacity on licensed spectrum, carrier aggregation (CA) technology [32] has been standardized in Long Term Evolution (LTE) Releases 10–12. CA was first proposed to aggregate multiple small band segments into maximum 100 MHz virtual bandwidth to achieve higher data rate in LTE small cells.

Frequency multi-connection is also being standardized by 3GPP. LTE dual connectivity is introduced in Release 12 [15] as a realization of different spectrum allocation between a macro cell and a small cell. Several work items in Release 13 differentiated between dual connectivity in LTE/LTE-A HetNets, the License Assisted Access (LAA), and in LTE/WLAN HetNets, the LTE/WLAN Aggregation (LWA).

Interworking Types

Several heterogeneous network types were considered in the literature. Heterogeneity in wired networks mainly consisted in accessing a server using more than one ISP, which means different routes. Generally, wired networks mutilhoming is considered as redundancy in case of failure. Few works tackled multihoming in such networks, we note [34] in which the authors conducted a study on multihoming

streaming in a residential context using a DSL and a cable connection. This study showed significant QoS improvement for connection splitting and migration in case of congestion.

Conversely, wireless networks interworking gained a huge reputation. Several HetNet models were proposed along with performance evaluation and interworking technologies standardization. Next, we present two main categories for wireless networks interworking:

(i) interworking between access networks with the same technology, mainly 3GPP, and

(ii) interworking between different wireless technologies with a focus on the interworing between 3GPP and WLAN networks.

Inter-3GPP interworking

Network densification using LTE small cells has been an important evolution direction in 3GPP, since LTE Release 10, to provide the necessary means to accommodate the anticipated huge traffic growth. Moreover, LTE small cells can be deployed both with macro coverage and standalone, indoor or outdoor, and can also be deployed sparsely or densely based on each case requirements. LTE interference coordination in such HetNets is widely studied and several radio coordination features are proposed. For example, we note downlink joint transmission, dynamic point blanking known as coordinated scheduling and enhanced inter-cell interference coordination (eICIC).

3. Heterogeneous Interworking

The ability to exploit different access network technologies while providing a seamless subscriber experience has a clear appeal for all service providers and network operators. This is why interworking between HetNets was adopted. Several combinations of access networks were studied including, but not limited to, UMTS/WiMAX [32], WiFi/UMTS [33], WiFi/WiMAX [44] WiFi/HSDPA [38], WiFi/LTE [32, 36], and recently in 2017 mmWave/LTE [37]. However, not too many studies considered simultaneous multihoming. In the following, we present an overview of research works concerning different cases of heterogeneous interworking.

Network Selection Decision

The network selection strategy in HetNets in the literature can be classified into three approaches: network centric, user centric, and hybrid decisions. We present here an overview for different research works in this domain and their contributions for network selection decision.

Network centric strategies generally propose a central scheduler managed by the operator. This central scheduler takes into consideration resource allocation between cell users. Several works addressed the interworking between HetNets using network centric scheduler, we note [36, 38, 40]. Alternatively, user centric strategies delegate the traffic splitting or offloading to the users. For example, the user equipment might decide based on the battery power level combined with the consumption on each access network with preferring to offload on WiFi networks in the battery saving mode [33, 37].

RAN Cloudification

Aiming to fill the blanks in the 5G's complete image, we introduce in this section the virtual radio access network (V-RAN). The rationale behind VRANs starts with the emergence of cloud computing such as Amazon Web Services, Microsoft Azure and Google App Engine. In parallel, the rapid growth in mobile media applications and platforms was limited by energy and computational resources which imposed restrictions on the advancement of multimedia applications. That's why cloud computing was proposed as a support for mobile platforms by leveraging the heavy-computational services by executing them on the cloud. The mobile cloud computing [38] was considered as the intersection between mobile computing and cloud computing. Cloud radio access networks (Cloud-RAN or C-RAN) architecture is considered as an innovation in HetNets. C-RAN allows scaling the mobile data network effectively under recent network challenges. C-RAN reduces both expenditures of mobile networks that are facing exponentially increasing data traffic demand [39] [40]. A logical evolution of C-RAN architecture is a V-RAN, a programmable architecture that is software definable and tuneable.

Macro cell

An LTE eNodeB is composed of one baseband unit (BBU) and up to three remote radio heads (RRHs) that can be connected. To connect the BBU and each RRH, an optical interface compliant with the common public radio interface (CPRI) specification, which is standard, is required (see Fig. 1.7). The BBU is responsible for digital baseband signal processing. IP packets received from the core network are modulated into digital baseband signals and transmitted to the RRH. The digital baseband signals received from the RRH are demodulated and IP packets are transmitted to the core network. As for RRH, an RRH transmits and receives wireless signals. An RRH converts the digital baseband signals from BBU that are subject to protocol-specific processing into radio frequency signals and power amplifies them to transmit them to UE. On the contrary, the RF signals received from UE are amplified and converted into digital baseband signals for transmission to the BBU.

C-RAN/V-RAN

In C-RAN, the RRHs are located at the cell site and the BBU is implemented separately and performs centralized signal processing for the RAN. The decentralized BBU enables agility, faster delivery, cost savings and improved coordination of radio capabilities across a set of RRHs. A number of BBUs can be aggregated to form a pool of baseband units (BBU pool).

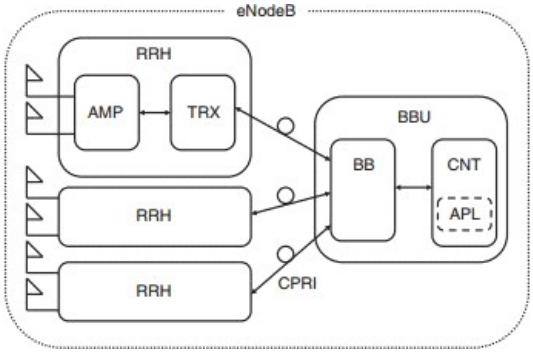

Figure 1.7: eNodeB hardware architecture (Source: [31]).

In other words, V-RAN will open the door for many new applications in 5G. For example, it offers the possibility of using signal processing software dedicated to a special purpose based on the actual service. However, the realization of these benefits requires suitable strategies for an efficient usage of computing resources [25] [26], energy efficient resource allocation [27], sufficient fronthaul capacity [48] and effective BBU placement [29].

Functional Splitting

The C-RAN architecture can be divided into two types, based on the RRH and BBU functionalities: Full Centralization and Partial Centralization.

In full centralization, the functionalities of Layer 1, Layer 2, Layer 3 and signaling as well as operations and maintenance (O&M) are concentrated in the BBU, while RRH has only the radio functionalities as shown in Fig. 1.8. This provides optimum architecture for implementing network optimization techniques, however, it requires a large bandwidth and very low latency link to BBU hotel, to carry the baseband in-phase/quadrature (I/Q) signals.

Partial centralization's baseband processing functions (Layer 1) are

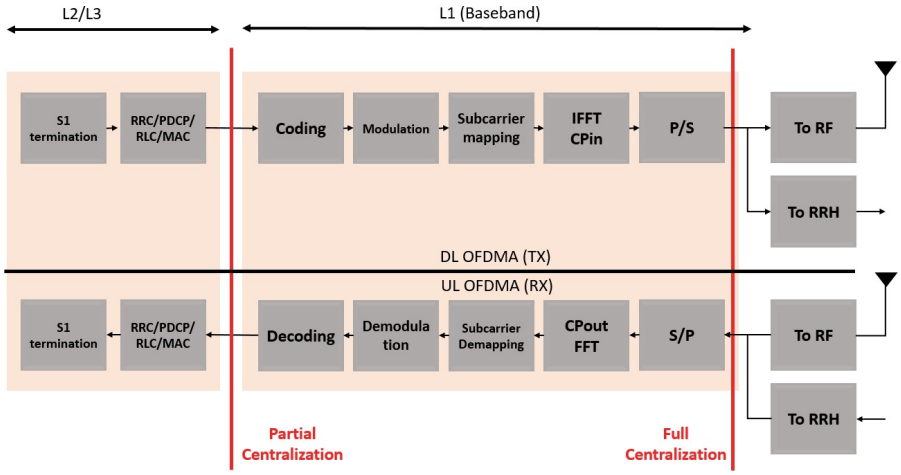

Figure 1.8: Functional splitting of full and partial centralization.

located in the RRH along with radio functions (see Fig. 1.8). This configuration greatly reduces front-haul bandwidth requirements as compared to full centralization. In return, bringing baseband processing in the RRH level makes the upgrade and multi-cell collaborative signal processing less convenient [40].

Resource Allocation Strategies

Resource allocation and scheduling is defined as the act of assigning resources to a set of tasks. A set of constraints must be met by any scheduler such as deadline and minimum resource allocation. The

decision and the scheduling problems address the feasibility of the scheduling. Resource scheduling started with the periodic scheduling in 1973 [22] by assigning zero or one resources at a time. Then another version allows sharing a resource or assigning more than one resource at a time. Among the proposed single-resource scheduling algorithms we note First In First Out (FIFO), Earliest Deadline algorithm (EDF) [22], Round Robin (RR), fair queuing (max-min fair scheduling), proportionally fair scheduling, and Scheduling optimization problems.

4. 5G and Energy Issues

The Information and Communications Technologies (ICT) account for a considerable portion of the total energy consumption. Statistics of 2017 tell that the annual average power consumption by ICT industries was over 200 GW, where telecommunication infrastructure and devices accounted for 25%. Moreover, it is expected that in 5G era, millions more base stations with higher functionality and billions more devices with ever higher data rates will be connected [31]. Therefore, dramatic improvements of Energy Efficiency (EE) are required to ensure sustainable energy consumption in ICT.

Various efforts are done to cut down the energy consumption of telecommunication networks. The Energy Aware Radio and Network Technologies (EARTH) project sponsored by EU, has built a framework to support the EE evaluation over the large scale and long term, which is named the EARTH Energy Efficiency Evaluation Framework (E3F). E3F offers the power consumption breakdown for eNodeB components of LTE wireless system. Meanwhile, a flexible power model is built to support the E3F evaluation, which considers differentiation of BSs types. Furthermore, each type of BS is divided into a group of hardware components. The power of each hardware component is affected by several scaling factors, including bandwidth, antenna, modulation, coding rate, and load as presented in [36].

- Energy consumption
- Energy consumption in cellular networks
- Energy consumption in cellular networks could be evaluated generally by considering the power consumed by all the components as well as the dynamic radio power used for transmission function of the load, or particularly by considering the power consumed by each allocated resources.

The consumed power at the base station follows the model provided by EARTH in generalized to all BS types, including macro, micro, pico and femto BSs. Different transceiver (TRX) parts power consumption is analyzed:

Antenna interface: The influence of the antenna type on the power efficiency is modeled by a certain amount of loss mainly at the feeder.

Power amplifier (PA): The power consumption in PA suffers from nonlinear effects which rises the poor power efficiency ηP A.

Radio Frequency RF: The RF power consumption depends of the required bandwidth, the allowable signal-to-noise-and-distortion ratio,and the resolution of the analog-to-digital conversion.

Baseband unit (BB): The BB unit power consumption includes the power consumed by functions such as filtering, modulation/demodulation, digital pre-distortion, signal detection, and channel coding/decoding.

Power supply and cooling: The power supply and active cooling consumption is presented as a loss that scales linearly with the power consumption of other components.

Energy Consumption in WiFi

The energy consumption in WiFi is less costly than cellular networks because of the reduced coverage and the lower number of users. The power consumption in this case depends of the AP's two states: Idle or Dynamic. In a WiFi AP, the power consumption of PA, RF, BB, and power supply and cooling components are reduced or neglected.

Energy Consumption in mm-wave

In a mm-wave small cell, the power consumption includes the baseband functions, the RF chains and the phase shifters. The other power consumingpart is the power amplifier (PA) which is the most power consuming part in a mm-wave access network. The power consumption in a mm-wave small cell depends of AP's state: Idle or Dynamic.

Energy Efficiency Maximization

EE and sustainability of 5G networks have recently received significant attention from mobile operators, vendors and research projects.

A large amount of work has been reported on EE resource allocation in mobile networks. An energy efficient analysis was provided for LTE HetNets in using realistic power models defined in the EARTH project. Mainly, energy saving techniques such as sleep mode were proposed for idle femto cells. In the same way, authors in proposed small cells activation for the offloading from macro cells to small cells as a strategy to increase power savings.

As for HetNets with multihoming, authors in and developed an uplink and downlink energy efficient allocation model for bandwidth and power resources in a heterogeneous wireless network. In the downlink case, they adopted a win-win strategy that achieves cooperation between different operators. Similar works on network resource allocation with multihoming are presented in with power consumption minimization.

Conclusion

We presented in this paper a general overview of HetNets in 5G cellular networks. HetNets emerged as a promising low-cost approach for network densification. The interworking schemes range from load balancing, to offoading and multihoming; the latter being the focus of the present paper. We described multihoming aspects and technology enablers available in 3GPP releases and those proposed by IETF. These technologies mainly include mobility protocols, transport layer's protocols, and dual connectivity mechanism in 5G. We reported on works on heterogeneous networks interworking, highlighting different network selection strategies.

We also described V-RAN's architecture and defined BBU and RRH entities based on the different functional splitting types. We showed that BBU virtualization offers new efficiency and coverage enhancements by means of CoMP and eICIC. We reported on resource allocation works for both single type and multiple types of resources. We focused on proportional fairness and dominant resource fairness

strategies for single resource and multi-resource allocations, respectively. We finally presented energy consumption aspects in different wireless networks, described power consuming parts and reported different energy efficiency works in the literature, for HetNets, C-RAN and multihoming.

REFERENCES

1. Nikola Tesla. Nikola tesla sees a wireless vision. http://www.tfcbooks.com/tesla/ 1915-10-03.htm. [Accessed: Apr. 26, 2021].
2. Ericsson White Paper. 5g radio access, capabilities and technologies. http://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf, Apr. 2016. [Accessed: Feb. 17, 2021].
3. M. Agiwal, A. Roy, and N. Saxena. Next generation 5g wireless networks: A comprehensive survey. IEEE Communications Surveys Tutorials, 18(3):1617–1655, thirdquarter 2016.
4. 5G PPP Architecture Working Group. View on 5g architecture. White Paper, Jul. 2016. NGMN Alliance. 5G White Paper – Final Deliverable. Technical report, White Paper, Feb. 2015.
5. Jose F. Monserrat, Genevieve Mange, Volker Braun, Hugo Tullberg, Gerd Zim- mermann, and O¨ mer Bulakci. Metis research advances towards the 5g mobile and wireless system definition. EURASIP Journal on Wireless Communications and Networking, 2015(1):53, 2015.
6. A. Kostopoulos, G. Agapiou, F. C. Kuo, K. Pentikousis, A. Cipriano, D. Panaitopol, D. Marandin, K. Kowalik, K. Alexandris, C. Y. Chang, N. Nikaein, M. Goldhamer, A. Kliks, R. Steinert, A. M¨ammel¨a, and T. Chen. Scenarios for 5g networks: The coherent approach. In 2016 23rd International Conference on KjTelecommunications (ICT), pages 1–6, May 2016.
7. Qualcomm. Initial concepts on 5G architecture and integration. Deliverable D3.1, 2016.
8. FCC. FCC Increases 5GHz Spectrum for Wi-Fi, Other Unlicensed Uses. https://www.fcc.gov/document/ fcc-increases-5ghz-spectrum-wi-fi-other-unlicensed-uses, Mar. 2014.
9. Ieee standard for information technology - telecommunications and information ex- change between systems - local and metropolitan networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications: Higher speed physical layer (phy) extension in the 2.4 ghz band. IEEE Std 802.11b-1999, pages 1–96, Jan. 2000.
10. S. G. Sankaran, B. J. Zargari, L. Y. Nathawad, H. Samavati, S. S. Mehta, A. Kheirkhahi, P. Chen, K. Gong, B. Vakili-Amini, J. A. Hwang, S. W. M. Chen, M. Terrovitis, B. J. Kaczynski, S. Limotyrakis, M. P. Mack, H. Gan, M. Lee, R. T. Chang, H. Dogan, S. Abdollahi-Alibeik, B. Baytekin, K. Onodera, S. Mendis,A. Chang, Y. Rajavi, S. H. M. Jen, D. K. Su, and B. A. Wooley. Design and imple- mentation of a cmo 802.11n soc. IEEE Communications Magazine, 47(4):134–143, Apr. 2009.
11. Iso/iec/ieee international standard - information technology – telecommunications and information exchange between systems – local and metropolitan area net- works – specific requirements – part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 4. ISO/IEC/IEEE 8802- 11:2012/Amd.4:2015(E) (Adoption of IEEE Std 802.11ac-2013), pages 1–430, Aug. 2015.
12. Iso/iec/ieee international standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks– specific requirements-part 11: Wireless lan medium access control (mac) and physi- cal layer (phy)

specifications amendment 3: Enhancements for very high throughput in the 60 ghz band (adoption of ieee std 802.11ad-2012). ISO/IEC/IEEE 8802- 11:2012/Amd.3:2014(E), pages 1–634, Mar. 2014.

13. E. Perahia, C. Cordeiro, M. Park, and L. L. Yang. Ieee 802.11ad: Defining the next generation multi-gbps wi-fi. In 2010 7th IEEE Consumer Communications and Networking Conference, pages 1–5, Jan. 2010.
14. 3GPP. (E-UTRAN), Overall description, Stage 2 (Release 12). TS36.300, v12.6.0.
15. ETSI TR 101-957. Requirements and architectures for interworking between hiper- lan/2 and 3G cellular systems. Technical report, ETSI, 2001. Online; accessed 24-Jan-2016.
16. Alcatel-Lucent. Wifi roaming-building on andsf and hotspot 2.0, 2012. 3GPP. Architecture enhancements for non-3gpp accesses. Technical specification TS 23.402, 2012. Release 10.
17. Victor C. M. Leung. Multihomed Communication with SCTP (Stream Control Transmission Protocol). Auerbach Publications, Boston, MA, USA, 2013.
18. X. Lagrange. Very tight coupling between lte and wi-fi for advanced offloading procedures. In 2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pages 82–86, Apr. 2014.
19. 3GPP TS 36.932. Scenarios and requirements for small cell enhancements for eutra and eutran. Release 12, Version 12.1.0, Oct. 2014.
20. J. Robson. A white paper by the ngmn alliance: Small cell backhaul requirements. Next Generation Mobile Networks, Jun. 2012.
21. 3GPP. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description, Stage 2. TS 36.300, v 12.7.0, Oct. 2015.
22. B. Bangerter, S. Talwar, R. Arefi, and K. Stewart. Networks and devices for the 5g era. IEEE Communications Magazine, 52(2):90–96, Feb. 2014.
23. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang. What will 5g be? IEEE Journal on Selected Areas in Communications, 32(6):1065–1082, Jun. 2014.
24. F. Khan, Z. Pi, and S. Rajagopal. Millimeter-wave mobile broadband with large scale spatial processing for 5g mobile communication. In 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pages 1517–1523, Oct. 2012.
25. O. El Ayach, S. Rajagopal, S. Abu-Surra, Zhouyue Pi, and R.W. Heath. Spatially sparse precoding in millimeter wave mimo systems. Wireless Communications, IEEE Transactions on, pages 1499–1513, Mar. 2014.
26. Z. Pi and F. Khan. An introduction to millimeter-wave mobile broadband systems. IEEE Communications Magazine, 49(6):101–107, Jun. 2011.
27. H. Peng, T. Yamamoto, and Y. Suegara. Extended user/control plane architec- tures for tightly coupled lte/wigig interworking in millimeter-wave heterogeneous networks. In 2015 IEEE Wireless Communications and Networking Conference (WCNC), pages 1548–1553, Mar. 2015.
28. 3GPP TS 36.300. E-UTRA and E-UTRAN, overall description. v12.1.0.
29. Wonyong Yoon and Beakcheol Jang. Enhanced non-seamless offload for lte and wlan networks. Communications Letters, IEEE, 17(10):1960–1963, Oct. 2013.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 15-23 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

РОЛЬ МОТИВАЦИОННОЙ ХАРАКТЕРИСТИКИ В ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ
ROLE OF MOTIVATIVE CHARACTERISTICS IN CYBER SECURITY ONTOLOGY

д.п.н., профессор РАЕ Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Professor of RAE, Igor Kozubtsov,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, Lesya Kozbtsova,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., доцент Лещина Валерий Александрович, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, Associate Professor, Valery Leshchina Lutsk National Technical University, Lutsk, Ukraine

АННОТАЦИЯ. Актуальность темы исследований о необходимости обеспечения кибербезопасности информационных систем и технологий в образовании обусловлена постоянно возрастающей уязвимостью, а также скрытым рыском потери активов учебных заведений.

Основных аспекты работы. В статье поднимается вопрос о необходимости рассмотрения обеспечения кибербезопасности информационных систем и технологий в образовании. Установлено, что в данное время исследователями не приделано надлежащего внимания вопросу обеспечения кибербезопасности в проектируемых информационных системах и технологиях в сфере образования.

Научная новизна. Научная новизна темы заключается в постановке задании о необходимости решение научно-практической задачи обеспечения кибербезопасности информационных систем и технологий в образовании.

КЛЮЧЕВЫЕ СЛОВА: *кибербезопасность, мотивация, характеристика, онтология, киберпротивостояние*.

ABSTRACT. The relevance of the research topic on the need to ensure the cybersecurity of information systems and technologies in education is due to the constantly increasing vulnerability, as well as the hidden risk of losing assets of educational institutions.

The main aspects of the work. The article raises the question of the need to consider the provision of cybersecurity of information systems and technologies in education. It is established that at this time, researchers have not paid proper attention to the issue of ensuring cybersecurity in the projected information systems and technologies in the field of education.

Scientific novelty. The scientific novelty of the topic lies in the formulation of a task about the need to solve the scientific and practical problem of ensuring the cybersecurity of information systems and technologies in education.

KEYWORDS: *cybersecurity, education, information system, technology, destructive information influence, cyber security, methodology.*

ВВЕДЕНИЕ

В настоящее время в многочисленных нормативных документах по вопросам обороны и безопасности любого государства ведущее место отводится проблеме противодействия киберугроз (КУ). Например, в [1; 2] КУ отнесены к актуальным угроз национальной безопасности государства, а создание системы кибербезопасности (КБ) и защиту от кибернетических атак определен неотложными задачами.

Анализ причин возникновения проблемы показал, что такими причинами являются:

наличие негативно настроенных группировок, которые желают реализации противоправных действий в кибернетическом пространстве путем нарушения целостности, доступности и конфиденциальности информации для и нанесения вреда информационным ресурсам и телекоммуникационным системам;

группировка программистов типа «хакер» гораздо быстрее создает вредоносное программное обеспечение нежели обновляется антивирусное (программное обеспечение);

эффективность применения информационных технологий и вредоносного программного обеспечения в

кибернетическом пространстве в интересах осуществления военно-политического и силового воздействия противоборства, враждебной информационной / кибероперации, поддержки терроризма и проведения хакерских атак.

Именно в ходе создания и настройки системы связи происходит выявление и обеспечение защиты от стремительное развитие кибернетических угроз.

Современные средства киберзащиты информации принимаются на вооружение с определенными трудностями, в связи с отсутствием достаточного финансирования.

Поэтому, учитывая выше изложенного, по нашему мнению, возникла необходимость в данной работе рассмотреть отдельный аспект, который связан с необходимостью изучения мотивационной характеристики защитника киберпространства что бы своевременно исключать смену позиции защитник-нарушитель.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Автор работы [3] при создании модели угроз информации и механизма ее эффективной защиты описывают модель нарушителя, как абстрактное формализованное или неформализованные описание действий нарушителя, который отражает его практические и теоретические возможности, априорные знания, время, место действия и тому подобное. Даная работа вдохновила на продолжения авторских исследований. Так в работе [4] обращено внимание на мотивационный портрет участники кибернетического противостояния, который меняется от множества условий. В связи с этим обстоятельством акцентировано внимание участников научно-практической конференции «Применение информационных технологий в подготовке и деятельности сил охраны правопорядка» (Харьков, 17-18 марта 2016 г.) на необходимость проведения исследований по более подробному изучению мотивационной характеристики военнослужащих при допуске их к кибернетическому противостоянию [5].Таким образом, не решенным вопросом является обоснование моделей участников киберпространства на основе классификации, что бы упростило процедуру математического расчета, а также сделало невозможным возникновение парадокса в случае отсутствия каких-либо расчетных данных.

ЦЕЛЬ СТАТЬИ

Раскрыть основные результаты исследования вопроса о необходимости изучения мотивационной характеристики участников противостояния в киберпространстве, от которой в первую очередь зависит изменения онтологии кибербезопасности.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Наше исследование основывается на предложенной стратегии игры в киберпространстве [6] и модели [7] при оценке устойчивости функционирования критическая информационная инфраструктура. В виду того, что данная модель используется в исследовании проблемы киберживучести энергосистемы Украины [8], тогда можно утверждать о ее адекватности и для нашего рассматриваемого случая. Таким образом, нами синтезировано графическая модель возможного противоборствия в киберпространстве.

В работе [9] автор четко дает понятие кибератаки, как формы враждебных (противоправных) действий в киберпространстве; действия, направленные против кибернетических систем, информационных ресурсов или информационной инфраструктуры для достижения какой-либо цели и осуществляемые при помощи специальных программно-аппаратных средств и приемов (способов) воздействия.

В контексте данной работы не будем рассматривать задачи, формы и способы ведения войн в киберпространстве, исчерпывающая информации представлена в работе [10].

Для понимания киберпротивостояние приведем наглядный пример в виде рисунка (рис. 1). Однако, при внимательном рассмотрении модели, представленной на рис. 1, можно обратить внимание, что не отображается блок мотивации участников возможного противоборствия в киберпространстве.

В тоже время очень наглядно мотивационная характеристика, как условия, продемонстрировано в работе [11], можно несущественно изменив его таким образом, чтобы оно решал нашу задачу исследования. Конечный результат предлагается дополнить предложенную ранее усовершенствованная онтология кибербезопасности.

Рассматривая киберугрози в контексте государства следует рассмотреть общую классификация видов угроз кибербезопасности любого государства, систематизировав ее представим в табл. 1 и устойчивые к тенденциям развития киберугроз в мировом информационном пространстве [12].

Таблица 1 – Угрозы кибернетической безопасности государства

Вид угрозы	Краткое содержание (характеристика)
Кибервойна	Большинство стран мира активно наращивает свои потенциалы в сфере обороны в направлении усиления кибервозможностей ведения боевых действий и защиты от аналогичных действий со

	стороны противника, поскольку все более актуальными становятся новые киберугрозы. Внедрение ведущими странами современных кибервооружений превращает киберпространство в сферу ведения боевых действий, а в ближайшем будущем уровень обороноспособности страны будет определяться в т.ч. наличием у нее эффективных подразделений для ведения боевых действий в киберпространстве, способным противостоять киберугрозам в сфере обороны.
Кибертерроризм	Ряд отечественных предприятий, нарушение работы которых может представлять угрозу жизни и здоровью граждан, может стать потенциальной целью для осуществления террористических актов, в том числе - по применению современных информационных технологий. Все большее распространение получает политически мотивированная деятельность в киберпространстве групп активистов (хактивистов), которые осуществляют атаки на правительственные и частные сайты, приводит к нарушениям работы информационных ресурсов, а также репутации и материальных убытков
Кибершпионаж	Не меньшей угрозой является совершение противоправных действий в ущерб третьим странам, которые осуществляются с использованием отечественной информационной инфраструктуры, угрожающих устойчивому и безопасному функционированию национальных информационно-телекоммуникационных систем
Киберпреступность	Преступления с использованием современных информационно-телекоммуникационных технологий становятся все обычной практикой в жизни украинских граждан. Больше всего внимание преступников сосредоточена на попытках нарушения работы или несанкционированного использования возможностей информационных систем государственного, кредитно-банковского, коммунального, оборонного и производственного секторов

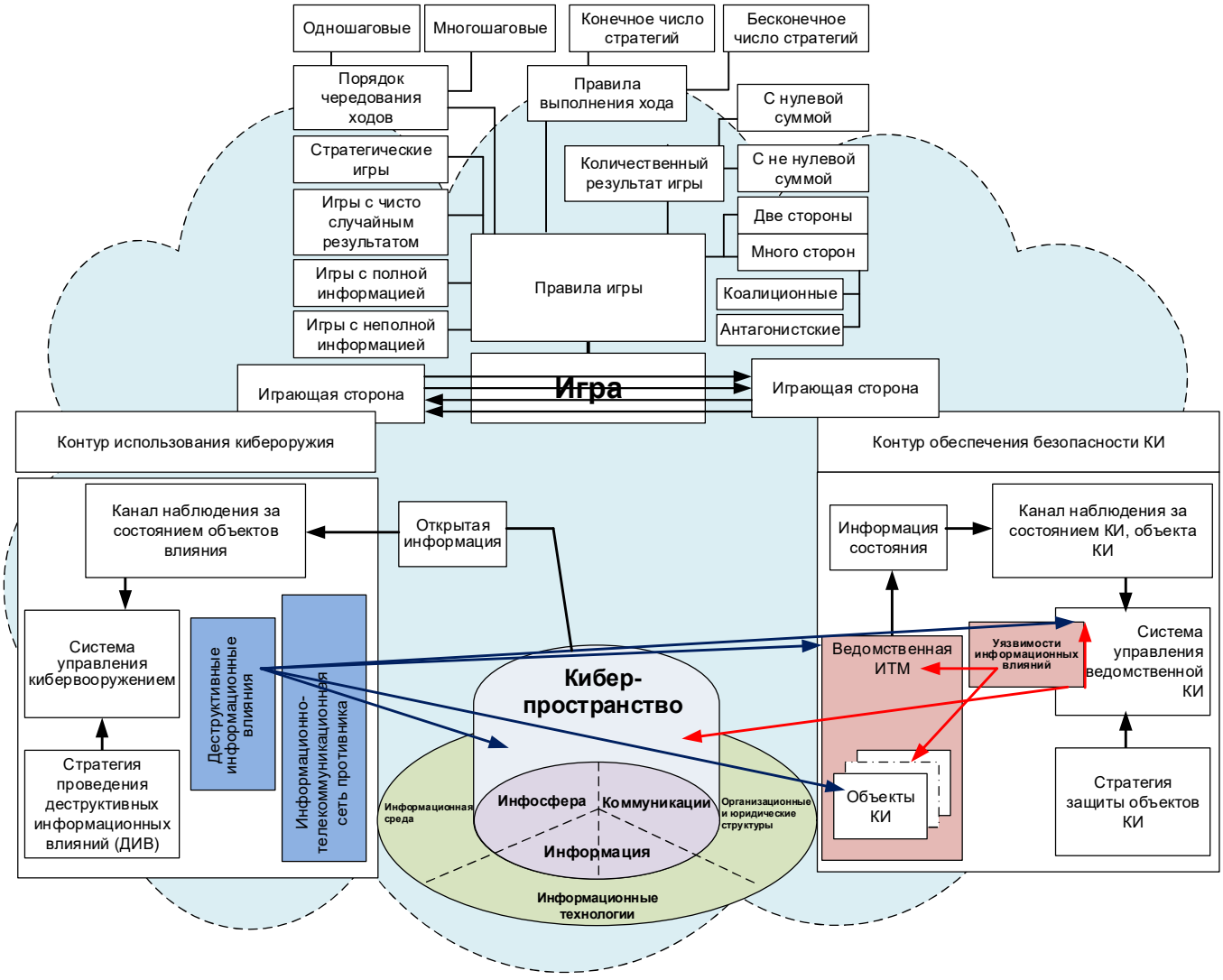

Рис. 1 – Модель противостояния в киберпространстве

Для разработки действенных путей борьбы с источниками киберугроз необходимо выяснить мотивацию всех участников киберпространства. По природе мотивы могут быть совершенно разными: от полного их отсутствия, стихийных бедствий, экономических и политических преимуществ в целенаправленных воздействий вовремя кибервойны (табл. 2).

Таблица 2 – Источники угроз для информации

вид угроз	источники угроз	Мотивация источники угроз
Кибервойна	другие государства	Получение преимуществ во внешнеполитической, внешнеэкономической, военной и других сферах
Кибервойна	политические партии	Получение преимуществ в политической борьбе за власть
Кибертерроризм	преступные группировки	Получение политических, экономических преимуществ, нанесения ущерба
Кибершпионаж	субъекты хозяйствования	Получение преимуществ в конкурентной борьбе, экономические преимущества
Киберпреступность	физические лица	Самоутверждения, получения экономических преимуществ и финансовых вознаграждений
Киберпреступность	Ошибки персонала (умышленные, неумышленные)	Низкая квалификация работников; образа; измена; принуждение

Предоставим описание участников игры.

Авторы работы [12 с. 156] определили субъекты киберпространства только в общем виде не предоставив принадлежность к гражданству. А это, по нашему мнению, важно, поскольку правила поведения в кибернетическом пространстве определяется этическими нормами поведения и нормативно-процессуальным законодательством страны. Зато нормативно-процессуальное законодательство стран мира имеет различия, которые постепенно устраняет глобализационный процесс.

Условно их можно сгруппировать в три группы: граждане страны, люди без гражданства, иностранные граждане. Согласно им, смоделируем следующие модели:

модель нарушителя информационно-киберпространства;

модель защитника информационно-киберпространства.

Также следует условно представить, что воздействие может осуществляться человеком как извне государства, так и изнутри.

Каждая из групп имеет за разногласиями нормативно-процессуальным законодательством страны, в которой она находится и собственных убеждений этическими нормами поведения.

Приближенную классификацию участников кибернетического пространства представлено в табл. 3.

Таблица 3 – Классификация участников кибернетического пространства

Участники киберпространства	уровень сети	Категория пользователя	Модель поведения	
			защитника	нарушителя
граждане своей страны	сеть внутренняя закрытая	военнослужащие; военнослужащие других воинских (силовых) формирований; работники военных (силовых) формирований	+	+ / –
	сеть внутренняя (корпоративная)	граждане своей страны (члены корпорации) нерезиденты (члены корпорации)	+	+ / –
	сеть Интернет	все перечисленные категории граждане	+	+ / –
иностранные граждане	сеть внутренняя закрытая (в пределах своего государства)	граждане страны, которым предоставлен допуск и доступ к сети	– / +	+
	сеть внутренняя (корпоративная)	граждане одной страны (члены корпорации) нерезиденты и резиденты (члены корпорации)	– / +	+
	сеть Интернет	все перечисленные категории граждане	– / +	+
лица без гражданства (находящихся внутри страны)	сеть внутренняя закрытая	доступ запрещен	– / +	+
	сеть внутренняя (корпоративная)	члены транснациональных корпорации	– / +	+
	сеть Интернет	все перечисленные категории граждане	– / +	+
лица без гражданства	сеть внутренняя закрытая	доступ запрещен	– / +	+

(находящихся за пределами страны)	сеть внутренняя (корпоративная)	члены транснациональных корпорации	– / +	+
	сеть Интернет	все категории граждане	– / +	+
провайдеры Интернета	ведущий	материальная мотивация	+	+ / –
	региональный	материальная мотивация	+	+ / –
	периферийный	материальная мотивация	+	+ / –
	проводной	материальная мотивация	+	+ / –
	(Беспроводной) сотовый	материальная мотивация	+	+ / –

Для построения игровой стратегии кибернетической безопасности выяснить вопрос при каких условиях участник кибернетического пространства принимает модель защитника, а при каких нарушителя. На этот вопрос можно частично найти ответ сразу выяснив факторы, влияющие, например, мотивация.

Условную классификацию мотивацию участников кибернетического пространства представлено в табл. 4.

Таблица 4 – Классификация мотиваций участников кибернетического пространства

Мотивации участников киберпространства	Дополнительная классификация	Модель		
		защитника	нарушителя	пользователя
материальные	телекоммуникационные компании	+ / –	+ / –	
	провайдер Интернета	+ / –	+ / –	
	абонент - пользователь	+ / –	+	+
духовные	абонент - пользователь	+	+ / –	+ / –
идейные	политические	+	+ / –	+ / –
	религиозные	– / +	+ / –	+ / –
	истинные патриоты	+	+	+ / –
	неискренни патриоты	– / +	+ / –	+ / –
	криминал	–	+	–
Устойчивое формирование мотивации, не поддается быстрому корректировке	любознательность	– / +	+	+
	энтузиасты	+	+	+ / –
	идиоты	–	+	–
профессиональные	разведчик	+	–	–
	шпион	–	+	–
Инсайдеры	все категории граждане	–	+	+ / –
Типичные условия и факторы влияния на мотивацию, побуждающих человека к правонарушению				
подкуп	все категории граждане	–	+	+ / –
шантаж	все категории граждане	–	+	+ / –
бюрократия	все категории граждане	+	+	+ / –
профессиональные	все категории граждане	+	+	+ / –
болезнь	все категории граждане	+	+	+ / –
особые потребности	все категории граждане	+	+	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	+ / –	–	+

Введя в таблицы 3 и 4 определенные условные сокращения и обозначения, можно математически сформировать матрицу параметров.

При разработке модели нарушителя киберпространства нами изучался опит построение таких моделей исчерпывающе представленных в работах М.М. Войтко [13], А.А. Конева [14], В.В. Семко [15] и других. С точки зрения рассматриваемой задачи интересен результат работы [13], в которой исследователь предложил рассматривать модель нарушителя в следующей математической форме так (1):

$$M_0 = \left(O_p, O_{\ln}, O_a\right) \quad (1)$$

где O_p – местоположение нарушителя;

O_{ln} – профессиональный уровень знаний и умений нарушителя;

O_a – сценарий возможного доступа O_{pn} – первичные знания нарушителя о системе.

Согласно работы [13] $O_p \in \{1, 2, 3\}$, где 1 – нарушитель внешний; 2 – нарушитель внутренний; 3 – преступная договоренность внутренних и внешних нарушителей, например, подкуп, шантаж.

Профессиональный уровень знаний и умений нарушителя $O_{ln} \in \{1, 2, 3\}$, где 1 – низкий уровень; 2 – средний уровень; 3 – высокий уровень.

Первичные знания нарушителя о системе КБ зависят от местоположения нарушителя относительно нее.

Однако автор работы [13] совершенно не учитывает мотивационной характеристики (МХ), как можно увидеть дальше модель в зависимости от этого параметра трансформируется в модель защитника КБ.

Все указанные в табл. 3 участники могут принимать модель защитника или нарушителя кибернетического пространства в зависимости от сложившейся внутренней характеристики мотивации.

В дальнейших исследованиях необходимо определить четко состав участников (организационную структуру) функциональные обязанности, сектор ответственности каждого участника, правила игры всех участников кибернетического пространства.

До сих пор не решенным вопросом является каким образом построить подобную мотивационную характеристику. Предположительно МХ имеет непосредственную связь с иерархической системой потребностей человека – пирамидой потребностей А. Маслоу [16]. В основе этой иерархии лежали наиболее насущные потребности (пища, вода, жилье), а на вершине – более высокие индивидуальные запросы (признание, самовыражение). Когда потребности самого низкого уровня удовлетворены хотя бы частично, человек начинает двигаться к удовлетворению потребностей другого и не обязательно следующего уровня иерархии. В каждый конкретный момент времени человек будет стремиться к удовлетворению той потребности, для нее важнее или сильной. Основной недостаток теории Маслоу сводится к тому, что ей не удалось учесть индивидуальные отличия людей. Исходя из прошлого опыта, один человек может быть больше заинтересована в самовыражении, в то время как поведение другого будет в первую очередь определяться потребностью в признании, социальными потребностями. Согласно результатов исследований [16] на психические (физиологические) потребности среднего гражданина удовлетворяются на 85%, экзистенциальные – на 70, социальные – на 50, престижные – на 40, самовыражения – на 10%. Статистика говорит, что только один-два процента людей стремится к вершине пирамиды Маслоу.

Что касается склонность всех категорий граждан можно с легкостью спрогнозировать вероятность наступления событий зная физиологическое положение страны или другие критерии по Маслоу.

Авторами [17] разработан принцип рефлексного управления, что нацелен на захват и удержание информационного превосходства над противником. На учет этого принципа акцентируют авторы монографии [18] поэтому игнорировать его неуместно. Цель принципа достигается путем управления личностью, если предложения внешней среды превышают ожидания личности. Модель представлена на рис. 2. Она напоминает модель рычагов, на чаше которых с одной стороны модель поведения защитника КБ, а на противоположной модель нарушителя КБ. Склонение человека к модели защитника или нарушителя КБ напрямую зависит от состояния мотивационной характеристики (МХ).

Отметим, что предложения внешней среды – это не только подкуп, шантаж, а еще выполнения задания, при этом человек делает правонарушения. Типичные условия и факторы влияния на мотивацию, побуждающих человека к правонарушению приведена в табл. 4. Следует обратить внимание на такой фактор как оценка уровня денежного обеспечения защитника КБ, а также чрезмерного бюрократического подхода допуска человека к системе КБ, условий ее эксплуатации, то есть создание деструктивных и некомфортных условий пользователю. Развивая данное направления исследования было подробней изучено и установлено дополнительные факторы, которые способствуют законопослушного гражданина к сознательному правонарушение т.е. с точки Закона стать нарушителем.

Таким образом, еще раз акцентируем внимание на то, что в результате законопослушный гражданин вынужден сознательно идти на правонарушение что бы выполнить задание руководства в установлений строк и надлежащим уровнем.

Рис. 2 – Инвариантная модель поведения участника киберпространстве

С учетом рис. 2 предложенная ранее усовершенствованная онтология кибербезопасности [19] примет дальнейшее развитие. Для этого изобразим логическое место предложенного алгоритма, результирующий результат отобразим на рис. 3.

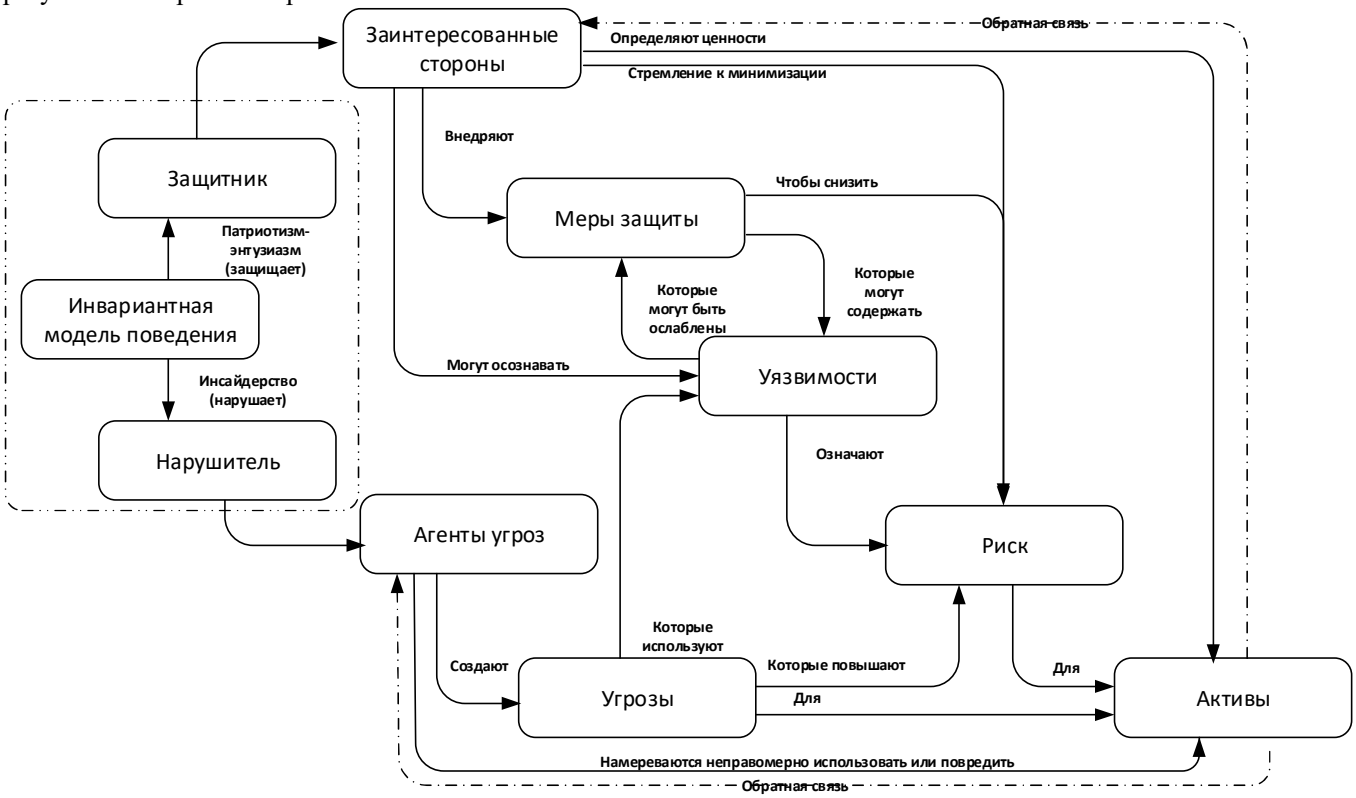

Рис. 3 – Функциональная зависимость онтология кибербезопасности

При моделировании следует учитывать человеческий фактор, который имеет место. Практика показывает, что на появление этого фактора влияют множество параметров, в том числе условия труда и отдыха. При определении степени влияния человеческого фактора на функционирование большой информационной системы нужно учитывать результаты о влиянии человеческого фактора на работоспособность информационных систем

[20].

ВЫВОДЫ

По результатам проведенного исследования можно сделать следующие выводи, которые вытекают из добавленных компонентов на функциональную зависимость онтология кибербезопасности.

1. Рационально необходимым является построения моделей нарушителя и защитника киберпространства с учетом мотивационной характеристики (портрета).

2. Созданием положительной мотивационной характеристики у защитников киберпространства уменьшает вероятность того, что ее защитник превратится в нарушителя киберпространства.

3. Для изучения мотивационной характеристики защитников киберпространства мы видим необходимость в подборе специальных психологических тестов. Такое тестирование позволит своевременное выявление потенциального инсайдера, его потребностей и склонности, а, следовательно, прогнозирования способности лиц к нарушениям в кибернетическом пространстве.

4. Мы намеренно не рассматривали нарушителей, имитирующие (создают) технические, вычислительные средства обработки информации (компьютера, ноутбуки, планшеты, мобильные приложения), поскольку они созданы биологической лицом (индивидуумом) исходя из собственной мотивационной характеристики. В таком случае они работают по определенному алгоритму. Задача может осложниться в будущем, когда искусственный интеллект начнет создавать собственное киберугрозу, что не исключается в будущем.

НАУЧНАЯ НОВИЗНА

В работе, в отличие от других, систематизировано и синтезировано в целостную систему последовательных явлений, а именно вытекающих от модели противостояния в киберпространстве и основных киберугроз до классификации классификация участников кибернетического пространства, их мотивационной характеристики до места и роли в усовершенствованной онтологии кибербезопасности. Эта информация в дальнейшем позволит упростить процедуру математического расчета, а также исключает возможность возникновения парадокса в случае отсутствия каких-либо расчетных данных.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Перспективы дальнейших исследований целесообразно сосредоточить на основе обоснованных участников доступа к киберпространству и их мотивационной характеристике, приступить к разработке стратегии кибербезопасности обоснованной на игровом подходе.

СПИСОК ЛИТЕРАТУРЫ

1. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України № 390/2012. URL: http://zakon3.rada.gov.ua/laws/ show/390/2012.
2. Про Доктрину інформаційної безпеки України: Указ Президента України №514/2009. URL: http://zakon2.rada.gov.ua/laws/show/514/2009.
3. Капустян М.В., Орленко В.С., Хорошко В.О. Створення моделі загроз інформації та механізму її ефективного захисту // Вісник Національного університету «Львівська політехніка». 2006. № 551: Автоматика, вимірювання та керування. С. 58 – 63.
4. Козубцов І.М. Про мотиваційний портрет учасники кібернетичного протистояння // Актуальні проблеми розвитку науки і техніки: Матеріали першої міжнародної науково-технічної конференції. К.: ДУТ, 2015. С. 208 – 211.
5. Козубцов І.М., Козубцова Л.М., Живило Є.О., Куцаєв В.В. Про необхідність дослідження мотиваційної характеристики військовослужбовців при допуску їх до кібернетичного протистояння // Науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» (Харків, 17-18 березня 2016 р.). Харків: Національна академія Національної гвардії України, 2016. С. 35 – 36.
6. Козубцов І.М., Козубцова Л.М Стратегія гри в кібернетичному просторі // Матеріали Міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» (Київ, 17– 20 листопада 2015 р.). Київ. Державний університет телекомунікацій, 2015. Том ІІІ Розвиток інформаційних технологій. С. 52 – 54.

7. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Т. 28. №4. С. 59 – 67.
8. Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал "Електронне моделювання". 2019. Т.41. №1. С. 43 – 54.
9. Антонович П. О сущности и содержании кибервойны // Военная мысль. 2011. №7. С. 39 – 46.
10. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. 2011. № 3 С. 35 – 42.
11. Гончар С., Леоненко Г., Юдін О. Загальна модель загроз безпеці інформації АСУ ТП // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. 2015. Вип. 1(29). С. 78 – 82.
12. Черняк О.Р., Федулов О.В. Тенденції розвитку кіберзагроз у світовому інформаційному просторі // Сучасні інформаційні технології у сфері безпеки та оборони. 2014. №1(19). С.155 – 158.
13. Войтко М.М. Побудова узагальненої моделі загроз для систем Інтернет-банкінгу // Фінансовий простір. 2014. №3 (15).С. 33 – 38.
14. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУРа. Томск, 2012. № 1(25). Часть 2. С. 34 – 40.
15. Семко В.В. Модель конфлікту взаємодії об'єктів кібернетичного простору // Проблеми інформатизації та управління. 2012. Вип. 2(38). С. 88 – 92. URL: http://jrnl.nau.edu.ua/index.php/PIU/article/download/6503/7279.
16. Маслоу А. Мотивация и личность / пер. А.М. Татлыбаевой; терминолог. правка В. Данченка. К.: PSYLIB, 2004. 384 с.
17. Лефевр В.А., Смолян Г.Л. Алгебра конфликта. М.: Знание, 1968. 64 с. (Математика, кибернетика).
18. Жарков Я.М., Дзюба М.Т., Замаруєв І.В. Інформаційна безпека особистості, суспільства, держави: підручник. К.: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.
19. Козубцов І.М., Хлапонін Ю.І., Козубцова Л.М. Ідея впровадження зворотного зв'язку як вдосконалення функціональної залежності реалізації кібернетичної безпеки // Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (Харків, 15 березня 2021 р.). Харків. Національна академія Національної гвардії України, 2021. С. 86 – 87.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 24-34 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF THE POST PROCESSING METHODS FOR THE QUANTUM RANDOM NUMBER GENERATORS

Tamari Kuchukhidze, Georgian Technical University, Scientific Cyber Security Association

ABSTRACT: Randomness is widely used in various fields including encryption, statistical analysis and numerical simulations. They are also a fundamental resource in science and engineering. For such applications, we usually need to provide unbiased and independent random bits. This raises the issue of where to get these supposed random bits.
Quantum Random Number Generators (QRNGs) generate real random numbers based on the inherent randomness of quantum measurements. In practice, unfortunately, quantum randomness is inevitably mixed with classical randomness due to classical noise. Also, randomness is often correlated and biased.
It is necessary to process the resulting raw bits sequence and convert them to good quality output values that are as close to uniform distribution as possible. Random extractors are required for this.
We will analyze the randomness obtained by quantum random number generators as well as various examples of postprocessing. We discuss the types of randomness extractors.

Keywords: *quantum, post processing, quantum random number generators, entropy, randomness extractors.*

რეზიუმე: შემთხვევითობა ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. ისინი ასევე ფუნდამენტური რესურსია მეცნიერებასა და ინჟინერიაში. ასეთი აპლიკაციებისთვის, ჩვეულებრივ, გვჭირდება მიუკერძოებელი და დამოუკიდებელი შემთხვევითი ბიტების მიწოდება. ეს აჩენს პრობლემას, საიდან უნდა მიიღოთ ეს სავარაუდო შემთხვევითი ბიტები.
კვანტური შემთხვევითი რიცხვის გენერატორებმა (QRNG) გამოაქვთ ნამდვილი შემთხვევითი რიცხვები კვანტური გაზომვების თანდაყოლილი შემთხვევითობის საფუძველზე. პრაქტიკაში, სამწუხაროდ, კვანტური შემთხვევითობა აუცილებლად შერეულია კლასიკურ შემთხვევითობასთან კლასიკური ხმაურის გამო. ასევე შემთხვევითობა ხშირად კორელირებული და მიკერძოებულია.
აუცილებელია დავამუშავოთ მიღებულ ნედლი ბიტების თანმიმდევრობა და გარდაქმნის კარგი ხარისხის გამომავალ მნიშნელობებად, რომლებიც თანაბარ განაწილებასთან რაც შეიძლება მიახლოებულია. ამისთვის საჭიროა შემთხვევითობის ექსტრაქტორები.
გავაანალიზებთ კვანტური შემთხვევითი რიცხვების გენერატორების მიერ მიღებულ შემთხვევითობას და ასევე დამუშავების სხვადასხვა მაგალითებს. განვიხილავთ შემთხვევითობის ექსტრაქტორების სახეობებს.

საკვანძო სიტყვები: *კვანტური, კვანტური შემთხვევითი რიცხვების გენერატორები, დამუშავება, ენტროპია, შემთხვევითობის ექსტრაქტორები.*

1. შესავალი

შემთხვევითი რიცხვები გადამწყვეტ როლს თამაშობს მეცნიერების, ტექნოლოგიებისა და მრეწველობის ბევრ სფეროში, მაგალითად, კრიპტოგრაფიაში, სტატისტიკაში, სამეცნიერო სიმულაციასა და ლატარიაში [1-5]. ალგორითმულად გამომუშავებული რიცხვები ჰგავს შემთხვევით რიცხვებს, მაგრამ ისინი ნამდვილად არ არიან შემთხვევითი; მათ ფსევდო შემთხვევით რიცხვებს უწოდებენ. ეს რიცხვები წარმოიქმნება კომპიუტერის გამოყენებით, დეტერმინესიული ალგორითმების საშუალებით, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ [6-8]. ფსევდო შემთხვევითი რიცხვების გენერატორები, რომლებიც ემყარება გამოთვლით სირთულეებს, კარგად განვითარდა ბოლო რამდენიმე ათწლეულის განმავლობაში და შეუძლიათ წარმოქმნან შემთხვევითი რიცხვები მაღალი სიჩქარით, მცირე რესურსების გამოყენებით. თუმცა, ფსევდო შემთხვევითი რიცხვების გენერატორების მთავარი ნაკლი არის, რომ ჩვენს მიერ მიღებული შემთხვევითობა არ არის ინფორმაცი-თეორიულად დასაბუთებადი. სინამდვილეში, ყველა პროგრამაზე დაფუძნებული ფსევდო შემთხვევითი რიცხვების გენერატორი შეიძლება განხორციელდეს დეტერმინისტული ალგორითმით, თუკი გავითვალისწინებთ საკმარის გამოთვლით სიმძლავრეს. ეს ფსევდო შემთხვევითობა გამოიწვევს პრობლემებს ბევრ გამოყენებაში, როგორიცაა კრიპტოგრაფია.

ფსევდო შემთხვევითი გენერატორების მიერ შექმნილი უსაფრთხოების პრობლემების გადასაჭრელად შეიქმნა ფიზიკური RNG-ები. კერძოდ, კვანტური მექანიკის ალბათური ბუნება გვთავაზობს ბუნებრივ გზას ინფორმაცია-თეორიულად დამტკიცებადი შემთხვევითი რიცხვების გენერატორების, კვანტური შემთხვევითი რიცხვების გენერატორების (QRNG) შესაქმნელად. საგულისხმოა, რომ ზოგიერთი ფიზიკური RNG შედის მიკროპროცესორებში, თუმცა წარმოქმნილი შემთხვევითობა არ არის კვანტური მექანიკური ხასიათის [9].

თეორიულად, QRNG-ს შეუძლია გამოიმუშავოს შემთხვევითი რიცხვები დასაბუთებადი შემთხვევითობით. პრაქტიკაში კი არ არის ასე, კვანტური სიგნალები (ჩვენთვის ჭეშმარიტი შემთხვევითობის წყარო) აუცილებლად შერეულია კლასიკურ ხმაურთან. ზოგადად, მოწინააღმდეგეს შეუძლია დაარეგულიროს კლასიკური ხმაური და მიიღოს ნაწილობრივი ინფორმაცია შემთხვევითი რიცხვების შესახებ. აქედან გამომდინარე, აუცილებელია გამოვიყენოთ შემდგომი დამუშავების პროცედურა, რათა გამოვავლინოთ ჭეშმარიტი შემთხვევითობა, რომლის შესახებაც ჩვენს მოწინააღმდეგეს თითქმის არ აქვს ინფორმაცია. ამ პროცედურას ეწოდება შემთხვევითობის მოპოვება (randomness extraction), რომელიც ხორციელდება შემთხვევითი ექსტრაქტორების გამოყენებით. სხვა სიტყვებით რომ ვთქვათ, შემთხვევითობის ექსტრაქტორები გამოიყენება ჭეშმარიტი შემთხვევითობის ამოღებისთვის და კლასიკური ხმაურის ეფექტების აღმოსაფხვრელად.

2. დამუშავების ეტაპი

სტანდარტული შემთხვევითი რიცხვის გენერატორები შექმნილია თანაბარი შემთხვევითი სტრინგის წარმოებისთვის. დამუშავების შემდგომი ეტაპი კი ამუშავებს მიღებულ ნედლი

ბიტების თანმიმდევრობას და გარდაქმნის კარგი ხარისხის გამომავალ მნიშნელობებად, რომლებიც თანაბარ განაწილებასთან რაც შეიძლება მიახლოებულია. დამუშავების პერიოდი შეიძლება მოიცავდეს ისეთ ამოცანებს, რომლებიც შეამოწმებენ გენერატორი მუშაობს თუ არა გამართულად ან ხდება საცდელი მნიშვნელობების გენერაცია, სანამ დავაგენერირებთ საბოლოო სტრინგებს [10].

გარდა ამ ამოცანებისა, რომლებიც სხვადასხვა გენერატორისთვის განსხვავებულია, დამუშავების შემდგომი ეტაპის მთავარი მიზანია შემთხვევითობის მოპოვება. ფიზიკური RNGs-ის უმეტესობა შეიცავს რომელიმე ფორმის შემთხვევითობის ექსტრაქტორს, მიკერძოებისა და კორელაციების გასასწორებლად. ისინი ჩნდება გაზომვისა და გენერაციის მოწყობილობების არასრულყოფილებით, თუნდაც გვქონდეს კარგი შემთხვევითობის წყაროები, მაღალი ენტროპიით.

მაღალი ენტროპია არ არის გარანტია იმისა, რომ წარმოქმნილი შემთხვევითი თანმიმდევრობა შესაფერისი იქნება ნებისმიერ შემთხვევაში. მიუხედავად იმისა, რომ არსებობს მეთოდები, რომლებსაც შეუძლიათ რანდომიზირებულ ალგორითმებში გამოსაყენებლად დააფიქსიროონ სუსტი წყაროები, ყველა პროტოკოლი ვერ მუშაობს არასრულყოფილ შემთხვევითობაში. კერძოდ, ბევრი კრიპტოგრაფიული პროტოკოლი ისეთი ამოცანებისთვის, როგორიცაა: ბიტების ვალდებულება, დაშიფვრა, ნულოვანი ცოდნა ან საიდუმლო გაზიარება არ არის უსაფრთხო თუ არ ვიყენებთ თითქმის თანაბარ შემთხვევით მიმდევრობას.

ზოგიერთი აპარატურული შემთხვევითი რიცხვების გენერატორი ერთმანეთში ურევს შემთხვევითობის სხვადასხვა წყაროებს, მათი ბიტების ლოგიკური XOR-ის აღებით ან კრიპტოგრაფიულ ჰეშირების ფუნქციას აწვდის სტრინგებს. ფონ ნოიმანმა შემოგვთავაზა მარტივი მიკერძოების მოშორების მეთოდი, რომლის დროსაც, წარმოქმნილი თითოეული ბიტის წყვილისთვის, შეგვიძლია გავაუქმოთ 00 და 11 შედეგები, მივანიჭოთ 01-ს 0 და 10-ს კი 1. თუკი გვაქვს სისტემური მიკერძოება, ეს მეთოდი ამოიღებს ამ მიკერძოებას, მაგრამ მინიმუმ ნახევრი ბიტების გადაგდების ხარჯზე და ბიტების სიჩქარე ერთი მეოთხედით მაინც შემცირდება (რაც უფრო მეტი ბიტს გადავაგდებთ, მით უფრო მიკერძოებული იყო ორიგინალი მიმდევრობა). ეს ძირითადი მეთოდი, რა თქმა უნდა, დაიხვეწა და უფრო ეფექტური გახდა [11].

სანამ შემთხვევითობის ექსტრაქციას განვიხილავთ უფრო დეტალურად, პირველ რიგში მნიშვნელოვანია განვსაზღვროთ რა არის ჩვენთვის მისაღები თანაბარი შედეგი. ჩვენთვის მნიშვნელოვანი ცნებაა მანძილი განაწილებებს შორის. ორი X და Y განაწილებების ალბათობა, განსაზღვრული ერთსა და იმავე მხარდაჭერაში (მათ შეუძლიათ მიიღონ იგივე მნიშვნელობები სასრულ ანბან A-ში), რომელიც შეგვიძლია განვსაზღვროთ სტატისტიკური მანძილით

$$dis(X,Y) = \max_{a \in A} |Pr_X(a) - Pr_Y(a)|$$

ეს მეტრიკა გვაძლევს მაქსიმალურ განსხვავებას კონკრეტული შედეგის მიღების ალბათობისას, შედარებით განაწილებებში. ვიტყვით, რომ ორი X და Y განაწილება არის ϵ-ახლო, თუკი

$$dis(X,Y) \leq \epsilon$$

შემთხვევითობის ექსტრაქციის მიზანია, მივიღოთ მიმდევრობა, რომელიც რაც შეიძლება ახლოს იყოს თანაბართან. ეს ჩვეულებრივ ნიშნავს, დაუმუშავებელი გამომავალი მნიშვნელობებიდან ავიღოთ n ბიტი და გარდავქმნათ m ბიტების სტრინგად, რომლის განაწილება ϵ-ახლოა U_m-თან ($\{0, 1\}^m$-ში არის თანაბარი განაწილება) მცირე ϵ-სთვის, რომელიც დამოკიდებულია ჩვენ საჭიროებებზე.

იდეალურ შემთხვევაში, ჩვენ გვსურს ექსტრაქტორები, რომლებიც მოგვცემს რაც შეიძლება მეტ გამომავალ ბიტს, მცირე დამატებითი რესურსების გამოყენებით, როგორიცაა გამოთვლის დრო ან დამატებითი შემთხვევითობა. ნედლი მიმდევრობის განაწილების მინიმალური ენტროპია გვაძლევს ზღვარს რამდენი ბიტის ამოღებაა შესაძლებელი. თუ ჩვენ ავიღებთ n ბიტიან სტრინგს ნედლი მიმდევრობიდან, რომელსაც X განაწილებით $H_\infty(X) = k$ მინიმალური ენტროპია გააჩნია, შეგვიძლია ამოვიღოთ მაქსიმუმ k შემთხვევითი ბიტი, რომელიც თანაბართან ახლოსაა. ორიგინალ სიგრძეს არ აქვს მნიშვნელობა. შემთხვევით წყაროს ეწოდება (n, k)-წყარო, თუ ის აწარმოებს n ბიტს $H_\infty(X) = k$ მინიმალური ენტროპიით, X განაწილებიდან.

განვიხილავთ ბიტების თანმიმდევრობის გენერაციის სხვადასხვა მეთოდებს, რომლებიც თანაბართან მიახლოებულ მიმდევრობას გვაძლევენ, მინიმალურ ენტროპიის ზღვართან ახლოს. ასევე განვიხილავთ სხვადასხვა შემთხვევითობის ექსტრაქტორების მიდგომების უპირატესობებსა და შეზღუდვებს.

3. შემთხვევითობის ექსტრაქტორები

შემთხვევითობის ექსტრაქტორები ფუნქციებია, რომლებიც ამოიღებენ თითქმის ერთგვაროვან ბიტებს მიკერძოებული და კორელირებული ბიტების წყაროებიდან. ისინი ენტროპიის სუსტ წყაროს თანაბარი ბიტების გენერატორად გადააქცევენ. ეს ფუნქციები თავიდან შემოიტანეს რანდომიზირებული ალგორითმების შესასწავლად, მაგრამ გახდა ძირითადი ინსტუმენტი თეორიული კომპიუტერული მეცნიერების მრავალ სფეროში. შემთხვევითობის ექსტრაქტორებს და მასთან დაკავშირებული ცნებებს, როგორიცაა დისპერსიები, კონდენსატორები და გაფართოების გრაფიკები, სხვადასხვა გამოყენება გააჩნია და ფსევდო შემთხვევითი რიცხვების გენერატორების მრავალ სფეროში გვხვდება, მათ შორის, შეცდომის გამოსწორების კოდებში, სინჯები, გაფართოების გრაფიკები და სიხისტის გამაძლიერებლები.

განვიხილავთ QRNG–სთვის ყველაზე შესაფერისი ექსტრაქტორების რამდენიმე ცნებას. შემთხვევითობის მოპოვების მრავალი ვარიანტი არსებობს და საბოლოო არჩევანზე გავლენას ახდენს თითოეული მეთოდის სიჩქარე და ტექნიკა. იმისათვის, რომ ეფექტური მეთოდი გვქონდეს და რაც შეიძლება მეტი ბიტი შევინარჩუნოთ, საჭიროა კარგად განვსაზღვროთ ჩვენთვის ხელმისაწვდომი ენტროპია და შემდეგ ავირჩიოთ ადეკვატური შემთხვევითობის ექსტრაქტორი. წინააღმდეგ შემთხვევაში, ექსტრაქტორის ფუნქციის გამომავალ მნიშვნელობებს არ ექნებათ სასურველი თვისებები.

შემდეგში, ჩვენ ჩავთვლით, რომ გვაქვს კარგად აღწერილი შემთხვევითობის წყარო. ვვარაუდობთ, რომ დაუმუშავებელ მიმდევრობას აქვს ნაცნობი მინიმალური ენტროპია ან ზოგიერთ შემთხვევაში, ისეთი ცნობილი თვისებები მაინც, როგორიცაა ბიტებს შორის დამოუკიდებლობა ან რომ ეს მიმდევრობა გამომდინარეობს მარკოვის პროცესიდან.

ჩვენ ასევე ჩავთვლით, რომ სტანდარტულად გვსურს (n, m, k, ϵ) - ექსტრაქტორი: ფუნქცია, რომელიც გარდაქმნის (n, k) - წყაროს n ბიტს m გამომავალ ბიტებად, რომლის განაწილება ϵ-ახლოსაა თანაბართან, ხოლო m რაც შეიძლება ახლოსაა k-სთან.

4. დეტერმინისტული ექსტრაქტორები

ჭეშმარიტი შემთხვევითობა შეიძლება წარმოიშვას ნებისმიერი კვანტური პროცესისგან, რომელიც მდგომარეობების თანმიმდევრულ სუპერპოზიციას არღვევს. დღესდღეობით, ხელმისაწვდომია მაღალი ხარისხის ოპტიკური კომპონენტებია, ამიტომ ყველაზე პრაქტიკული QRNG- ები ხორციელდება ფოტოსისტემებში.

დეტერმინისტული ექსტრაქტორები ფუნქციებია

$$Ext: \{0,1\}^n \rightarrow \{0,1\}^m$$

რომლებიც იღებს n ბიტების $\{0, 1\}^n$ შემავალ სტრინგებს და გვაძლევს m გამომავალ ბიტებს. ეს ფუნქციები განსაკუთრებით მიმზიდველია, რადგან დეტერმინისტული ალგორითმებია, რომლებსაც მუშაობისთვის მხოლოდ შემავალი თანმიმდევრობა სჭირდება. თუმცა, აქვთ გარკვეული შეზღუდვები, რომლებიც ხელს უშლის მათ გამოყენებას შემთხვევითობის გარკვეულ წყაროებში.

ელემენტარული არგუმენტი გვიჩვენებს, რომ შეუძლებელია ზოგადი დეტერმინისტული ექსტრაქტორები. წარმოვიდგინოთ ფუნქცია $\{0, 1\}^n$-დან $\{0, 1\}$. შეგვიძლია გამოვყოთ ყველა შესაძლო შემავალი მნიშვნელობების n ბიტიანი სტრიქონი ერთ ნაკრებში, რომელიც გვაძლევს 0 მნიშვნელობას, $Ext^{-1}(0)$, და გვექნება მეორე ნაკრები, რომელიც გვაძლევს 1-ს, $Ext^{-1}(1)$. მინიმუმ ერთ-ერთს მაინც აქვს 2^{n-1} ან მეტი ზომა. შემავალ მნიშვნელობას, რომელიც წარმოადგენს თანაბარ განაწილებას უფრო დიდ ნაკრებში, გააჩნია $n-1$ მინიმალური ენტროპია მაინც, მაგრამ ყოველთვის გვაძლევს ერთი და იგივე გამომავალ მნიშვნელობებს,

რაც გვიჩვენებს, რომ არ არსებობს ერთი ზომის ექსტრაქტორი, რომელიც ვალიდურია ნებისმიერი შემავალი განაწილებისთვის.

თუმცა, არსებობს მოქმედი ექსტრაქტორები, პროცესების გარკვეულ ოჯახების შემავალი განაწილებებისთვის, რომლებიც მიეკუთვნებიან პროცესების გარკვეულ ოჯახებს და აღწერენ გონივრულ წყაროებს. სხვათა შორის, არსებობს პრაქტიკული დეტერმინული ექსტრაქტორები შერჩევითი განაწილებისთვის, ბიტების ფიქსირებული წყაროებისთვის, სადაც მოწინააღმდეგეს შეუძლია დააყენოს ბიტების ნაწილი და განზოგადოება აფინური წყაროებისთვის ან წყაროები, ისეთი გამომავალი მნიშვნელობებით, რომლებიც თანაბრადაა განაწილებული უცნობ ალგებრულ ნაირსახეობაზე.

ცვლადი სიგრძის დეტერმინისტული ექსტრაქტორები ქმნიან საინტერესო დეტერმინისტული ექსტრაქტორების კიდევ ერთ ჯგუფს, რომლებიც ოდნავ გადაიხრება დეტერმინისტული ექსტრაქტორის მოცემული განმარტებიდან. ეს ნაჩვენებია ფონ ნოიმანის ალგორითმში: დეტერმინისტული მეთოდი, რომელიც მუშაობს უცნობი განაწილებისთვის და გვაძლევს სიგრძის გამომავალ მნიშვნელობას, რომელიც არ არის ცნობილი ექსტრაქციამდე.

ფონ ნოიმანმა შემოგვთავაზა მეთოდი, რომლის დროსაც, წარმოქმნილი თითოეული ბიტის წყვილისთვის, შეგვიძლია გავაუქმოთ 00 და 11 შედეგები, მივანიჭოთ 01-ს 0 და 10-ს კი 1.

აღწერილი ფონ ნოიმანის შემთხვევითობის ექსტრაქტორის ერთადერთი აუცილებელი პირობაა, რომ თითოეული შემავალი ბიტი იყოს დამოუკიდებელი წინა და მის შემდგომი ბიტებისგან. ფონ ნოიმანის მეთოდის დახვეწილი ვერსიები ამცირებენ გადაყრილ ენტროპიას და გვაძლებს ეფექტურობას ინფორმაციის თეორიის ზღვართან ახლოს, რომელიც მოცემულულია წყაროს შანონის ენტროპიით. შემდგომი ცვლილებების შედეგად მივიღეთ ალგორითმები, რომლებიც აწარმოებენ მიუკერძოებელ მიმდევრობებს უფრო ზოგადი პირობებით, შეყვანის თანმიმდევრობა მოდის მარკოვის ჯაჭვიდან.

ორიგინალი მეთოდის მთავარი მომხიბვლელობა მისი სიმარტივეა. ის მოითხოვს მინიმალურ გამოთვლით ენერგიას. ის შეძლება განხორციელდეს მხოლოდ ძირითადი აპარატურით და წყაროზე განაწილების სრულყოფილად ცნობა არ არის აუცილებელი. თუმცა, ორიგინალ მეთოდს გააჩნია რამდენიმე მნიშვნელოვანი შეზღუდვა. თუ ჩვენ გვყავს გარე შემტევი, რომელსაც შეუძლია მიკერძოების შეცვლა ბიტიდან ბიტზე, თუნდაც მცირედით, ფონ ნოიმანის ექსტრაქტორი აღარ იმუშავებს. სინამდვილეში, არ არსებობს დეტერმინისტული ალგორითმი, რომელიც $X = (X_1, X_2, \dots, X_n)$ ცვლადისთვის n ბიტით მოგვცემს თანაბარ გამომავალ მნიშვნელობას, თუ შეყვანილი ბიტების მიკერძოება იცვლება ისე, რომ 1-ის პოვნის ალბათობა მე-n ბიტისთვის დამოკიდებულია წინა ბიტის s მნიშვნელობის გაზომილ სტრინგზე

$$\delta \leq P_{X_i}(1|x_1 x_2 \dots x_{n-1} = s) \leq 1 - \delta$$

$0 < \delta \leq \frac{1}{2}$ -სთვის. ამას Santha-Vazirani-ის წყაროს უწოდებენ. აღწერილია სუსტი შემთხვევითობის წყაროების მოდელი დეტერმინისტული ექსტრაქტორის შეუძლებლობის მტკიცებულებასთან.

ამ შეზღუდვის მიუხედავად, არსებობს დეტერმინისტული ალგორითმები, რომლებიც საშუალებას გვაძლევს გამოვიყენოთ სუსტი Santha-Vazirani-ის წყარო, შემთხვევითი ალგორითმების სიმულაციისთვის. რანდომიზაციის მოთხოვნები ნაკლებად მკაცრია, ვიდრე სხვა გამოყენებისთვის, როგორიცაა კრიპტოგრაფია. ზოგჯერ სუსტი წყაროები, რომლებიც ვერ ახერხებენ თითქმის ერთნაირი შედეგების გამომუშავებას, ზოგიერთ შემთხვევაში მართებულია.

მაშინაც კი, თუ ჩვენ ვიყენებთ დეტერმინისტულ ექსტრაქტორს, ერთი სუსტი წყარო არ არის საკმარისი მრავალი კრიპტოგრაფიული პროტოკოლისთვის. მიუხედავად იმისა, რომ სუსტი შემთხვევითობა შეიძლება უსაფრთხოდ გამოვიყენოთ ხელმოწერის სქემებში, დაშიფვრასა და მასთან დაკავშირებულ სხვა პროტოკოლებში მაღალი ხარისხის გასაღებია საჭირო, სხვა შემთხვევაში ისინი გახდებიან დაუცველები.

მოწყობილობებისთვის, სადაც აუცილებელია გამომავალი მნიშვნელობები თანაბართან იყოს ახლოს, არსებობს მარტივი გადაწყვეტა. გავაერთიანოთ ორი, დამოუკიდებელი, სუსტი Santha-Vazirani წყაროს შედეგები, რათა გამოვიტანოთ გამომავალი მიმდევრობა, რომელსაც ვერ გამოვარჩევთ პოლინომიური დროის ალგორითმით თანაბარი განაწილებიდან. სანამ გვაქვს წვდომა ფიზიკურ მეთოდზე, რომელიც გარკვეულ შემთხვევითობას წარმოქმნის, შეგვიძლია დავაგენერიროთ ბიტის სტრინგები, რომლებსაც ვერ გამოვარჩევთ შემთხვევითი სტრინგებისგან ნებისმიერი ეფექტური ალგორითმით. ეს ისეთივე კარგია, როგორც ჭეშმარიტი შემთხვევითობა შემთხვევითობის ბევრ იმპლემენტაციაში, მათ შორის კრიპტოგრაფიაში.

აქამდე საუბარი იყო ერთი წყაროს ექსტრაქტორებზე. მრავალი წყაროს ექსტრაქტორები მისდევენ ამ მოდელს და იღებენ შედეგს ორი ან მეტი სუსტი წყაროდან. ამუშავებენ მათ და წარმოიქმნება მიმდევრობა, რომელიც თანაბართან არის მიახლოებული. არსებობს ბევრი მეთოდი, რომელიც დამოკიდებულია კონკრეტული შემავალი მნიშვნელობების განაწილებაზე, წყაროების რაოდენობაზე და გამომავალი მიმდევრობის სასურველ თვისებებზე.

წყაროების შერწყმა ასევე გამოიყენება შემთხვევითობის ექსტრაქტორების მეორე მთავარ ჯგუფში, თესლიან ექსტრაქტორებში (seeded extractors). ისინი შეგვიძლია წარმოვიდგინოთ მრავალი წყაროს ექსტრაქტორების სპეციალური შემთხვევა, ერთი სუსტი წყაროსა და იდეალურად თანაბარი წყაროთი, რომელიც წარმოქმნის მხოლოდ მცირე ოდენობის ბიტებს.

5. თესლიანი ექსტრაქტორები

როგორც ვნახეთ, ბევრი ნედლი ბიტის განაწილებისთვის, შეგვიძლია მივაღწიოთ მხოლოდ თანაბარ შედეგს, მხოლოდ რაიმე დამატებითი შემთხვევითობის დახმარებით. თესლიან ექსტრაქტორებში კი გვაქვს ფუნქცია

$$Ext: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

ამ ფუნქციაში შედის n ბიტები ნედლი მიმდევრობა, d თანაბარი შემთხვევითი თესლის ბიტები, ხოლო წარმოიქმნება m გამომავალი ბიტები. ვთვლით, რომ d გაცილებით მცირეა, ვიდრე m. თესლის დამატებით, გვაქვს იმის გარანტია, რომ არსებობს ექსტრაქტორები, რომლებიც წარმოქმნიან თითქმის თანაბარ გამომავალ მნიშვნელობებს, რომლის სიგრძე მიახლოებულია მაქსიმალურ სიგრძესთან. ეს თესლი მსგავს როლს თამაშობს, როგორც თესლი, ფსევდო შემთხვევითი რიცხვების გენერატორებში. (k, ϵ) ექსტრაქტორს ვუწოდებთ ფუნქციას, ნებისმიერი k შემავალი წყაროსთვის (ნედლი მიმდევრობა, მინიმალური ენტროპია k მაინც), რომელიც წარმოქმნის გამომავალ თანმიმდევრობას, რომელიც ϵ-თი ახლოსაა თანაბართან. თესლი მოქმედებს, როგორც კატალიზატორი, რომელიც საშუალებას გვაძლევს ვიპოვოთ ზოგადი მეთოდები, რომლებიც ყოველთვის იმუშავებს.

შემთხვევითობის თესლიანი ექსტრაქტორები პირველად განისაზღვრა შემთხვევითი ალგორითმების კონტექსტში. ალბათური მეთოდების გამოყენებით, ნაჩვენებია, რომ ყოველთვის არსებობს ექსტრაქტორები, რომლებიც მოიცავს თითქმის ყველა არსებულ ფარულ ენტროპიას, შეყვანილი k წყაროს ნედლ თანმიმდევრობიდან. k წყაროს n ბიტების ბლოკების შესაყვანად, შეგვიძლია ავაწყოთ ექსტრაქტორები $m \approx k + d$ ზომის, რომელიც ϵ-თი ახლოსაა თანაბართან, გამოიყენება d სიგრძის თესლი $\log_2 n$. ამ თესლიანი ექსტრაქტორებისთვის არსებობს სხვადასხვა კონსტრუქციები.

თანაბარი თესლის საჭიროება, როგორც ჩანს, წინააღმდეგობრივია: ჩვენ გვჭირდება რესურსი, რომლის წარმოებასაც ვცდილობთ. თუმცა, თესლზე რეკვიზიტები ნაკლებად შემზღუდველია, ვიდრე ჩანს. ბევრ აშკარა ექსტრაქტორში თესლის სიგრძის ზომა ლოგარითმულია შემავალი სტრინგის ზომის. საკმარისად მცირე d- სთვის, შეგვიძლია შეცვალოთ შემთხვევითობის აუცილებელი მოთხოვნა ყველა 2^d შესაძლო თანმიმდევრობით. რანდომიზებულ ალგორითმებში, ანგარიშს, რომელსაც მოსდევს უმრავლესობის ხმის მიცემის ნებართვები, კარგია თანაბარი წყაროს სიმულაციისთვის. თუმცა, ეს მიდგომა აშკარად არ არის ვალიდური კრიპტოგრაფიისთვის, სადაც ჩვენ გვჭირდება არაპროგნოზირებადობა. კვანტური შემთხვევითი რიცხვის გენერატორებში, თესლიანი ექსტრაქტორები გვიცავს გარე თავდამსხმელებისგან. არსებობს კონსტრუქციები, რომელთათვისაც არსებობს უსაფრთხოების მტკიცებულებები, სხვადასხვა ძალის კვანტური თავდამსხმელების წინააღმდეგ.

პირველი თვალსაჩინო შედეგია Trevisan- ის ექსტრაქტორი. მნიშვნელოვანი თეორიული ინტერესი გამოიწვია მან მისი მონაცემების სიმცირის გამო, არამედ განსაკუთრებით იმიტომ, რომ ის უსაფრთხოა კვანტური მოწინააღმდეგეებისგან [12]. ტრევიზანის ექსტრაქტორის

თესლის სიგრძე შემავალი მნიშვნელობის სიგრძის პოლიგარითმულია და ასევე შეიძლება დადასტურდეს, რომ ის არის ძლიერი ექსტრაქტორი [13]. ანუ, ტრევიზანის ექსტრაქტორის შემთხვევითი თესლი შეიძლება ხელახლა გამოვიყენოთ. ეს განსაკუთრებით მნიშვნელოვანია პოპულარული უნივერსალური ჰეშინგის ფუნქციებისთვის, მაგალითად Toeplitz hashing.

ტრევიზანის ექსტრაქტორი აგებულია Nisan-Widgerson-ის ფსევდო შემთხვევითი რიცხვების გენერატორზე. ეს შეიძლება ჩაითვალოს, როგორც შემთხვევითი ფუნქცია, რომლის ჭეშმარიტობის ცხრილი მოცემულია ბიტების სუსტი წყაროდან. შემთხვევითი ფუნქცია აფართოებს თანაბარი შემთხვევითი თესლია d ბიტებს, როგორც PRNG, ისე ექსტრაქტორის მნიშვნელობით. ტრევიზანის ექსტრაქტორის სხვადასხვა ვარიაციები განხორციელდა კვანტური შემთხვევითი რიცხვების გენერატორებით და კვანტურ გასაღების განაწილებაში. მათი მთავარი უპირატესობა არის ის, რომ შემთხვევითი, თანაბარი თესლის ზომა მხოლოდ პოლი-ლოგარითმულია შეყვანის ბლოკების ზომის. თუმცა, პრაქტიკულმა იმპლემენტაციამ შეიძლება შეანელოს ბიტების გენერაციის პროცესი, რადგან ექსტრაქციის დროს საჭიროა გამოთვლები.

მეორე ზოგადი მეთოდია ორი უნივერსალური ჰეშირება (two-universal hashing). The Leftover Hash Lemma გვიჩვენებს, რომ ორი უნივერსალური ჰეშირების ფუნქცია, საკმაოდ მაღალი ენტროპიის შეყვანილი მნიშვნელობებით, თითქმის თანაბრად შემთხვევითია [14]. ორი უნივერსალური ჰეშირების ფუნქციებს, შეუძლია შემთხვევითობის ამოღება სუსტ წყაროში, საიმედოდ, ჯაშუშის თანდასწრებით. თუ ჩვენ გვაქვს კარგი შეფასება ან ჩვენი სუსტი შემთხვევითი წყაროს კორელაციაზე კონსერვატიული შეზღუდვა მომსმენთან, პირობითი ენტროპიების გამოყენებით შესაძლებელია გამოვიყენოთ ლემას განზოგადება, გვერდითი ინფორმაციის გამოყენებით [15]. ფართო გაგებით, გვერდითი ინფორმაციაც შეიძლება იყოს კვანტური. კვანტური შემთხვევითი რიცხვების გენერატორში სადაც არის ტექნიკური ხმაური შეგვიძლია ვივარაუდოთ, რომ ყველა შემთხვევითობა, რომელიც არასრულყოფილებისგან მოდის, ან სხვაგვარად არ ეგუება კვანტური სისტემის ჩვენს მოდელს, რომელიც აწარმოებს ნედლეულ ბიტს, არის ჯაშუშის გამო. ამ პირობებში ჯერ კიდევ შესაძლებელია თესლიანი ექსტრაქტორის შემუშავება, რომელიც იძლევა თითქმის თანაბარ შედეგს, რომელიც დამოუკიდებელია გარე სისტემებისგან. ეს მეთოდები ასევე გამოიყენება კვანტური გასაღების განაწილებაში, კონფიდენციალურობის გაძლიერების დროს.

შემთხვევითობის ექსტრაქტორი ორი უნივერსალური ან უფრო ზოგადად I-უნივერსალური ჰეშირებით გვაიძულებს გამოვიყენოთ შედარებით გრძელი თესლი, რომელიც ეკვივალენტურია n ბლოკის ზომის, მაგრამ მისი გადამუშავება შესაძლებელია. ასევე შემთხვევითად შერჩეული თანაბარი თესლის ხელმეორედ გამოყენება შესაძლებელია.

ტრევიზანის ექსტრაქტორის დანერგვისგან განსხვავებით, ეს მეთოდი გვთავაზობს სწრაფი ამოღების ფუნქციას, რომელიც იყენებს ნაკლებ გამოთვლით რესურსებს, უფრო დიდი თესლის ხარჯზე. ზოგიერთი იმპლემენტაცია, მაგალითად, Toeplitz–ის შემთხვევითი ორობითი მატრიცებით ჰეშირება, განსაკუთრებით ეფექტურია. შეგვიძლია განვსაზღვროთ ერთი ასეთი ექსტრაქტორი, სადაც თესლი გამოიყენება როგორც მართკუთხა მატრიცა,

რომელიც მრავლდება n- ვექტორებზე წყაროდან და წარმოქმნის თითქმის დამოუკიდებელ ბიტებს. ეს მიდგომა გამოიყენება ზოგიერთ კომერციულ მოწყობილობაში, რომლებიც შეიცავს ექსტრაქციის ფუნქციას, როგორც წინასწარ გამოთვლილ შემთხვევით მატრიცა, რომელიც ასრულებს თესლის როლს და გადანაწილებულია მოწყობილობაში კოდირებულად. მიუხედავად იმისა, რომ თესლის მაღალი ხარისხის შემთხვევითობა რთული პროცესია, ამის გაკეთება მხოლოდ ერთხელაა საჭირო. გრძელი არადახვეწილი მეთოდები, როგორებიცაა მრავალჯერადი დამოუკიდებელი გენერატორის XOR– ის განმეორებით აღება, მისაღებია.

ბიბლიოგრაფია

1. M. Iavich, T. Kuchukhidze, T. Okhrimenko and S. Dorozhynskyi, "Novel Quantum Random Number Generator for Cryptographical Applications," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 727-732, doi: 10.1109/PICST51311.2020.9467951.
2. M. Iavich, T. Kuchukhidze, T. Okhrimenko and S. Dorozhynskyi, "Novel Quantum Random Number Generator for Cryptographical Applications," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 727-732, doi: 10.1109/PICST51311.2020.9467951.
3. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems," *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.
4. Kabiri Chimeh, M., Heywood, P., Pennisi, M. et al. Parallelisation strategies for agent based simulation of immune systems. BMC Bioinformatics 20, 579 (2019). https://doi.org/10.1186/s12859-019-3181-y
5. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
6. P. A. W. Lewis, A. S. Goodman and J. M. Miller, "A pseudo-random number generator for the System/360," in IBM Systems Journal, vol. 8, no. 2, pp. 136-146, 1969, doi: 10.1147/sj.82.0136.
7. Lambić, D., Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn 90, 223–232 (2017). https://doi.org/10.1007/s11071-017-3656-1
8. J. M. Mcginthy and A. J. Michaels, "Further Analysis of PRNG-Based Key Derivation Functions," in IEEE Access, vol. 7, pp. 95978-95986, 2019, doi: 10.1109/ACCESS.2019.2928768.
9. Ma, Xiongfeng, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi-Kwong Lo. "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction." Physical Review A 87, no. 6 (2013): 062327.
10. Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/RevModPhys.89.015004.
11. Rožić, Vladimir, Bohan Yang, Wim Dehaene, and Ingrid Verbauwhede. "Iterating von Neumann's post-processing under hardware constraints." In 2016 IEEE international symposium on hardware oriented security and trust (HOST), pp. 37-42. IEEE, 2016.
12. De, Anindya, Christopher Portmann, Thomas Vidick, and Renato Renner. "Trevisan's extractor in the presence of quantum side information." SIAM Journal on Computing 41, no. 4 (2012): 915-940.

13. Raz, Ran, Omer Reingold, and Salil Vadhan. "Extracting all the randomness and reducing the error in Trevisan's extractors." Journal of Computer and System Sciences 65, no. 1 (2002): 97-128.
14. Stinson, Douglas Robert. Universal hash families and the leftover hash lemma, and applications to cryptography and computing. Faculty of Mathematics, University of Waterloo, 2001.
15. Tsurumaru, Toyohiro, and Masahito Hayashi. "Dual universality of hash functions and its applications to quantum cryptography." IEEE transactions on information theory 59, no. 7 (2013): 4700-4717.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 35-52 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

DESIGN & DEVELOPMENT OF A CYBER SECURITY CONCEPTUAL FRAMEWORK FOR HIGHER EDUCATION INSTITUTIONS IN THE REPUBLIC OF MOLDOVA

Alexei Arina, Department of Telecommunications and Electronic Systems, Technical University of Moldova

ABSTRACT: This scientific paper reflects the results of research, which aimed to develop a Cyber Security Conceptual Framework for Higher Education Institutions in the Republic of Moldova, to increase cyber security in academic environment. The scientific method Design Science Research was selected for the development of the security framework, due to the practical value it generates, being one of the most used qualitative scientific methods in the field of engineering. The identification of the key processes and stages of implementation of the Cyber Security Conceptual Framework, assessed according to value criteria, supports the way in which cyber security in universities in the Republic of Moldova can be increased. Important contributions are for the academic environment in the Republic of Moldova, where until now, there has been no reference framework to ensure the protection of academic processes.

KEYWORDS*: cyber security, framework, Higher Education Institution, DSR, academic processes.*

1. INTRODUCTION

With the development of information technology, cyber security has become one of the biggest global challenges for organizations implementing new technologies worldwide (Asosheh et al., 2013). Cyber security is defined as a collection of tools, techniques, policies, security measures, security guidelines, risk mitigation strategies, actions, training, good practices, security reinsurance and the latest technologies that can be used to protect cyberspace and user assets (Humayun et al., 2020; von Solms & von Solms, 2018). Common cyber security regulations and requirements would allow a more comprehensive approach to cyber security in organizations with a similar profile. Creating a common cyber security framework, covering core processes, to ensure compliance with the three principles of cyber security: confidentiality, integrity and availability; it would facilitate the implementation of comprehensive security mechanisms and, as a result, increase cyber security. An important role, in this regard, is played by the Government, which has a proactive role in the management of cyber security policies and infrastructure in order to issue standardized recommendations, at state level, especially in the case of public institutions. The harmonization of cyber security strategies developed by the state with international standards ensures compliance and international recognition (Asosheh et al., 2013).

The Republic of Moldova is a developing country, that in recent decades has been trying to align with international practices in the public domain. Information technology plays a very important role in providing public services. According to the annual report on monitoring the evolution of the global information society "Measuring the information society 2017", launched by the International Telecommunication Union, the Republic of Moldova ranks 59th out of 176 countries in the ranking. At the European level, the Republic of Moldova has advanced compared to the global and regional average, being among the top 10 countries with the most dynamic developments in the world (Alexei, 2021).

At the same time, the Information Security Strategy for 2019-2024 (RM Parliament, 2018), adopted by the Parliament of the Republic of Moldova, also identified as a major problem in the field of cyber security, the lack of an integrated cyber security management system that would provide a comprehensive approach to cyber security (points 39 and 40 of the Strategy), solving this problem is identified as a key step in the development of a secure information society in the Republic of Moldova.

There are currently 15 public and 9 private Higher Education Institutions in the Republic of Moldova. Higher Education Institutions are subordinated to the Ministry of Education and Research, so the provisions of the Information Security Strategy must be implemented. However, the results of the survey, conducted by the author between September-November 2020, in which stakeholders from the 9 largest public institutions in the Republic of Moldova participated, show that Higher Education Institutions are not certified with an information security standard and have not implemented an authorized cyber security framework (Alexei Arina, 2021).

Moreover, the diversity of electronic services provided by academia is constantly growing, especially as a result of the pandemic with Covid 19 and the transition to online education. To ensure access to learning platforms, digital libraries, or university management systems, university information systems are open by design (Jang-Jaccard & Nepal, 2014), decentralized and multi-user. Software and network applications have become an integral part of the university environment both in Moldova and internationally. Access to modern technologies is valuable, on the one hand, for the development of

modern learning environments, but on the other hand, it increases the vulnerability of communication networks and the number of threats.

Thus, in the context of the above, the research problem is:" the lack of a cyber security framework focused on academic processes in Higher Education Institutions in the Republic of Moldova, which could be used as a reference framework".

Implementing a security concept that does not take into account the security requirements specific to the academic environment and the activities they carry out, increases the likelihood of a false sense of security.

So, the purpose of this scientific paper is to develop a cyber security conceptual framework (CSCF), focused on the academic processes of Higher Education Institutions in the Republic of Moldova, which complies with the provisions of international standards and best practices in the field, in order to solve the research problem.

The following section presents the results of the literature review, the purpose of which was to identify cyber security strategies for academia, recommended by researchers, internationally. The third section presents the scientific method used to solve the research problem, and the fourth section presents the research results.

2. LITERATURE REVIEW

To achieve the purpose of this research work, the author has carried out a literature review of the last 10 years, using the method proposed by Kitchenham (Barbara Kitchenham 2004), to determine the strategies approached by researchers at the international level and how a cyber security framework can be integrated into academic processes. A comprehensive research paper has already been published (Alexei, 2021).

The implementation of a cyber security framework in HEIs has been recommended by several researchers over time. Cybersecurity frameworks assist in the implementation of Information Security Management Systems, providing a comprehensive approach and comprehensive solution, which includes: policies, tools and procedures needed to increase security (Itradat et al. 2014) and strengthen information systems (Oltramari et al. 2014; Donaldson et al. 2015; Koong and Yunis 2015; Merchan-Lima et al. 2020).

The effectiveness of the proposed solution depends on risk management, which is a mandatory process when conceptualizing the cyber security framework, because identifying assets that assist academic processes, and determining threats and vulnerabilities that influence confidentiality, integrity and availability, have a major impact on the outcome, which will have the security framework (Hommel, Metzger, and Steinke 2015). Risk management can reduce the risks of certain important processes, financial losses or damage to the reputation of higher education institutions (Suroso and Fakhrozi 2018) and can support the creation of security policies (Hommel, Metzger, and Steinke 2015).

These arguments served as a reason for analyzing the recommended strategies for creating the cybersecurity framework, risk management and how to integrate into HEIs, to increase cyber security.

2.1 INTERNATIONAL CYBER SECURITY STANDARDS

Analyzing the literature in the field, we identified 3 international standards recommended in various scientific studies, indexed by the largest databases, such as: Scopus, ScienceDirect, ACM Digital Library, IEEE Xplore, Springer; to be implemented in HEIs. These are: ISO 27001, COBIT AND ITIL.

ISO 27001

The most widely used international standard in the field is ISO 27001 (Rehman, Masood, and Cheema 2013; Itradat et al. 2014), and if we analyze the results of the annual surveys presented by ISO (International Organization for Standardization 2020), the number of organizations certified with ISO 27001 is constantly increasing from 31 910, in 2018, to 44 486 in 2020. The Republic of Moldova is no exception, so the number of organizations certified in 2020 has increased compared to 2018, from 3 to 8.

In the field of Education can be seen a positive trend, at international level, so that if in 2018, the number of institutions certified with ISO 27001 was 137, in 2020 they are 187. Unfortunately, in the field of education, in 2020, there is no institution certified with ISO 27001 in the Republic of Moldova. Although the empirical research conducted by the Rotterdam School of Management, Erasmus University, based on 645 responses from companies, internationally, ISO 27001 certification, had a significant positive effect on increasing information security, estimated by 85% of respondents (Nowak 2015).

ISO 27001 is based on the implementation of an information security management system within organizations and addresses systematic processes, technologies and human resources, for risk assessment and assistance in the information

management process. It is based on the Deming cycle (Haufe et al. 2016), which is a closed action process that assists in information security management processes.

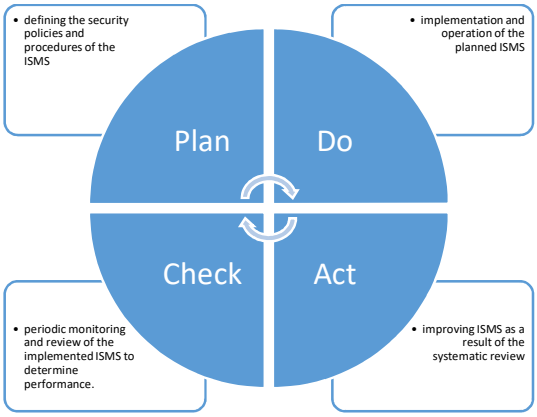

Fig. 1 Deming cycle

With regard to ISMS in HEIs, the Deming cycle represents consecutive actions aimed at achieving the main objective, the implementation of information security within an institution (Szczepaniuk et al. 2020).

The ISO 27001 standard is organized into 14 sections, 35 objectives and 114 security controls, but not all sections of the standard are applicable in HEIs (Rehman, Masood, and Cheema 2013). Researchers recommend the use of at least 8 sections from ISO 27001 in HEIs: asset management, human resource management, physical controls, access control, communications control, operational control, incident management, information system control, and business continuity (Cheung 2014; Esparza et al. 2020).

COBIT

Another standard recommended by researchers to be implemented in HEIs is COBIT. COBIT is a strategy that applies IT Governance and is classified into 4 areas: Planning and Organization, Procurement and Implementation, Delivery and Support, Monitoring and Evaluation (Wolden, Valverde, and Talla 2015).

COBIT's control objectives refer to policies, procedures, practices and organizational structures that ensure the organization's objectives, as well as to prevent or detect any unexpected events (Khther and Othman 2013). COBIT includes 34 IT processes and 13 control objectives. Each process contains a RACI diagram (Khther and Othman 2013), which shows the role of each process in a managerial activity. The activities are identified from the control objectives and have a detailed structure.

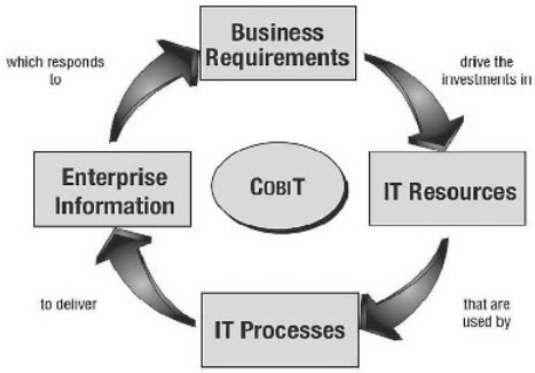

Fig 2. COBIT framework principle (Khther and Othman 2013)

As COBIT controls are mainly focused on achieving organizational objectives, it is further necessary for the security model to comply with the controls of the ISO 27001 standard, in order to ensure an optimal level of cybersecurity. Within the HEIs, it is recommended to use COBIT to verify the maturity level of the model used (Yustanti et al. 2018) and to evaluate IT processes (Khther and Othman 2013).

ITIL

The ITIL framework is presented as an association between different practices and information technology services for better management of IT services (Suwito et al. 2016). Services are characterized as a means of providing value to customers without increasing security risks or cost. ITIL is a bookstore containing a set of 5 books and 34 processes that describe different phases of implementation and provide a systematic approach to IT Governance, operations management and control of IT services (Gërvalla, Preniqi, and Kopacek 2018).

As in the case of COBIT, it is recommended to use the ITIL framework combined with the ISO 27001 standard, in order to integrate the security practices recommended by ISO 27001 in providing the best practical process management services recommended by ITIL. This will reduce the cost of maintaining an acceptable level of security, provide effective risk management and reduce security risks at all levels (Suwito et al. 2016).

Although it would appear that these 3 frameworks contain identical instructions, the implementation requirements are still different, which drastically affects the effect of implementation, especially the required budget. Therefore, before using any of the listed frameworks, it is necessary to clarify the implementation costs, which are usually limited within the HEIs.

ISO 27001 is the most widely used security standard internationally, so it can be concluded that it is the easiest to implement, recognized and implementation costs are lower than ITIL and COBIT, ISO 27001 is like English, has a proven international value.

2.2 RECOMMENDED TECHNIQUES FOR RISK MANAGEMENT IN HEIS

Risk management includes coordinated activities to lead and control an organization in terms of cyber risk (ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary 2018). Cyber risk can be defined as a security event that exploited a vulnerability in the information system and caused the threat (Wangen, Hallstensen, and Snekkenes 2018; Ulven and Wangen 2021). An information security event is an identified occurrence of a system, service, or network condition that indicates a possible breach of information security policy, or failure of controls, or a previously unknown situation that may be relevant to security (ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary 2018) and has a impact and a likelihood (Wangen, Hallstensen, and Snekkenes 2018). At the basis of information risk analysis is the process of identifying threats (Szczepaniuk et al. 2020), threats are defined as "any phenomenon (process, event), undesirable in terms of undisturbed operation of a system" (Szczepaniuk et al. 2020).

A holistic approach to cybersecurity management in HEIs is essential because it provides an overview of all resources that need to be protected. Risk assessment methods should take into account the dependencies between resources that assist university electronic services (Hariyanti, Djunaidy, and Siahaan 2018), so the methods must be able to adapt and be dynamic and appropriate for the university environment. As electronic services are constantly changing, risk factors are changing (Harkins 2016) and affecting the value of university activities (Rojas and Lesmes 2016).

Following the study, it was identified that the main recommended models for risk management in HEIs are: ISO 27005, OCTAVE and OCTAVE Allegro (Alexei, 2021).

ISO 27005

The standard ISO 27005 is part of the ISO 27000 family of security standards. It is the standard underlying risk management, which must be achieved before the creation and implementation of an ISMS, according to ISO 27001.

ISO 27005 addresses security risks from the perspective of information assets, defined as any asset that has value to the organization and requires protection (ISO/IEC 27000:2018, 2018).

According to ISO 27005 (ISO/IEC 27005: Information technology — Security techniques — Information security risk management 2018), all information assets should be classified as primary assets and support assets. The primary assets are all academic processes and information, and the assets: hardware, software, network and communications, personnel and infrastructure, are support assets (Asosheh, Hajinazari, and Khodkari 2013).

OCTAVE

The OCTAVE model is implemented in university activities to reduce the risk of cyber threats, by identifying the causes that make the university system vulnerable (Joshi and Singh 2017). OCTAVE contains specific activities, performed in 3 phases (Joshi and Singh 2017; Das, Mukhopadhyay, and Bhasker 2013). The first phase is to identify the weaknesses of the system, dynamically (for each new technology the risk is assessed). In the second phase, the risk score is calculated,

an important resource in this regard is the Common Vulnerability Scoring System (CVSS) (Singh Umesh Kumar and Joshi C. 2016), to validate the vulnerability that can be exploited. The final step is to create a security risk remediation plan and recursive risk assessment activities (Joshi and Singh 2017).

OCTAVE Allegro

OCTAVE Allegro has been recommended by researchers because it allows for a more comprehensive assessment of the operational risk environment in order to produce better results without the need for extensive knowledge of security risk assessment (Suroso and Fakhrozi 2018). It focuses mainly on information assets in the context of how they are used, where they are stored, processed and transferred, as well as extended to threats, vulnerabilities and any disruption (Hommel, Metzger, and Steinke 2015).

2.3 SECURITY FRAMEWORK IMPLEMENTATION PHASES

Having a security framework focused on university processes, it is necessary to know the stages of its implementation. The security framework can be very well structured, but if implemented incorrectly, it could cause serious harm to organizations instead of benefits.

Following the study, the recommended common steps for the implementation of the security framework within the HEIs can be defined. According to the classification of implementation stages in public organizations, made by Szczepaniuk E and others (Szczepaniuk et al. 2020), there are 6 stages of implementation of security frameworks in public organizations: defining security policies, defining purpose, security risk assessment, risk management, selection of controls and the statement of applicability.

3. RESEARCH METHOD

An essential part of any research paper is the scientific method selected for the study and the tools that facilitate the achievement of relevant scientific results. Without a strong component to produce explicitly applicable research solutions, cyber security research faces the potential to lose influence on the research flows for which such applicability is important (Peffers et al. 2007).

The challenge was to select a method that would allow the creation of a product, a security framework that would contribute to increasing cyber security in HEIs in the Republic of Moldova, to solve the research problem defined above. This premise was the basis for identifying the scientific method of Design Science Research (DSR), which is widely used internationally, and the research results can be models, concepts or frameworks (vom Brocke, Hevner, and Maedche 2020; Hevner et al. 2004; Baskerville et al. 2018). DSR is defined as "a problem-solving paradigm that seeks to improve knowledge by creating innovative artifacts" (vom Brocke, Hevner, and Maedche 2020). The DSR method has been appreciated as one of the main research methods for the engineering field (Dresch, Lacerda, and Antunes Jr 2015).

The literature identifies 6 typical stages of the DSR project: problem identification and motivation, definition of objectives for solution, design and development / design of the artifact, demonstration, evaluation, followed by communication of results (Peffers et al. 2007; Chandra Kruse, Seidel, and vom Brocke 2019; vom Brocke, Hevner, and Maedche 2020). Figure 3 shows the actions performed according to the DSR steps for CSCF development.

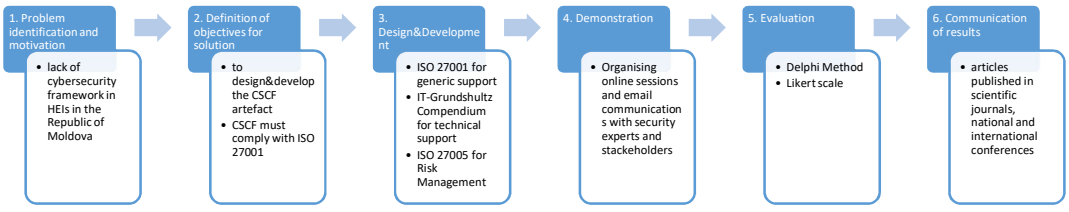

Fig 3. CSCF development on DSR stages

A. Problem identification and motivation

Higher Education Institutions in the Republic of Moldova are not certified with any security standards and have not implemented a comprehensive cybersecurity framework, such as an Information Security Management System, which

is recommended by ISO 27001, or another cyber security framework. Although it provides a variety of digital educational services.

B. Definition of objectives for solution

The result of this type of research, as mentioned above, is an artifact that solves a problem in the field, in this case, it will achieve the purpose of this research paper, also known as the concept of solution, which must be evaluated by criteria of value or utility (Dresch, Lacerda, and Antunes Jr 2015). The value criteria according to which the CSCF artifact can be evaluated are reflected in Table 1.

Table 1. Value criteria of CSCF artifact

Nr	Criterion	Arguments
1	Target group oriented	Contain controls corresponding business processes in academia
2	Implementation phases	The artifact must determine the main steps after which the cybersecurity framework will be implemented within the HEI
3	Predefined roles	The roles of staff involved in the implementation of cybersecurity in HEIs must be clearly defined, in order to know the responsibilities of the post and to designate the owners of critical assets.
4	Risk management	In order to increase the effectiveness of the security framework, it is necessary to identify the real risks, related to the critical assets and the threats that may affect them. To assess the impact of risks.
5	Efficient	The efficiency of the artifact depends directly on how well it is understood by HEI specialists, who are going to implement it. How clearly the objectives, purpose and implementation phases were defined.
6	Scalable	It can be implemented in any institution, regardless of its size and the complexity of the services it provides
7	International importance	To comply with the Bologna Process, which is being implemented in Moldovan universities. Subsequent certification of institutions with an international standard is an appreciable objective.

C. Design and development

The development of the CSCF artifact was based on the knowledge gained from the review of the literature, the result of which showed that researchers recommend for implementation in HEIs the standard ISO 27001, because it has a proven value over time and satisfies the value criteria of point B. The challenge was to determine how ISO 27001 controls could be implemented, being generic. Thus, it was established that the development of the CSCF artifact should be achieved through the synergy of ISO 27001, ISO 27002 which is a guide used to implement information security standards and IT - Grundschutz Kompendium, which is a German technical guide containing the tools necessary for the implementation of security controls. ISO 27005 has been used to achieve risk management, through interdependencies between the university's business processes and supporting assets.

D. Demonstration

Stakeholders from universities and experts in the field of cybersecurity in the Republic of Moldova were contacted via email. Online sessions were held to demonstrate how CSCF artifact can be implemented in HEIs.

E. Evaluation

The qualitative method of evaluating the artifact was used, through several Delphi rounds, which allowed obtaining the evaluation through empirical evidence (feedback from experts and specialists in the field) and evidence proven by applying the international standard ISO 27001. The qualitative approach facilitates a better understanding of the perceptions, beliefs and attitudes of the participants in the philosophical interpretive study of information systems (Myers and Newman 2007). The qualitative method allows to understand the context of a solution, including based on the comments made by HEIs specialists.

Thus, for the initial evaluation, the CSCF artifact was presented to the experts for evaluation, a great value representing the recommendations given by the experts. Subsequently, for empirical evaluation, the CSCF artifact was presented to HEIs stakeholders. The post-implementation feedback will be presented after the CSCF artifact will be implemented for a certain period of time in the HEIs of the Republic of Moldova.

F. Communication of results

The communication of the results took place through the publication of scientific articles and participation with communiqués at national and international conferences. Thus, the criteria according to which the CSCF artifact was developed, the novelty of the product and how it will have an impact on the increase of cybersecurity in the HEIs will be exposed. The CSCF artifact was presented to both the technology-oriented and the management-oriented public.

4. RESULTS

The approach to cybersecurity as a system requires a holistic approach, an overview, not a segmented one (Szczepaniuk et al. 2020), because security is interdisciplinary and does not necessarily refer only to information systems, but involves applicable law, organizational structure and other aspects that may influence this process.

The CSCF artifact is a cybersecurity management system focused on academic activities. The main purpose of the CSCF implementation is to increase cybersecurity in HEIs in the Republic of Moldova.

4.1 CSCF ARTIFACT DESIGN

The conceptual framework takes into account the mission of the organization, the academic institution in this case, and ensures the provision of electronic services respecting the three principles of security: Confidentiality, Integrity and Availability.

The IPO (Input, Process, Output) model (MacCuspie et al. 2014) was used to model the preliminary conceptual framework, the result obtained is reflected in figure 4.

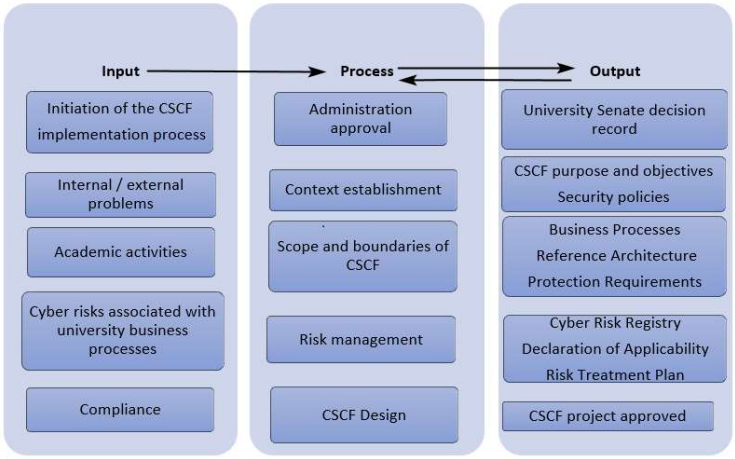

Fig 4. Preliminary conceptual framework

The inputs will influence the processes. The outputs are the goal to be achieved, each stage indicates the life cycle of the proposed conceptual framework.

To operationalize the conceptual framework described above, the Deming cycle will be used to continuously increase the quality of the security framework (Disterer, 2013), due to the dynamic nature of cybersecurity and the mandatory iterative nature of a cybersecurity management system. The application of the Deming cycle emphasizes the need for process guidance, as well as the integration of operations planning and constant verification of implementation in line with planning (Haufe et al. 2016).

As mentioned above, the conceptual framework for cybersecurity will be proposed through the synergy of the following international standards:

- ISO 27001 - which will support the creation of the CSCF;
- ISO 27002 - for the implementation of the CSCF, represents the code of practice for security controls and a good support for ISO 27001;
- ISO 27005 - for the management of security risks in HEIs;

- IT-Grundschutz-Kompendium for technical support.

Conceptual framework processes modeled using the IPO method, the four dimensions of the Deming cycle, and the recommendations of international organizations were applied to determine the design of the CSCF. Framework implementation stages in Moldovan HEIs is reflected in Figure 5.

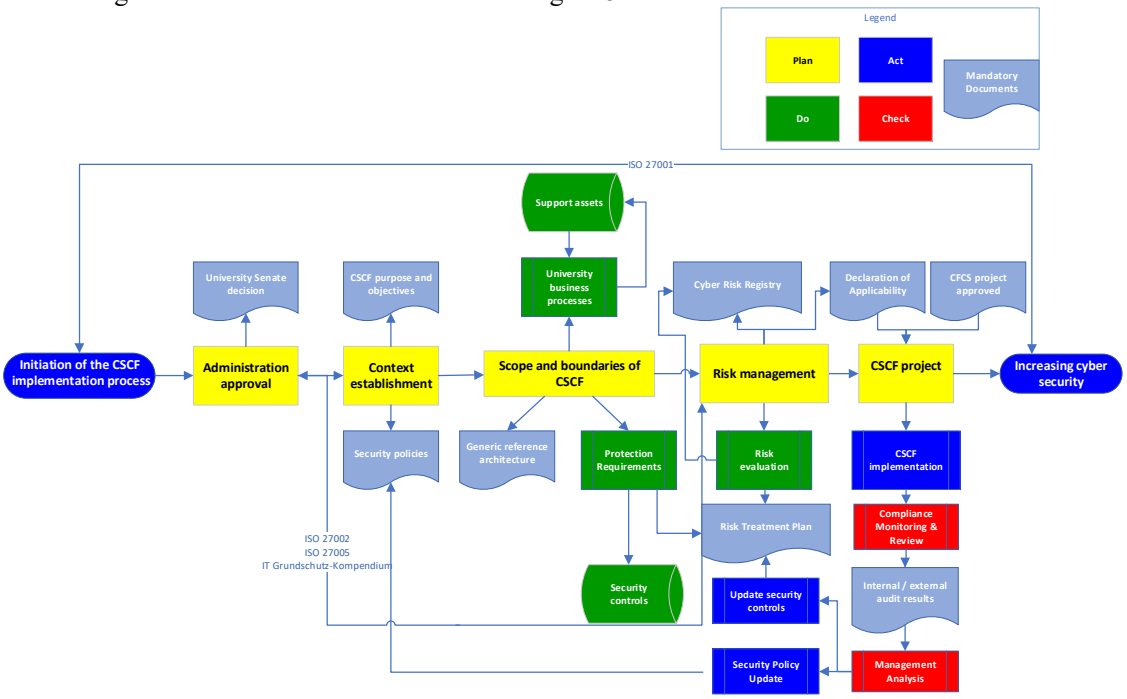

Fig 5. CSCF implementation stages

4.2 CSCF ARTIFACT DEVELOPMENT

CSCF is designed to be a valuable resource and support for Moldovan universities that will implement their own security concept, aligned with the specifics and activities of HEIs, supported by research results, empirical study and international standards. This section will analyze and set out as explicitly as possible these important issues that will result in an increase and a comprehensive approach to cybersecurity, so that the results of this research can be reproduced and put into practice by stakeholders.

4.2.1 Administration approval

The approval of the administration in the university environment of the Republic of Moldova refers to the Senate of the Institution, the supreme governing authority, which consists of the President of the Senate, Secretary and Senators. At this stage, the preliminary goal and organizational priorities are set (Asosheh, Hajinazari, and Khodkari 2013). The main goal for implementing a concept of security in universities is the comprehensive approach to cybersecurity, based on existing reasoning, that it is more cost effective to protect properly than to recover in the event of a disaster, whether it is intentional or not. An additional argument is the provisions of the National Strategy for Information Security of the Republic of Moldova, for the period 2019-2024, which identifies as the main problem for ensuring information security, the lack of information security management systems at the national level (RM Parliament, 2018).

According to ISO 27001, the organization, which aims to implement a cybersecurity framework, must constantly allocate resources "for the establishment, implementation, maintenance and continuous improvement" (ISO/IEC 27001, 2013). The allocation of the necessary resources refers to: human resources, financial resources, information resources, necessary infrastructure.

4.2.2 Context establishment

In order to develop CSCF, the academic institution must define the purpose of implementing the security framework, identify business processes and support assets.

According to ISO 27001, the HEI must identify external and internal issues (Disterer 2013), which are relevant to its purpose (ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT 2013). In order to analyze the internal problems faced by the HEI, it is necessary to take into account: the strategy and objectives of the organization, business processes and support assets, national / international contracts and derivative relations, intellectual property and research results, physical infrastructure and environment, information systems and media used.

This can define the following internal issues: manipulation of personal data, breach of confidentiality, unauthorized access to assets containing sensitive data of the organization, financial losses, interruption of basic activities (courses, exams, inability to enroll in studies), interruption of services, disruption of internal operations and with third parties, financial costs associated with loss of staff, replacement of equipment, value of research, loss of assets, loss of competitive advantage.

External issues cannot be controlled by HEIs, and the following issues need attention: higher-level laws and regulations (state, governmental), socio-cultural and natural environment, financial and macroeconomic, technological.

Depending on the structure and size of the HEI, for the implementation of the CSCF, it is necessary to form a team responsible for the implementation and control of the concept of cybersecurity, consisting of the Information Security Officer and other members. The ISO 27001 standard requires regular and mandatory qualifications of the Information Security Officer, who can be recruited both from university staff and from outside, as long as there are documents attesting the qualification required to hold this position.

Security policies

Security policy reflects the attitude of HEI management towards cybersecurity. The main objective for the implementation of security policies, according to ISO 27002, is to provide management direction and support for information security in accordance with relevant business requirements, laws and regulations (ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls 2013).

The analysis of university websites in the Republic of Moldova revealed that academic institutions have published the GDPR Policy, but there are no general or specific security policies, as confirmed by the results of the author's survey involving 9 stakeholders from the most large higher education institutions in the Republic of Moldova, of which only 22.2% stated that they have internal security policies.

According to several researchers (Ghazvini, Shukur, and Hood 2018; Flowerday and Tuyikeze 2016) the way in which security policies are developed and implemented remains uncertain, which is a shortcoming of this stage. The content of security policies also differs, creating uncertainty about the content.

It is recommended for the development of security policies in academic institutions in Moldova to follow the following steps, reflected in Figure 6.

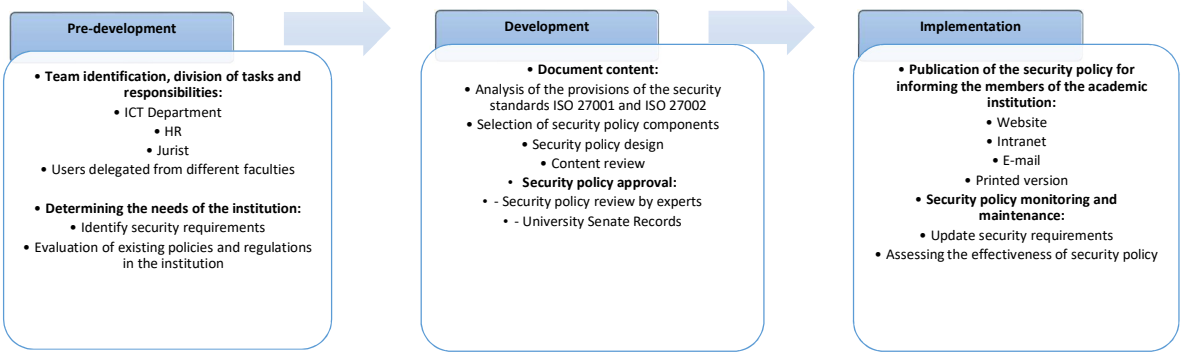

Fig 6. Generic framework for security policies development in HEIs

It is recommended that the security policy as well as the specific security policies be established in accordance with the structure reflected in Table 2.

Table 2. The structure of security policy

Key items	**Justification** (According to the provisions of the ISO 27002 standard)
Title	General or specific: control access, backups, BYOD, etc.
Version and authors	It will include all existing versions of the respective security policy, the date of the changes, the responsible person

Goal	Describes the expectations of the administration of the institution as a result of the implementation of the policy and the problems that will be solved
Scope and boundaries	Describe the area to be covered by the policy, such as: access control, security of communication, acceptable use, etc .; to whom that security policy is addressed
Presentation	A brief description of cybersecurity issues, which may include threats, vulnerabilities and risks specific to the field of education
Security policy requirements	Describe in detail, as clearly and explicitly as possible, the requirements of the institution
Roles and responsibilities	Defines who is responsible for violating security policy requirements and where security incidents can be reported
Related documents	Describe other relevant policies (if any) that may help minimize security issues and incidents, or links to additional support

4.2.3 Scope and boundaries of CSCF

The need to reflect a generic reference architecture specific to the university environment on the one hand provides an overview of the typical functionality (Pääkkönen and Pakkala 2015) of academic activities, and on the other hand supports the creation of architectures for each institution (Angelov, Grefen, and Greefhorst 2012), which aims to implement a security concept.

The empirical study facilitated the creation of a generic reference architecture specific to the university environment in Moldova, obtained from semi-structured interviews with university network administrators reflected in Figure 7.

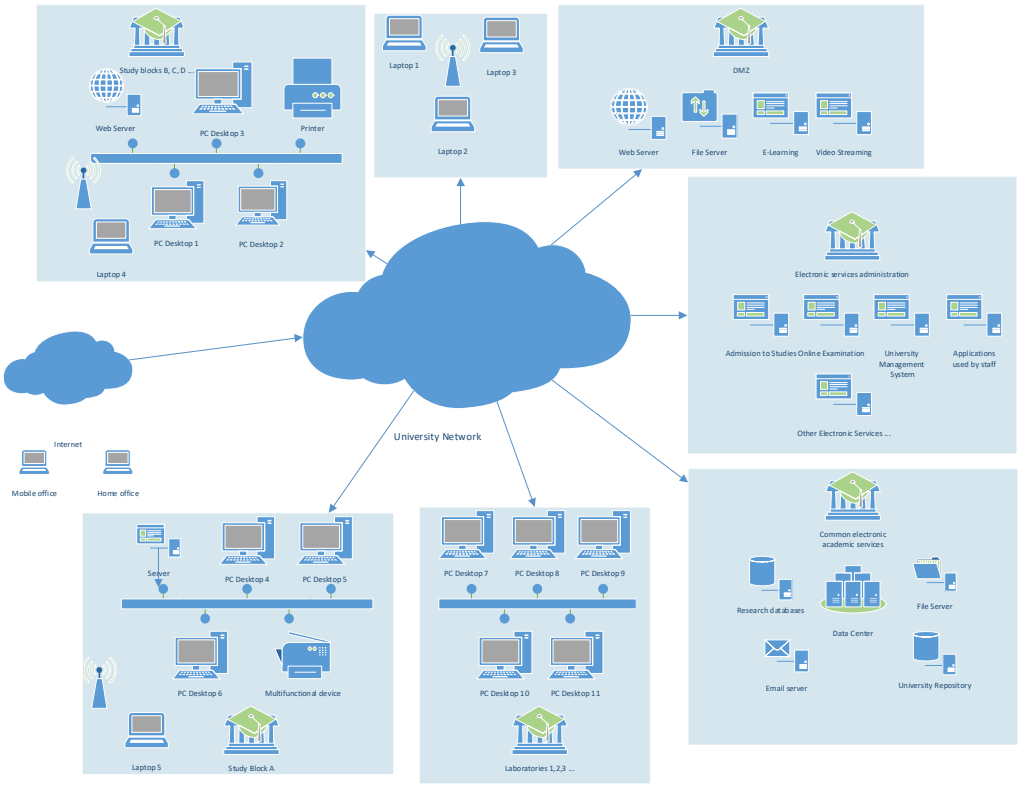

Fig 7. The reference architecture of HEIs in Moldova

The identification of the academic business processes allowed the development of the CSCF artifact oriented towards the university environment, in order to satisfy the Target Group Oriented criterion. Business processes can be defined as "sets of interconnected tasks that lead to the creation of a product or service" (Ivanov et al. 2011). Basic university business processes are education and research. The CSCF will only consider the components of the education process, as it also includes the research aspects, the results are exposed in the table 3.

Table 3. Academic business processes

Academic business processes	Description

Common academic services	Network infrastructure Stationary workstations (Laboratories) Mobile workstations or BSOD Remote work (VPN, WLAN) Centralized services: - website - virtual servers - centralized access control, - user identification and authentication - email services - file services
Admission to Studies	- application process - preliminary examination - the approval processes - generate notifications - final approval - deletion of the applicant's data
IT infrastructure for students	- laboratories with specialized equipment - video conferencing applications - online learning platforms
Online examination	- creating exam questions - creating the evaluation test - attendance control - exam evaluation - notation in the dean's office system - publishing / announcing test results, archiving the results - creating backups - creating the archive - creating the paper archive - verification of information
University Management System	- administration of the student's entire academic career, - results of examination sessions, - contract and study agreement - electronic register - anti-plagiarism system for students, - additional fees, - holiday order, - employee pay slips, - orders and regulations, university news

This list is not exhaustive, other university activities can be excluded / included, depending on the spectrum of electronic services provided by HEI, thus supporting the scalability criterion of CSCF.

Depending on the protection requirements, the recommended security controls are proposed to be classified into:

- Basic (mandatory) security controls required to be mandatorily implemented by any HEI that creates a security concept;
- Standard security controls for institutions aimed at certification with ISO 27001 or another security standard.

4.2.4 Risk management

In order to support the criteria of International Importance and Risk Management, it is recommended to use the ISO 27005 standard, due to its international importance and because it is a direct support for the implementation of ISO 27001, a standard selected as a reference for creating the CSCF artifact. Risk management includes coordinated activities to manage and control an organization in terms of risk (ISO/IEC 27000:2018, 2018.).

Cyber risk can be defined as a security event that exploited a vulnerability in the information system and caused the threat (Wangen, Hallstensen, and Snekkenes 2018; Ulven and Wangen 2021). An information security event is an identified occurrence of a system, service, or network state that indicates a possible breach of information security policy, or a failure of controls, or a previously unknown situation that may be relevant to security (ISO/IEC 27000:2018, 2018) and has a impact and a likelihood (Wangen, Hallstensen, and Snekkenes 2018; ISO/IEC 27005: Information technology — Security techniques — Information security risk management 2018). The basis of information risk analysis is the process of identifying threats (Szczepaniuk et al. 2020), which are defined as "any phenomenon (process, event), undesirable in terms of undisturbed operation of a system" (Szczepaniuk et al. 2020).

As previously stated in this research paper, a holistic approach to cybersecurity management in HEIs is essential because it provides an overview of all resources that need to be protected. Risk assessment methods should take into account the dependencies between the resources that assist university electronic services (Hariyanti, Djunaidy, and Siahaan 2018), so the methods must be able to adapt and be dynamic and appropriate for the university environment. As electronic services are constantly changing, risk factors are changing (Harkins 2016) and affecting the value of university activities (Rojas and Lesmes 2016).

From the considerations presented above, a new approach to risk management is proposed in terms of university business processes, because they are limited in number, versus the impressive number of support assets, and the assessment of security risks in terms of business processes supports the holistic approach to cybersecurity in academia. Thus, when designing a new business process, security risks are taken into account, this new concept is called "risk conscious business process management" (Ahmed and Matulevičius 2014; Khanmohammadi and Houmb 2010; Jakoubi et al. 2010).

Another problem that can be solved by addressing the security risks associated with business processes are the information assets in the Cloud and the services provided by third parties, which make the identification of information assets a very difficult process (Hariyanti, Djunaidy, and Siahaan 2018).

The ISO 27001 standard does not stipulate the obligation to implement a risk register, but such an approach will allow to comprehensively address the security risks, in which all the data related to the risks, impact, likelihood and controls that are already in place will be systematized implemented to change the risk. This hypothesis has been confirmed by other researchers (Haji, Tan, and Costa 2019) and international best practices (ISACA Germany Chapter, 2017). The risk register can serve in the case of certification as a mandatory document, namely the Risk Assessment Report. The model proposed by me, which can be used for the holistic approach in the risk assessment process is presented in figure 8.

SECURITY RISKS REGISTER											
Department:		Risk Assessment Manager:					Approved by:			Reference No.	
Business process:		Member RA 1:									
BP location:		Member RA 2:					Signature				
Date:		Member RA 3:					Name:				
Version:		Member RA 4:					Position:				
Scheduled review:		Member RA 5:					Date:				
Identifying threats / vulnerabilities				Risk assessment			Risk control				
Asset category	Support assets	Threats / Vulnerabilities	Risk ID	Impact	Likelihood	Risk value	Risk options	Implemented controls	Asset owner	Comments	
Hardware											
Software											
Network and communications											
Personell											
Infrastructure											

Fig 8. Risk Register

A very important document for HEIs, which aims to be certified with ISO 27001, or which want to verify the level of compliance of the security controls implemented with Annex A of the ISO 27001 standard, is the Statement of Applicability, which identifies the applicable controls. A recommended pattern is shown in Figure 9.

Clause Annex A ISO 27001	Anexa A ISO 27001 Control	Control Description	Applicable	Justification	Reference Control	Status
A.5 Information Security Policies						
A.5.1 Management direction for information security	A.5.1.1Policies for Information Security	A set of information security policies must be defined, approved by management, published and communicated to employees and relevant third parties.	Yes	Security policy is required to inform employees / students and third parties about HEI's attitude towards information security	General security policy	Done
	A.5.1.2 Review of the policies for information security	Information security policies need to be reviewed at planned intervals or when changes occur to ensure their continued compliance, compatibility and effectiveness.	Yes	Updating security policy objectives and requirements is necessary due to the dynamic environment specific to university services	Information about the date and person responsible for reviewing the security policy	In process

Fig 9. Statement of Applicability

The final step is to implement the Risk Treatment Plan (RTP). Security controls for risk management, according to ISO 27005, can be taken from any source [37], the only condition is that they align with Annex A of ISO 27001 [4] and the Statement of Applicability of the academic institution. CSCF security checks are recommended to be retrieved from the IT Grundschutz Kompendium, which is a German-German guide, updated annually with recommended technical checks. The proposed model for the Risk Treatment Plan is reflected in Figure 10.

Risk Treatment Plan																
Department:			Responsabil RT:									Approved by:				
Business process:			Member RT 1:													
BP location:			Member RT 2:									Signature				
Date:			Member RT 3:									Name:				
Version:			Member RT 4:									Position:				
Scheduled review:			Member RT 5:									Date:				
Asset category	Support assets	Common Threats / Vulnerabilities	Specific Threats / Vulnerabilities			Security Controls						Compliance with ISO 27001	Comments			
							Implemented			Implemented						
						Basic Controls	Yes	No	Standard Controls	Yes	No					
Hardware																
Software																
Network and Communication																
Personnel																
Infrastructure																

Fig 10. Risk Treatment Plan

An important role is played by the owners of university business processes, in order to identify an effective and real risk-oriented Risk Management Plan, because they know best the business process support assets, which was the basis of the decision to interview HEIs stakeholders.

4.2.5 CSCF project

According to ISO 27003 (ISO&IEC, 2010), which provides clear guidance for implementing the security management system in an organization based on ISO 27001; the whole procedure by which the organization adopts a concept of cybersecurity must be carried out as a project.

The project represents the CSCF plan, which will include the organizational structure of the HEI and the required documentation, which demonstrates the concept's compliance with the reference standard (Asosheh, Hajinazari, and Khodkari 2013).

Once the CSCF has been implemented, it is necessary to regularly monitor all processes in order to ensure the compliance, compatibility and efficiency (ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT 2013) of

security controls. An important role is played by the internal audit, which aims to identify the CSCF's compliance (Cheung 2014) with the organization's requirements for cyber security and with the requirements of the international standard.

The results of the internal audit can be finalized by updating the security controls that have proven to be ineffective or by updating the security policies for those areas that are not covered.

The involvement of university top management in the design and implementation of the concept of cybersecurity is the key to successful IT governance.

5. DISCUSSION

Increasing cybersecurity in Higher Education Institutions by implementing a conceptual framework that represents the synergy between international standards in the field, such as: ISO 27001, ISO 27002, ISO 27005; and best practices developed by the Information Systems Audit and Control Association (ISACA) (ISACA Germany Chapter, 2017), will ensure the success of the implementation and the effectiveness of the security framework focused on the academic processes of HEIs in the Republic of Moldova.

The identification of university business processes, specific to Moldovan universities and the author's recommendations related to the stages of implementation of the conceptual framework, will be an important resource for any Moldovan university that wants to implement a security concept. The resulting CSCF artifact is a practical guide according to which Higher Educational Institutions that have already implemented certain provisions of ISO 27001 will be able to assess their level of compliance, and those institutions that have not yet implemented, will be able to use it as a guide to secure their assets.

6. CONCLUSION

The current trends of HEIs in the Republic of Moldova are to provide quality studies that meet the standards of academic institutions around the world. Thus, in recent years a revolutionary evolution can be attested, through the implementation and use of learning platforms, university management systems or platforms for online examination. Migration from the traditional to the electronic environment has added value to academic processes on the one hand, and on the other hand has significantly increased cyber risks.

Thus, the need to implement a cybersecurity framework that reduces information risks increases over time. This scientific paper identified as a research problem: "the lack of a cybersecurity framework focused on academic processes in HEIs in the Republic of Moldova, which could be used as a reference framework", problem also defined in the Information Security Strategy for 2019-2024 (RM Parliament, 2018), adopted by the Parliament of the Republic of Moldova. So, the aim was to develop a Cyber Security Conceptual Framework, which can be used to implement a security concept.

The DSR scientific method was selected to develop the conceptual framework due to its potential to contribute to encouraging the innovation capacities of organizations, as well as to contribute to the sustainable transformation of society (vom Brocke, Hevner, and Maedche 2020; Watson, Boudreau, and Chen 2010), but especially because the finality of the processes DSR is an artifact that solves a problem in the field. DSR projects must offer both intellectual merit in creative design and extended impact in the field of application through original solutions to the research problem (Hevner et al. 2004; Baskerville et al. 2018). The analysis of the business environment and the derivation of the specific needs to be solved build the starting point of a DSR project.

Based on the above, CSCF was created by analyzing the academic processes of HEIs in the Republic of Moldova, the specific needs, which were identified by empirical study, conducted by a survey completed by HEIs stakeholders and by semi-structured interviews to identify support assets of university business processes.

The selection of the ISO 27001 standard, as a reference standard, is argued by the international importance it demonstrates, but also as a result of the review of scientific articles from the last 10 years. The Bologna Process, implemented by all HEIs in the Republic of Moldova, also recommends the implementation in academic institutions of standardized practices or those with recognized international value.

Identifying the key processes and phases of CSFC implementation in the university environment would increase the cybersecurity of HEIs. Patterns for mandatory documents, according to the ISO 27001 standard, which must be held by the institution, have been proposed.

However, the author does not state the completeness of the proposed framework, and future research directions will focus on the completeness and refinement of the processes of the Cyber Security Conceptual Framework.

The results of the research presented in this paper have significant practical and research contributions.

The practical contribution refers to the Cyber Security Conceptual Framework, oriented on the academic processes of the universities of the Republic of Moldova, in which concrete actions are proposed, focused on the needs of the

researched environment. The practical contribution also solves a national problem, defined in the Information Security Strategy for 2019-2024 of the Republic of Moldova.

Being a pioneer in this field in the Republic of Moldova, I dare to hope that the results of this project will increase the cybersecurity of HEIs in Moldova. With the growth of academic electronic services, the need to implement the concept of security will be growing, and the CSCF artifact will be a valuable guide.

Due to the international standards, used as a reference for the proposed framework, CSCF will be able to be implemented by other academic institutions, outside the country, the academic processes are similar.

There are not many studies in the field of research that reflect how cybersecurity can be enhanced by HEIs, so this paper will add value. The analysis of scientific papers published by researchers in the Republic of Moldova, focusing on the cybersecurity of universities, apart from the articles previously published by the author, showed, that there are no other studies, so important contributions are made to the knowledge base.

7. REFERENCES

1. Ahmed, Naved, and Raimundas Matulevičius. 2014. "Securing Business Processes Using Security Risk-Oriented Patterns." *Computer Standards & Interfaces* 36 (4): 723–33. https://doi.org/10.1016/j.csi.2013.12.007.
2. Alexei, Arina. 2021. "Ensuring Information Security in Public Organizations in The Republic of Moldova through the ISO 27001 Standard." *Journal of Social Sciences* IV (1) (March). https://doi.org/10.52326/jss.utm.2021.4(1).11.
3. Alexei, Arina. 2021. "Network Security Threats to Higher Education Institutions." In *CEE E|Dem and E|Gov Days*, 323–33. Budapest. https://doi.org/10.24989/ocg.v341.24.
4. Alexei, Arina. 2021. "Using Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova." In *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: Technical University of Moldova.
5. Alexei, Arina. 2021. "Cyber Security Strategies for Higher Education Institutions." *Journal of Engineering Science* XXVIII (4): 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07.
6. Alexei, Arina, and Alexei Anatolie. 2021. "Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning." *International Journal of Scientific & Technology Research* 10 (3).
7. Alexei, Arina, Nistiriuc Pavel, and Alexei Anatolie. 2021. "Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions." In *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: Technical University of Moldova.
8. Angelov, Samuil, Paul Grefen, and Danny Greefhorst. 2012. "A Framework for Analysis and Design of Software Reference Architectures." *Information and Software Technology* 54 (4): 417–31. https://doi.org/10.1016/j.infsof.2011.11.009.
9. Asosheh, Abbass, Parvaneh Hajinazari, and Hourieh Khodkari. 2013. "A Practical Implementation of ISMS." In *7th International Conference on E-Commerce in Developing Countries:With Focus on e-Security*. IEEE. https://doi.org/10.1109/ECDC.2013.6556730.
10. Barbara Kitchenham. 2004. "Procedures for Performing Systematic Reviews." *Eversleigh NSW 1430*, Australia.
11. Baskerville, Richard, Abayomi Baiyere, Shirley Gergor, Alan Hevner, and Matti Rossi. 2018. "Design Science Research Contributions: Finding a Balance between Artifact and Theory." *Journal of the Association for Information Systems* 19 (5). https://doi.org/10.17705/1jais.00495.
12. Brocke, Jan vom, Alan Hevner, and Alexander Maedche. 2020. "Introduction to Design Science Research." In: vom Brocke J., Hevner A., Maedche A. (eds) Design Science Research. Cases. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-030-46781-4_1.
13. Chandra Kruse, Leona, Stefan Seidel, and Jan vom Brocke. 2019. "Design Archaeology: Generating Design Knowledge from Real-World Artifact Design." In: Tulu B., Djamasbi S., Leroy G. (eds) *Extending the Boundaries of Design Science Theory and Practice*. DESRIST 2019. Lecture Notes in Computer Science, vol 11491. Springer, Cham. https://doi.org/10.1007/978-3-030-19504-5_3.
14. Cheung, Simon K. S. 2014. "Information Security Management for Higher Education Institutions." In: Pan JS., Snasel V., Corchado E., Abraham A., Wang SL. (eds) Intelligent Data analysis and its Applications, Volume I. Advances in Intelligent Systems and Computing, vol 297. Springer, Cham. https://doi.org/10.1007/978-3-319-07776-5_2

15. Das, Saini, Arunabha Mukhopadhyay, and Bharat Bhasker. 2013. "Today's Action Is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School." *Journal of Cases on Information Technology* 15 (3). https://doi.org/10.4018/jcit.2013070101.
16. Disterer, Georg. 2013. "ISO/IEC 27000, 27001 and 27002 for Information Security Management." *Journal of Information Security* 04 (02). https://doi.org/10.4236/jis.2013.42011.
17. Donaldson, Scott E., Stanley G. Siegel, Chris K. Williams, and Abdul Aslam. 2015. "Cybersecurity Frameworks." In *Enterprise Cybersecurity*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4302-6083-7_17.
18. Dresch, Aline, Daniel Pacheco Lacerda, and José Antônio Valle Antunes Jr. 2015. *Design Science Research*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07374-3.
19. Esparza, Daisy Elizabeth Imbaquingo, Francisco Javier Diaz, Tatyana Katherine Saltos Echeverria, Silvia Rosario Arciniega Hidrobo, Diego Andres Leon Villavicencio, and Adrian Robayo Ordonez. 2020. "Information Security Issues in Educational Institutions." In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE. https://doi.org/10.23919/CISTI49556.2020.9141014.
20. Flowerday, Stephen v., and Tite Tuyikeze. 2016. "Information Security Policy Development and Implementation: The What, How and Who." *Computers & Security* 61 (August). https://doi.org/10.1016/j.cose.2016.06.002.
21. Gërvalla, Muhamet, Naim Preniqi, and Peter Kopacek. 2018. "IT Infrastructure Library (ITIL) Framework Approach to IT Governance." In *IFAC-PapersOnLine*, 51:181–85. Elsevier B.V. https://doi.org/10.1016/j.ifacol.2018.11.283.
22. Ghazvini, Arash, Zarina Shukur, and Zaihosnita Hood. 2018. "Review of Information Security Policy Based on Content Coverage and Online Presentation in Higher Education." *International Journal of Advanced Computer Science and Applications* 9 (8). https://doi.org/10.14569/IJACSA.2018.090853.
23. Haji, Sami, Qing Tan, and Rebeca Soler Costa. 2019. "A Hybrid Model for Information Security Risk Assessment." *International Journal of Advanced Trends in Computer Science and Engineering*, February, 100–106. https://doi.org/10.30534/ijatcse/2019/1981.12019.
24. Hariyanti, Eva, Arif Djunaidy, and Daniel Oranova Siahaan. 2018. "A Conceptual Model for Information Security Risk Considering Business Process Perspective." In *2018 4th International Conference on Science and Technology (ICST)*. IEEE. https://doi.org/10.1109/ICSTC.2018.8528678.
25. Harkins, Malcolm W. 2016. *Managing Risk and Information Security*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-1455-8.
26. Haufe, Knut, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis, and Vladimir Stantchev. 2016. "ISMS Core Processes: A Study." *Procedia Computer Science* 100 (January): 339–46. https://doi.org/10.1016/J.PROCS.2016.09.167.
27. Hevner, March, Park, and Ram. 2004. "Design Science in Information Systems Research." *MIS Quarterly* 28 (1). https://doi.org/10.2307/25148625.
28. Hommel, Wolfgang, Stefan Metzger, and Michael Steinke. 2015. "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization." *EUNIS Journal of Higher Education IT*.
29. Humayun, Mamoona, Mahmood Niazi, NZ Jhanjhi, Mohammad Alshayeb, and Sajjad Mahmood. 2020. "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study." *Arabian Journal for Science and Engineering* 45 (4). https://doi.org/10.1007/s13369-019-04319-2.
30. ISO/IEC 27003: Information technology — Security techniques — Information security management systems — Guidance. 2017. "International Organization for Standardization." Geneva. https://www.iso.org/standard/63417.html.
31. ISACA Germany Chapter e.V. Oberwallstr. 24 10117 Berlin, Germany. 2017. "Implementation Guideline ISO/IEC 27001:2013." Berlin.
32. ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls. 2013. "International Organization for Standardization." *Switzerland*.
33. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. 2013. "International Organization for Standardization." Geneva, Switzerland. https://www.iso.org/isoiec-27001-information-security.html.
34. ISO/IEC 27005: Information technology — Security techniques — Information security risk management. 2018. "International Organization for Standardization." Geneva, Switzerland.

35. ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2018. "International Organization for Standardization." Geneva, Switzerland. 2018. https://www.iso.org/standard/73906.html.
36. Itradat, Awni, Sari; Sultan, Maram; Al-Junaidi, Rawa'a; Qaffaf, Feda'a; Mashal, and Fatima Daas. 2014. "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study." *Jordan Journal of Mechanical & Industrial Engineering* 8 (2): 102–18.
37. Ivanov V., Tzaneva M., Murdjeva A., Kisimov V. 2011. "Securing the Core University Business Processes." In: Camenisch J., Kisimov V., Dubovitskaya M. (eds) Open Research Problems in Network Security. iNetSec 2010. Lecture Notes in Computer Science, vol 6555. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19228-9_9
38. Jakoubi, Stefan, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler. 2010. "Risk-Aware Business Process Management—Establishing the Link Between Business and Security." In: Xhafa F., Barolli L., Papajorgji P. (eds) Complex Intelligent Systems and Their Applications. Springer Optimization and Its Applications, vol 41. Springer, New York, NY. https://doi.org/10.1007/978-1-4419-1636-5_6.
39. Jang-Jaccard, Julian, and Surya Nepal. 2014. "A Survey of Emerging Threats in Cybersecurity." In *Journal of Computer and System Sciences*, 80:973–93. Academic Press Inc. https://doi.org/10.1016/j.jcss.2014.02.005.
40. Joshi, Chanchala, and Umesh Kumar Singh. 2017. "Information Security Risks Management Framework – A Step towards Mitigating Security Risks in University Network." *Journal of Information Security and Applications* 35 (August). https://doi.org/10.1016/j.jisa.2017.06.006.
41. Khanmohammadi, Kobra, and Siv Hilde Houmb. 2010. "Business Process-Based Information Security Risk Assessment." In *2010 Fourth International Conference on Network and System Security*, 199–206. IEEE. https://doi.org/10.1109/NSS.2010.37.
42. Khther, Rasha Adnan, and Marini Othman. 2013. "Cobit Framework as a Guideline of Effective It Governance in Higher Education: A Review." *International Journal of Information Technology Convergence and Services* 3 (1). https://doi.org/10.5121/ijitcs.2013.3102.
43. Koong, K., and M Yunis. 2015. "Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework." In *AMCIS 2015 Proceedings*.
44. MacCuspie, Robert I., Harvey Hyman, Chris Yakymyshyn, Sesha S. Srinivasan, Jaspreet Dhau, and Christina Drake. 2014. "A Framework for Identifying Performance Targets for Sustainable Nanomaterials." *Sustainable Materials and Technologies* 1–2 (December): 17–25. https://doi.org/10.1016/J.SUSMAT.2014.11.003.
45. Merchan-Lima, Jorge, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. 2020. "Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review." *Annals of Telecommunications*, July. https://doi.org/10.1007/s12243-020-00783-2.
46. Myers, Michael D., and Michael Newman. 2007. "The Qualitative Interview in IS Research: Examining the Craft." *Information and Organization* 17 (1). https://doi.org/10.1016/j.infoandorg.2006.11.001.
47. Nowak, G. J. 2015. "Information Security Management with Accordance to ISO27000 Standards: Characteristics, Implementations, Benefits in Global Supply Chains." In *Logistyka*, 639–54.
48. Oltramari, Alessandro, Noam Ben-Asher, Lorrie Cranor, Lujo Bauer, and Nicolas Christin. 2014. "General Requirements of a Hybrid-Modeling Framework for Cyber Security." In *2014 IEEE Military Communications Conference*. IEEE. https://doi.org/10.1109/MILCOM.2014.28.
49. Pääkkönen, Pekka, and Daniel Pakkala. 2015. "Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems." *Big Data Research* 2 (4): 166–86. https://doi.org/10.1016/J.BDR.2015.01.001.
50. Parlamentul RM. 2018. "Strategia Securității Informaționale a RM Pentru Perioada 2019-2024." November 22, 2018. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fgov.md%2Fsites%2Fdefault%2Ffiles%2Fdocument%2Fattachments%2Fintr23_86.pdf.
51. Peffers, Ken, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. 2007. "A Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems* 24 (3). https://doi.org/10.2753/MIS0742-1222240302.

52. Rehman, Huma, Ashraf Masood, and Ahmad Raza Cheema. 2013. "Information Security Management in Academic Institutes of Pakistan." In *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/NCIA.2013.6725323.
53. Rojas, Oscar González, and Sebastián Lesmes. 2016. "Value at Risk Within Business Processes: An Automated IT Risk Governance Approach." In *BPM*.
54. Singh Umesh Kumar, and Joshi C. 2016. "Quantitative Security Risk Evaluation Using CVSS Metrics by Estimation of Frequency and Maturity of Exploit." In *Proceedings of the World Congress on Engineering and Computer Science*. San Francisco.
55. Solms, Basie von, and Rossouw von Solms. 2018. "Cybersecurity and Information Security – What Goes Where?" *Information & Computer Security* 26 (1). https://doi.org/10.1108/ICS-04-2017-0025.
56. Suroso, Jarot S., and Muhammad A. Fakhrozi. 2018. "Assessment of Information System Risk Management with Octave Allegro at Education Institution." *Procedia Computer Science* 135. https://doi.org/10.1016/j.procs.2018.08.167.
57. Suwito, Misni Harjo, Shinchi Matsumoto, Junpei Kawamoto, Dieter Gollmann, and Kouichi Sakurai. 2016. "An Analysis of IT Assessment Security Maturity in Higher Education Institution." In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-10-0557-2_69.
58. Szczepaniuk, Edyta Karolina, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. "Information Security Assessment in Public Administration." *Computers and Security* 90 (March): 101709. https://doi.org/10.1016/j.cose.2019.101709.
59. Ulven, Joachim Bjørge, and Gaute Wangen. 2021. "A Systematic Review of Cybersecurity Risks in Higher Education." *Future Internet* 13 (2): 39. https://doi.org/10.3390/fi13020039.
60. Wangen, Gaute, Christoffer Hallstensen, and Einar Snekkenes. 2018. "A Framework for Estimating Information Security Risk Assessment Method Completeness." *International Journal of Information Security* 17 (6). https://doi.org/10.1007/s10207-017-0382-0.
61. Watson, Boudreau, and Chen. 2010. "Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community." *MIS Quarterly* 34 (1). https://doi.org/10.2307/20721413.
62. Wolden, Mark, Raul Valverde, and Malleswara Talla. 2015. "The Effectiveness of COBIT 5 Information Security Framework for Reducing Cyber Attacks on Supply Chain Management System." In *IFAC-PapersOnLine*, 28:1846–52. Elsevier. https://doi.org/10.1016/j.ifacol.2015.06.355.
63. Yustanti, W, A Qoiriah, R Bisma, and A Prihanto. 2018. "An Analysis of Indonesia's Information Security Index: A Case Study in a Public University." *IOP Conference Series: Materials Science and Engineering* 296 (January). https://doi.org/10.1088/1757-899X/296/1/012038.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 53-58 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

DEVELOPMENT OF THE STRUCTURAL AND ANALYTICAL MODELS FOR EARLY APT-ATTACKS DETECTION AND INTRUDERS IDENTIFICATION

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab, National Aviation University, Kyiv, Ukraine
Zhadyra Avkurova, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
Andriy Tolbatov, NAU Cybersecurity R&D Lab, National Aviation University, Kyiv, Ukraine
Yevheniia Krasovska, Professional College of Engineering and Management, National Aviation University, Kyiv, Ukraine
Bagdat Yagaliyeva, Yessenov University, Aktau, Kazakhstan
Oleksii Verkhovets, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine

ABSTRACT: Modern information and communication technologies (ICT) are vulnerable to APT-attacks (advanced persistent threats) and other relevant threats. APT-attack is a stealthy threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to ICT and remains undetected for an extended period. Early detection of APT-attack is very important for ICT of critical infrastructure sectors. But existed approaches don't allow to detect attacks effectively in cyberspace as fuzzy environment. In this paper, a method of linguistic terms using statistical data was used for structural and analytical models of parameters (both host and network parameters) as well as intruder model based on the defined host and networks parameters was developed. Based on this, logical rules can be developed to provide the functioning of IDS based on honeypot (or other) technology for APT-attacks detection and intruder type identification in ICT.

KEYWORDS*: APT-attack, Early Detection, Identification, Honeypot, Fuzzy Logic, Parameter, ICT.*

1. Introduction

The development of information and communication technology (ICT) creates new types of threats to information security, among which the intruder in computer systems and networks (for example, APT-attacks or other negative influences) occupies a prominent place. To effectively counter this threat, IDS (intruder detection system) are being developed to detect and identify an intruder. Early detection is important and not simple task for security side. Typical IDS should perform the following main functions [1]:

- monitor and analyze the activity of ICS (information and communication system) users;
- capture system configurations and vulnerabilities;
- assess the integrity of critical system files and data files;
- recognize activity patterns that reflect known attacks;
- perform statistical analysis to detect abnormal behavior;
- recognize violations of security policy by the system user.

2. Related papers analysis and problem statement

The IDS tasks can be divided into global and local. Global tasks is recognition of the violator (intruder) and legitimate user. The solution of this problem contains the following stages [2-3]: data collection, filtering, behavior classification – directly the process of recognizing the violator, report and response system. As can be seen from the main functions and tasks of IDS, one of the most important aspects of their functioning is not only the fixation of intrusion in ICS, but also its identification.

There are many studies related with APT-attacks early detection. In [4-5] the big data processing approach was proposed for APT-attacks detection. In [6-9] authors proposed malware and DoS-attacks detection system as well as game theory based approach for APT-attacks detection. Presented techniques have many advantages (indicators, correlation, high-speed and others), but they don't allow identifying intruders` category as well as don't give possibility to operate with fuzzy parameters. That is why, the ***main task*** of this study is creation the possibility for early APT-attacks detection using developed structural and analytical models based on network and host parameters as well as method of linguistic terms using statistical data.

3. Development of the structural and analytical models based on host and network parameters

Basic parameters for intruders identification

In the process of attack, the violator, acting on the system, changes certain parameters, creates or terminates its inherent processes, and so on. All these actions are reflected in the state of the system. Evaluating these parameters, you can detect the fact of intrusion into the system. The work of modern IDSs is based on this principle. Thus, the NIDES system performs audits of such processes as logging in, working with files and processes, administration and fixing errors and failures. Previous works describe the parameters by which the violator is identified by the developed system. These parameters (are host settings) include:

Host Parameters (HIDS): Username at login, *UID;* Login time, *Tlog;* Frequency of login requests, *Nlog;* Time spent logging in, *TSlog;* Intensity of actions, *I;* Processor time / CPU usage, *CPU;* The amount of RAM load, *Muse;* Number of executable files, *NEF;* The type of files used in the attack, *AtEF;* Number of failures and errors, *NEr;* Process / file execution time, *RTPr/F;* Unusual processes, *UPr;* File transfer to the system, *TrFin;* Files changes, *ModF;copying* / transferring files from the system, *TrFout;* Pressing the keyboard keys, *KS.*

Network Parameters (NIDS) – characteristics of *ARP-, IP-, ICMP-* and *TCP*-packages.

Since the process of detection and identification of the violator takes place in conditions of uncertainty, and some of the parameters of the IDS are unclear, the operation of such a system should be based on fuzzy logic. To identify the violator, we can use the logical-linguistic approach and the basic model of parameters, partially described in [10], which will be the basis for the construction of the developed IDS. For example, to detect the process of port scanning in section [11] used linguistic variables (LV) "Number of virtual channels" and "Age of virtual channels", and in section [12] LV "Number of simultaneous connections", "Query processing speed", "Delay between requests" and 'Number of packets with the same sender and recipient address"– to detect DDoS attacks and spoofing.

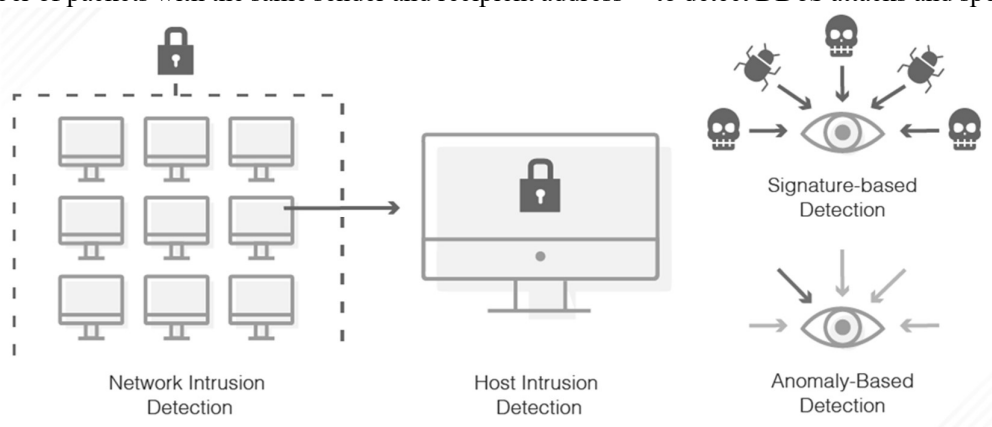

Figure 1. Difference between HIDS and NIDS

The process of detecting and identifying the violator requires determining the necessary parameters and their properties. In this regard, the main purpose of this work is to build models of standards required for the operation of IDS in a vaguely defined, poorly formalized environment.

Method of linguistic terms using statistical data

Consider the method of linguistic terms using statistical data (MLTS) [13], where as a measure of belonging of the element to the set is an estimates of the frequency of use of the concept, which is given by a fuzzy set to characterize the element. To do this, the values of the linguistic variable (LV) are placed on the universal scale [0; 1] $X=\{x_1, x_2, \dots, x_n\}$. The method is based on the condition that the same number of experiments falls into each interval of the scale, but this is usually not followed in practice. An empirical table is compiled in real conditions, in which experiments can be unevenly distributed over intervals. Some of them may not be involved, and then the data is processed using a matrix of prompts. May it is necessary to estimate in values of LV deviations of the parameter $\Delta B \in [0, B]$ (where B is the maximum possible deviation), which characterizes the current measurements. Next for $n = 5$ determine the value of LV $\{x_1, x_2, x_3, x_4, x_5\}$. Interval $[0, B]$ and $\Delta B/B$ (estimated ratio) divided

into k segments (for example, 5), on which the statistics characterizing frequency of use by the expert of the value of drugs for the display of the conclusions gathers. Then the data are entered into the table and processed to reduce the errors made during the experiment: the table is removed individual elements on the left side and on the right side of which there are zeros in the row. The tooltip matrix is a string whose elements are calculated by the formula:

$$k_j = \sum_{i=1}^{n} b_{ij} = \sum_{i=1}^{5} b_{ij},\ j = \overline{1,5}. \quad (1)$$

Next, in the resulting row of the matrix, the maximum element is selected $k_{\max} = \max k_j$, and then all elements of the table are converted by expression

$$c_{ij} = b_{ij} k_{max} / k_j,\ i = \overline{1,5}; j = \overline{1,5}, \quad (2)$$

and for columns, where $k_j = 0$ the linear approximation is applied $c_{ij} = (c_{ij-1} + c_{ij+1})/2,\ i = \overline{1,5}; j = \overline{1,5}$.

Next, calculate the value of MF (membership function) by the formula

$$\mu_{ij} = c_{ij} / c_{imax},\ c_{imax} = \max_j c_{ij},\ i = \overline{1,5}; j = \overline{1,5}. \quad (3)$$

The described method uses data from statistical studies. Their processing is quite time consuming, because to build a MF of one term it is necessary to conduct statistical studies of all terms of LV. We construct a model of standards of linguistic variables for fuzzy parameters of violator identification from the set of parameters (host and network). Model contains (4) as well as Table 1 and Table 2.

DIO = <UID, Tlog, Nlog, TSlog, I, CPU, MUse, NEF, AtEF, NEr, RTPr/F, UPr, TrFin, ModF, TrFout, KS, ARP, IP, ICMP, TCP>. (4)

Models of intruders host and networks parameters

The system must monitor certain parameters of the IS (Table 1), record them and identify violator.

Table 1 – Host parameters for violator identification and their characteristics

Parameter	Blur	Human				Bot	
		Misinformer	*Spammer*	*Cracker*	*Hacker*	*Spam-bot*	*Bot-hackers*
UID	-	+	-	+	+	-	+
Tlog	+	Depending on the time of day (*)	-	*	*	-	*
Nlog	+	Above average (***)	-	***	***	-	High
TSlog	+	***	-	***	***	-	***
I	+	Within the norm	Within the norm	Within the norm	Within the norm	Above the norm	***
CPU	+	***	***	***	***	***	***
MUse	+	***	***	***	***	***	***
NEF	+	Not within the norm	-	Not within the norm	Not within the norm	-	Not within the norm
AtEF	-	Scripts and PHP scripts	PHP scripts	Executa-ble files	Scripts	PHP scripts	Scripts
NEr	+	***	***	***	***	***	***
RTPr/F	+	Differs from the typical time (**)	**	**	**	**	**
UPr	-	Present	Present	Present	Present	Present	Present
TrFin	-	Present	Present	Present	Mostly absent	Present	Mostly absent
ModF	-	Present	Absent	Present	Mostly	Absent	Mostly present

TrFout	-	Absent	Absent	Mostly present	Present	Absent	Present
KS	-	It is fixed	It is fixed	It is fixed	It is fixed	It is not fixed	It is not fixed

Network part works with network traffic and detect attacks associated with low-level impact on network protocols, and can detect attacks on multiple network hosts. Network VDS is based on an intelligent traffic analyzer, which processes each frame of data passing through it, in order to search for prohibited signatures that indicate attacks. Network data, network traffic is received from a network adapter operating in a promiscuous mode (i.e. receiving all packets on the network).

Consider ***network parameters*** (with the characteristics of the TCP / IP protocols) in more detail:

Table 2 – Network parameters for intruder identification and their characteristics

Parameter	Blur	Human				Bot	
		Misinformer	*Spammer*	*Cracker*	*Hacker*	*Spam bot*	*Bot hackers*
ARP- request	-	Doesn't meet the allowed (****)	****	****	****	****	****
IP- fragment	-	****	****	****	****	****	****
ICMP- message	-	****	****	****	****	****	****
TCP- package	-	****	****	****	****	****	****

ARP request is monitored by the following parameters: IP address of source; source hardware address; network interface that limits the ARP request.

IP-fragment: source address; receiver address; protocol field; offset field; length; header length; MF bit; identification.

ICMP message: source IP address; IP address of the receiver; ICMP field type; ICMP identifier; ICMP sequence number.

TCP-package: source IP address; IP address of the receiver; TCP source port; TCP receiver port; bits of the TCP code.

All these network parameters, provided the correct configuration of the interconnection policy, clearly indicate the attack, and therefore belong to the group of clear.

4. Structural and analytical models

System login time, Tlog. This parameter is based on the fact that the activity of the ICS and users of this system depends on the time of receipt. Usually, the usual greater activity of users to log in is detected on the last day, less – at night. Still, other statistics are possible, determined by the mode of operation of the organization to which the ICS belongs. The nature of these parameters is unclear, due to which it is impossible to conclude the message's illegal activity unambiguously. Thus, in organizations working from 08.00 to 16.00, the probability of who is the user who logs in – the message is lowest at 08.00 and increases over time, reaching a maximum in the years after 16.00. However, it should be changed that in the concepts of honeypot-technology, this parameter loses weight, as any activity on them is considered criminal. Let's evaluate the LV "Level of legitimacy over time". Determine the value of the linguistic variable $\{x_1, x_2, x_3\}$, corresponding {legitimate, suspicious, illegitimate}. That is $T_{Tlog} = \bigcup_{i=1}^{3} T^i{}_{Tlog} = \{legitimate, suspicious, illegitimate\}$, we use statistics for $B = 24$ hours. It is advisable to divide the total interval into 4 intervals [00:00;06:00], [06:00;12:00], [12:00;18:00], [18:00;24:00].

Table 3 – Data for LV *Tlog*

The value of LV	Interval			
	№1	№2	№3	№4
High	0	8	6	1
Middle	2	1	2	3

Low	6	1	1	4

Using expression (1), we define $k_j = \|8\ 10\ 9\ 8\|$, where k_{max} = 10, and in accordance with (2) calculate:

$$\|c_{ij}\| = \begin{Vmatrix} 0 & 8 & 6,66 & 1,25 \\ 2,5 & 1 & 2,22 & 3,75 \\ 7,5 & 1 & 1,11 & 5 \end{Vmatrix}.$$

Calculate the MF by formula (3):

$$\|\mu_{ij}\| = \begin{Vmatrix} 0 & 1 & 0,83 & 0,16 \\ 0,66 & 0,26 & 0,59 & 1 \\ 1 & 0,13 & 0,15 & 0,66 \end{Vmatrix}.$$

For $\bigcup_{i=1}^{3} \mu_{ij}$ accordingly, we find the evaluation relationship $\bigcup_{i=1}^{3} \Delta B_i / B = \{0,25;\ 0,5;\ 0,75;\ 1\}$, and we obtain the following fuzzy numbers:

$$L = \{0/0,25;\ 1/0,5;\ 0,83/0,75;\ 0,16/1\},$$

$$P = \{0,66/0,25;\ 0,26/0,5;\ 0,59/0,75;\ 1/1\},$$

$$N = \{1/0,25;\ 0,13/0,5;\ 0,15/0,75;\ 0,66/1\}.$$

Schedule MF terms LV *Tlog* is shown in Fig. 2.

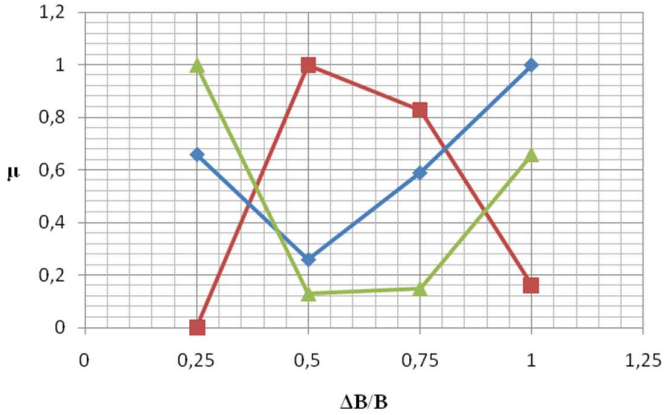

Figure 2. Linguistic standards of fuzzy numbers for *Tlog*

Analogically, using (1) - (3), structural and analytical models for other defined parameters (4) can be formed and presented.

5. Conclusions

In this paper, defined linguistic variables were introduced as well as structural and analytical models of parameters *Tlog, Nlog, TSlog, I, CPU, Muse, NEF, NEr, RTPr/F* were built. Also, for each described linguistic variables, MF were calculated and schedules of their terms were constructed. The formed standards are necessary for formation the system of logical rules allowing to provide functioning of IDS for APT-attacks detection and intruder category identification. Also, the intruder model based on the defined host and networks parameters was developed. These results can be used in sectors of critical infrastructure because APT-attacks are directed on them frequently.

The obtained results will be further used to build an IDS system (or other cyber threat detection system) based on honeypot technology or cloud architecture [14-17]. In the future, authors plan to create the rules system for effective detection the fact of intrusion in ICS and identification of the person (category) of the intruder.

REFERENCES

1. M. Khosravi and B. T. Ladani, "Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection", in IEEE Access, Vol. 8, pp. 162642-162656, 2020.
2. Denning D.E. "An Intrusion-Detection Model", IEEE Transactions On Software Engineering, February 1987, Vol. SE-13, No. 2, pp. 222-232.
3. Hu Z., Odarchenko R., Gnatyuk S., Zaliskyi M., Chaplits A., Bondar S., Borovik V. "Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior", International Journal of Computer Network and Information Security, Vol. 12, Issue 6, pp. 1-13, 2020.
4. Y. Qi, R. Jiang, Y. Jia and A. Li, "An APT Attack Analysis Framework Based on Self-define Rules and Mapreduce", 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020, pp. 61-66, doi: 10.1109/DSC50466.2020.00017.
5. D. Liu, H. Zhang, H. Yu, X. Liu, Y. Zhao and G. Lv, "Research and Application of APT Attack Defense and Detection Technology Based on Big Data Technology", 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2019, pp. 1-4, doi: 10.1109/ICEIEC.2019.8784483.
6. X. Liu, L. Li, Z. Ma, X. Lin and J. Cao, "Design of APT Attack Defense System Based on Dynamic Deception", 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 1655-1659, doi: 10.1109/ICCC47050.2019.9064206.
7. S. -P. Hong, C. -H. Lim and H. J. Lee, "APT attack response system through AM-HIDS", 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp. 271-274, doi: 10.23919/ICACT51234.2021.9370749.
8. Y. Su, "Research on APT attack based on game model", 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020, pp. 295-299, doi: 10.1109/ITNEC48623.2020.9084845.
9. M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova. A. Chaplits, "Method of traffic monitoring for DDoS attacks detection in e-health systems and networks", CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.
10. A. Paradise et al., "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks", in IEEE Transactions on Computational Social Systems, vol. 4, No. 3, pp. 65-79, Sept. 2017.
11. Svarovskiy S. "Approximation of membership functions for linguistic variables", Mathematical issues of data analysis, pp. 127-131, 1980.
12. M. Zuzcak and P. Bujok, "Causal analysis of attacks against honeypots based on properties of countries", in IET Information Security, Vol. 13, No. 5, pp. 435-447, 9 2019, doi: 10.1049/iet- ifs.2018.5141.
13. W. Zhang, B. Zhang, Y. Zhou, H. He and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks", in IEEE Internet of Things Journal, Vol. 7, No. 5, pp. 3991-3999, May 2020, doi: 10.1109/JIOT.2019.2956173.
14. Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M. "Studies on cloud-based cyber incidents detection and identification in critical infrastructure", CEUR Workshop Proceedings, 2021, Vol. 2923, pp. 68-80.
15. Gnatyuk S., Berdibayev R., Smirnova T., Avkurova Z., Iavich M. "Cloud-Based Cyber Incidents Response System and Software Tools", Communications in Computer and Information Science, Vol. 1486, pp. 169-184, 2021.
16. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
17. Iavich M., Gnatyuk S., Odarchenko R., Bocu R., Simonov S. (2021) The Novel System of Attacks Detection in 5G. In: Barolli L., Woungang I., Enokido T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 226. Springer, Cham. https://doi.org/10.1007/978-3-030-75075-6_47

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 59-63 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE GLOBAL CYBERSECURITY INDEX (GCI) ACCORDING TO A RECENT STUDY

Tinatin Mshvidobadze Professor Gori State University (Georgia)

ABSTRACT: The paper illustrates and analyzes the data of the International Telecommunication Union (ITU) survey on the Global Cyber Security Index. The model of the new concept of information security is offered. It is described and analyzed in the paper how countries can consider the use of the ITU Guide to Developing a National Cybersecurity Strategy as a toolkit to support the creation or enhancement of their national strategy. The comparison of global IDI and GCI ranking by different countries is also offered in the paper.

KEYWORDS: *Information society, Development Index, Cybersecurity, GCI.*

The ICT Development Index

Society is challenged by the information cyber threats such as denial of e-services, data integrity breaches, and data confidentiality breaches, and the effectiveness of the Internet is linked to cybersecurity as more countries are advancing in the use of ICTs.

In such ~~a~~ situation, an advanced protection solution is needed. Not long ago, vendors introduced a new platform that will facilitate the identification, analysis of incidents and helped block to attack. The concept will allow information security specialists to see the entire spectrum of threats, even events that were not included in the field of view of security experts.

XDR (Extended Detection and Response) - advanced detection, responses the threats of complex levels and targeted attacks. The system is aimed at working not only with endpoints, but also focuses on the analysis of network traffic, e-mail, cloud complex of structures.

The innovative new XDR concept continues to evolve gradually to provide comprehensive information security. The platform quickly processes a huge array of logs, responds quickly and in a timely manner to incidents. XDR can also be combined with SIEM / SOAR work models to speed up incident handling.

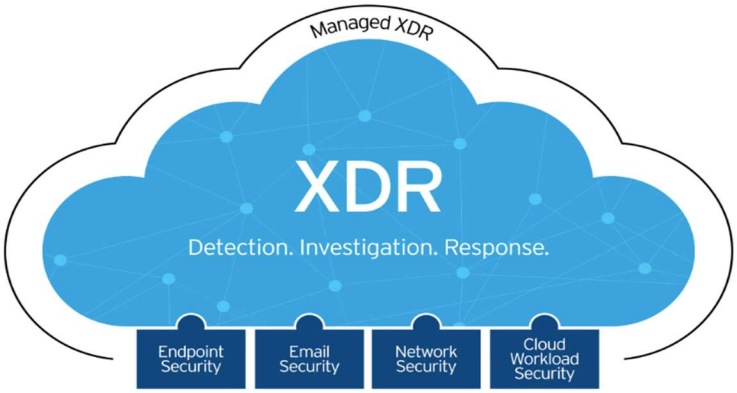

Fig.1. system XDR

The ICT Development Index (IDI) has been produced and published annually by International Telecommunication Union (ITU) since 2009. It is a composite index that combines 11 indicators into one benchmark measure. It is used to monitor and compare developments in the information and communication technology (ICT) between countries and over time. The report features key ICT data and a benchmarking tool to measure the information society, the ICT Development Index (IDI).[1]

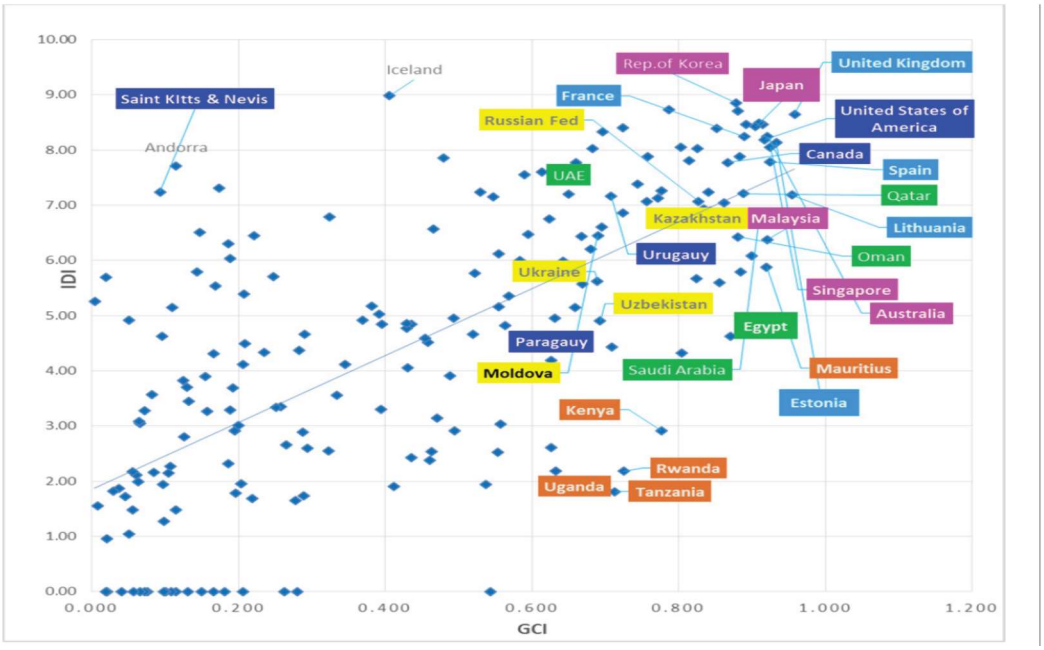

Fig.2. Comparison of global IDI and GCI ranking

[1] https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

Figure 2 shows that not all countries with high IDI scores have a similarly high score in GCI, for instance Iceland took the top place in IDI scoring 8.98 while only 0.406 in the GCI. Andorra, and Saint Kitts and Nevis, also score high in IDI and yet very low in GCI, although some countries are maintaining their leading positions in both indices.

Global Cyber Security Index (GCI) According to a 2020 study

Japan – The Japan National center of Incident readiness and Strategy for Cybersecurity (NICS) is building an information sharing system among public-private sectors[2]. The Japan National Institute of Information and Communication-Technology has established a National Cyber Training Center that has developed many projects, such as CYDER, CYBER COLOSSEO and Sec Hack 365 (a security innovator training program for young talents).

Lithuania - To consolidate functions and resources, which were previously scattered among various institutions into single entity, the National Cyber Security Centre (NCSC)[3] has been created. Consolidation has helped to concentrate best expertise and avoid not always efficient inter-institutional interaction issues, thus enabling faster decision-making and response time. The National Cyber.

Malaysia - Best practice guidelines have been developed for security services and cloud security practice in collaboration with the industry [1]. A cloud security practice document is being prepared to establish a cloud security certification scheme. An Internet Banking Task Force, consisting of local financial institutions, the Malaysian Communications and Multimedia Commission (MCMC), Cybersecurity Malaysia, and the Royal Malaysian Police, is being established to combat online banking fraud [4].

According a framework of Information Security Management System (ISMS) The Digital Forensics Working Group, comprising all law enforcement agencies that operate digital forensic laboratories, is being created. [2]

Singapore – The public and private sectors in Singapore have worked together to develop or adopt new cybersecurity standards to address gaps in cybersecurity standards. According to Irene Tham this new standard caters for different levels of security, depending on the level that service providers can offer to their users. The Singapore Standards Council has also embarked on the development of new standards that are currently not available at the international level. These include cybersecurity standards for autonomous vehicles and general requirements for IoT security for smart nation projects in Singapore [3].

[2] https:// www .nisc .go .jp/ eng/

[3] https://www.nksc.lt/en/

[4] https://www.cybersecurity.my/data/content_files/11/1170.pdf?.diff=1375349394

United Kingdom – The NCSC Active Cyber Defense Program aspires to protect the majority of people in the United Kingdom. Four initial measures have already had a significant impact: blocking fake emails; stopping systems veering into malicious websites; helping organizations easily fix website problems; phishing and malware mitigation. The program is expected to continue to drive change over the next two to five years. The NCSC launched Active Cyber Defense, which has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour. There has been a 43 percent increase in visits to the Cyber Security Information Sharing Partnership (CiSP), which allows the community to share information about cyber threats.[5]

Ukraine – The CERT-UA[6] team is constantly taking steps to engage with other Member State CERT teams, as well as with the Cisco Talos Intelligence Group on issues related to overcoming the effects of cyber-attacks on critical information infrastructure and identifying the causes and circumstances of cyber incidents.

Moldova – In the context of the development of information society aspirations, the Government of the Republic of Moldova approved a strategic and legislative framework for the development of the ICT domain in Moldova, the most important being the National Strategy for Information Society Development "Digital Moldova 2020" [4].

Georgia started a cyber research project in 2018, a Portal of Online Cyber exercises[7]. Cyber Lab – a new online resource created by Computer Emergency Response Team (CERT.GOV.GE) and Georgian Research and Educational Networking Association (GRENA) with the support of EU funded EaP- Connect project. The portal helps IT students from educational institutions interested in cybersecurity to deepen their practical skills, so they can better discover and then respond to cyber incidents. The portal will also help IT personnel from both the public and private sectors, where readiness is critically important to defend against attack, ensure cyber sustainability, and improve skills[5].

CONCLUSION

Measuring progress towards the cybersecurity commitment of countries globally is a complex task which entails striking a balance between different dimensions of cybersecurity experiences in different countries.

[5] https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

[6] https:// cert .gov .ua/

[7] www .cyberlab .tech

The GCI originally succeeded in measuring commitment to cybersecurity and generated interest on cybersecurity assessment among countries.

The GCI continues to contribute to the cybersecurity awareness in the least developed countries providing capacity building activities through the production of guidelines on cybersecurity legislation, regulation and technology, asserting the need and importance for countries to establish national computer incident response teams (CIRTs) and providing fundamental tools to develop a national cybersecurity strategies.

REFERENCES:

1. ISO/IEC DIS 27001:2018, Information technology - Security techniques - Information security management systems – Requirements;

2. ISO/IEC DIS 27002:2018, Information technology - Security techniques - Code of practice for information security controls;

3. Irene Tham, Campaign to ready public servants for Internet separation, https://www.straitstimes.com/singapore/campaign-to-ready-public-servants-for-internet-separation%20;

4.О Национальной стратегии развития информационного общества «Цифровая Молдова 2020», ПОСТАНОВЛЕНИЕ Nr. 857, http://lex.justice.md/viewdoc.php?action=view&view=doc&id=350246&lang=2

5. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019

Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 64-71 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ПОКАЗАТЕЛИ И МАТЕМАТИЧЕСКИЕ КРИТЕРИИ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

INDICATORS AND MATHEMATICAL CRITERIA FOR EVALUATING THE EFFECTIVENESS OF THE INFORMATION SECURITY SYSTEM AND CYBERSECURITY OF THE OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

к.т.н., Козубцова Леся Михайловна,Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, Lesya Kozbtsova,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., Гуда Оксана Викторовна,Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Technical Sciences, Oksana, Guda Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Крадинова Татьяна Адамовна,Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Technical Sciences, Tatyana Kradinova, Lutsk National Technical University, Lutsk, Ukraine
Палагута Анастасия Михайловна Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Palaguta Anastasia Military Institute of Telecommunications and Informatization named after Heroes of Krut, Kiev, Ukraine
д.п.н., к.т.н., профессор РАЕ Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Candidate of Engineering Sciences, Professor of RAE, Igor Kozubtsov, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

АННОТАЦИЯ. Каждого руководителя (распорядителя) объекта критической информационной инфраструктуры интересует ответ на вопрос как оценить эффективность функционирования систему защиты информации и кибербезопасности. Актуальность темы исследований обусловлено отсутствием показателей и математических критериев оценивания эффективности функционирования объектов критической информационной инфраструктуры. **Основные аспекты работы.** Для однозначного ответа на вопрос, как и чем оценить эффективность функционирования системы защиты информации и кибербезопасности в статье продолжены показатели и математические критерии эффективности. **Научная новизна.** Научная новизна полученного результата заключается в том, что предложены показатели и определены математические критерии возможной оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА: *показатель, критерий эффективности, функционирование, система, защита информации, кибербезопасность, объект критической информационной инфраструктуры.*

ABSTRACT. Each manager (manager) of a critical information infrastructure facility is interested in the answer to the question of how to evaluate the effectiveness of the information security and cybersecurity system. The relevance of the research topic is due to the lack of indicators and mathematical criteria for evaluating the effectiveness of the functioning of critical information infrastructure facilities. The main aspects of the work. For an unambiguous answer to the question of how and how to evaluate the effectiveness of the functioning of the information security and

cybersecurity system, the article considers the indicators and mathematical criteria of effectiveness. Scientific novelty. The scientific novelty of the obtained result lies in the fact that indicators are proposed and mathematical criteria for possible evaluation of the effectiveness of the information security system and cybersecurity of critical information infrastructure objects are determined.

KEYWORDS: *indicator, efficiency criterion, functioning, system, information protection, cybersecurity, object of critical information infrastructure.*

ВВЕДЕНИЕ

Система защиты информации и кибербезопасности (СЗИКБ) – это сложный комплекс программных, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности. Так как система «Система защиты информации и кибербезопасности» является относительно новой, то для нее еще неразработанное метрологическое обеспечения. Тем не менее каждого руководителя объекта критической информационной инфраструктуры (ОКИИ) интересует ответа на вопрос, в какой степени его настроенная система защиты информации и кибербезопасности ОКИИ обеспечивает необходимый уровень кибербезопасности. Ответом на этот вопрос может служить результат оценивания эффективности системы защиты информации и кибербезопасности по частичным показателям, которые носят вероятностный характер. Эффективность системы – это свойство системы, характеризующее ее способность выполнять свою целевую функцию в заданиях условиях. То есть под эффективностью системы понимают степень достижения цели этой системой. Тогда применительно к нашей системы под эффективностью системы защиты информации и кибербезопасности ($E_{СЗИКБ}$) будем понимать степень соответствия достигнутых результатов поставленным целям по защите информации.

Для осуществления оценки эффективности функциональной способности системы защиты информации и кибербезопасности ОКИИ необходимо наличие методики проведения, совокупность показателей оценивания и критерий оценки – признаков, основание принятия решения относительно оценки эффективности на соответствие предъявленным требованиям.

В связи с отсутствием для нового объекта исследования показателей и критерий оценивания в данном исследовании возникает необходимость в решении новой научной задачи. Сформулируем ее в следующей постановке. Необходимо изучить подходы и показатели, их математические модели, позволяющие оценить эффективности функционирования системы защиты информации и кибербезопасности.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Анализ последних исследований и публикаций для целостности проведем в основной части нашего исследования.

Решение вопроса по выбору критериев оценки эффективности функционирования любой системы защиты по показателю максимального эффекта предложено в работе [1]. Расчет осуществляется по формуле (1):

$$E = Эф/В \quad (1)$$

где Е – под эффективностью понимают степень достижения цели этой системой;

Эф – эффект, который достигается при внедрении данной системы;

В – расходы, совокупные расходы на приобретение, установку и конфигурирование, сопровождение и поддержку, а также затраты связанные с простоем оборудования вовремя техническое обслуживание или устранение неисправностей системы.

Однако ввиду специфики использования СЗИКБ определить прямой эффект от их внедрения (в временных или финансовых этого возникает задача выбора метода оценки, все множество показателях) трудно. Применение данного подхода требует наличия методики расчета стоимости потери информационных активов, без которых невозможно осуществлять расчет эффективности функционирования системы защиты информации и кибербезопасности.

Подход к оценке эффективности функционирования системы защиты информации и кибербезопасности в информационно-телекоммуникационных системах по показателю предотвращения потерь. Расходы на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной

безопасности организации.

Предложенный метод оценки экономической эффективности подразделения по защите информации [2] не совсем решает поставленную задачу. Для расчета показателя эффективности по результату внедрения и проведения мероприятий по обеспечению информационной и кибербезопасности необходимо иметь значение предотвращенных потерь (ЗВ). Он рассчитываются исходя из вероятности возникновения инцидента информационной и кибербезопасности и возможных экономических потерь от него до и после реализации мероприятий по обеспечению кибербезопасности. Применение данного подхода затруднено вследствие отсутствия подходов к расчету В1 и В2.

Изложенный в работе [3] подход к оценке эффективности мероприятий информационной безопасности в условиях неопределенности позволяет продолжить поиск в этом направлении и предложить еще другие показатели, которые могут охарактеризовать эффективности функциональной способности системы защиты информации и кибербезопасности ОКИИ.

ЦЕЛЬ СТАТЬИ

Рассмотреть показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности ОКИИ.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Прежде чем выбрать возможные показатели и математические критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объекта критической информационной инфраструктуры, рассмотрим некоторые определения.

Средство криптографической защиты информации – программный, аппаратно-программный и аппаратный средство, предназначенное для криптографической защиты информации.

Средства технической защиты информации – программный, аппаратно-программный и аппаратный инструмент, предназначенный для технической защиты информации и имеет соответствующее экспертное заключение.

Средство кибернетической защиты информации – программный, аппаратно-программный и аппаратный средство, предназначенное для киберзащиты информации.

Показатель эффективности – это величина, характеризующая степень достижения системой любой из поставленных перед ней задач.

Требования к показателю эффективности: иметь определенный физический смысл; быть пригодным для количественного анализа; иметь простую и удобную форму; отражать одну из значимых сторон функционирования системы; обеспечивать необходимую чувствительность.

Единичные (частные) показатели эффективности, отражают какую-то из значимых сторон функционирования системы (вероятность обнаружения нарушителя или вероятность его нейтрализации силами охраны и т.п.);

Комплексные (обобщенные) показатели эффективности, представляют собой комбинацию частичных показателей.

Согласно этого определения предложим следующие частные показатели эффективности, как числовые величины, которые будут характеризовать степень достижения системой защиты информации и кибербезопасности поставленных перед ней задач:

киберзащищенность ($P_{КЗ}$). Киберзащищенность – способность системы связи выполнять задачи по назначению в условиях программно-математических воздействий противника, то есть вероятность того, что эта система будет защищенной от кибернетического вмешательства;

коэффициент укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты ($K_{УС}$). Показатель укомплектованность средствами криптографической защиты информации, технической защиты информации и киберзащиты характеризуется соотношением штатных и в наличии средств криптографической защиты информации, технической защиты информации и киберзащиты. Показатель рассчитывается отдельно по средствам криптографической защиты информации, технической защиты информации и киберзащиты;

коэффициент технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты ($K_{ТГС}$). Коэффициент технической готовности – отношение количества технически исправных средств криптографической защиты информации, технической защиты информации и киберзащиты к фактически имеющаяся в

наличии. Характеризует готовность средств к применению по назначению и показывает, насколько хорошо поддерживается техническое состояние средств криптографической защиты информации, технической защиты информации и киберзащиты на ОКИИ.

коэффициент укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты ($К_{УИС}$). Коэффициент технической готовности – отношение количества технически исправных средств криптографической защиты информации, технической защиты информации и киберзащиты к их списочному количеству. Характеризует готовность средств к применению по назначению и показывает, насколько хорошо поддерживается техническое состояние средств криптографической защиты информации, технической защиты информации и киберзащиты на ОКИИ;

коэффициент укомплектованности штатных должностей системными администраторами ($К_{СА}$). Показатель укомплектованность штатных должностей системными администраторами характеризуется соотношением штатных и к занятым должностям;

коэффициент укомплектованности штатных должностей обслуживающим персоналом ($К_{СА}$). Показатель укомплектованность штатных должностей обслуживающим персоналом характеризуется соотношением штатных и к занятым должностям;

киберзащищенность по результатам penetration testing($P_{КЗ}^{РТ}(S)$). Реальное значение киберзащищенность ОКИИ по результатам активного тестирования.

Математическая модель расчета эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ по показателю киберзащищённости. Под киберзащищённостью будем понимать способность системы выполнять задачи по назначению в условиях программно-математических воздействий [1].

Для реализации на практике оценивания эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по показателю киберзащищённости рекомендуется применить методику, изложенную в работе [4; 5] адаптировав ее для решения новой задачи.

Киберзащищенность в первом приближении может служить ярким индикатором эффективности функционирования системы защиты информации и кибербезопасности ОКИИ (2):

$$E_{СЗIКБ} \approx P_{КЗ} \quad (2)$$

Расчет коэффициента укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты предлагается осуществляется по формуле (3):

$$К_{УС} = \frac{Ф_С}{Ш_С} \quad (3)$$

где $К_{УС}$ – коэффициент укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты;

$Ш_С$ – штатная численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_С$ – фактически имеющаяся численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

Оценивания способности укомплектованности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 1.

Таблица 1. *Критерии оценивания способности укомплектованности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности средствами				
	$0 \le К_{УС} \le 0{,}25$	$0{,}25 < К_{УС} \le 0{,}5$	$0{,}5 < К_{УС} \le 0{,}75$	$0{,}75 < К_{УС} \le 0{,}9$	$0{,}9 < К_{УС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0{,}25$	ОН	ОН	ОН	ОН	ОН
$0{,}25 < Э_{СЗИКБ} \le 0{,}5$	Н	Н	Н	Н	Н
$0{,}5 < Э_{СЗИКБ} \le 0{,}75$	С	С	С	С	С
$0{,}75 < Э_{СЗИКБ} \le 0{,}9$	С	С	С	В	В
$0{,}9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты осуществляется по формуле (4):

$$К_{ТГС} = \frac{Ф_{ИС}}{Ф_{С}}. \quad (4)$$

где $К_{ТГС}$ – коэффициента технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{ИС}$ – количество исправных средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{С}$ – фактически имеющаяся численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

Оценивания способности технической готовности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 2.

Таблица 2. *Критерии оценивания технической готовности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент технической готовности средств				
	$0 \le K_{ТГС} \le 0,25$	$0,25 < K_{ТГС} \le 0,5$	$0,5 < K_{ТГС} \le 0,75$	$0,75 < K_{ТГС} \le 0,9$	$0,9 < K_{ТГС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты осуществляется по формуле (5):

$$К_{УИС} = К_{УС} \times К_{ТГС} = \frac{Ф_{ИС}}{Ш_{С}} \quad (5)$$

где $К_{УИС}$ – коэффициента укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты;

$К_{УС}$ – коэффициента укомплектованности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$К_{ТГС}$ – коэффициента технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{ИС}$ – количество исправных средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ш_{С}$ – штатная численность средств криптографической защиты информации, технической защиты информации и киберзащиты.

Оценивания способности укомплектованности исправными средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 3.

Таблица 3. *Критерии оценивания укомплектованности исправными средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности исправными средствами				
	$0 \le K_{УИС} \le 0,25$	$0,25 < K_{УИС} \le 0,5$	$0,5 < K_{УИС} \le 0,75$	$0,75 < K_{УИС} \le 0,9$	$0,9 < K_{УИС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности штатных должностей системными администраторами системы защиты информации и кибербезопасности ОКИИ осуществляется по формуле (6):

$$К_{СА} = \frac{Ф_{СА}}{Ш_{СА}} \quad (6)$$

где $К_{СА}$ – коэффициент укомплектованности штатных должностей системными администраторами системы защиты информации и кибербезопасности ОКИИ;

$Ш_{СА}$ – штатная численность должностей системных администраторов системы защиты информации и кибербезопасности ОКИИ;

$Ф_{СА}$ – фактически имеющаяся численность системных администраторов системы защиты информации и кибербезопасности ОКИИ.

Оценивания способности укомплектованности штатных должностей системными администраторами оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 4.

Таблица 4. *Критерии оценивания способности укомплектованными штатными должностей системными администраторами критически оказывать влияние на* $Э_{СЗИКБ}$

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности штатных должностей системными администраторами				
	$0 \le К_{СА} \le 0,25$	$0,25 < К_{СА} \le 0,5$	$0,5 < К_{СА} \le 0,75$	$0,75 < К_{СА} \le 0,9$	$0,9 < К_{СА} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности штатных должностей обслуживающим персоналом системы защиты информации и кибербезопасности ОКИИ осуществляется по формуле (7):

$$К_{ОП} = \frac{Ф_{ОП}}{Ш_{ОП}} \quad (7)$$

где $К_{ОП}$ – коэффициент укомплектованности штатных должностей обслуживающим персоналом системы защиты информации и кибербезопасности ОКИИ;

$Ш_{ОП}$ – штатная численность должностей обслуживающего персонала системы защиты информации и кибербезопасности ОКИИ;

$Ф_{ОП}$ – фактически имеющаяся численность обслуживающего персонала системы защиты информации и кибербезопасности ОКИИ.

Оценивания способности укомплектованности штатных должностей обслуживающим персоналом оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 5.

Таблица 5. *Критерии оценивания способности укомплектованными штатными должностей обслуживающим персоналом критически оказывать влияние на* $Э_{СЗИКБ}$

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности штатных обслуживающим персоналом				
	$0 \le К_{ОП} \le 0,25$	$0,25 < К_{ОП} \le 0,5$	$0,5 < К_{ОП} \le 0,75$	$0,75 < К_{ОП} \le 0,9$	$0,9 < К_{ОП} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Математическая модель расчета эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по критерию выявленных активных угроз по результатам penetration testing. Данный подход видит цель контроль киберзащищённости средств и их

компонентов ОКИИ состоянию на момент времени $t_{ДИВ1}$ за условий действий тестовых деструктивных информационных влияний (ДИВ) ($F_{ДЕВ}$=1).

Если в ОКИИ есть средства (компонента) активного противодействия кибервлянию, то в таком случае исчисление $P_{КЗ}(S)$ осуществляется с использованием показателей удачных и неудачных попыток нарушения нормального функционирования указанного средства. Расчет киберзащищённости $P_{КЗ}(S)$ системы S осуществляется по формуле (8):

$$\mathrm{P}_{\mathrm{КЗ}}^{\mathrm{РТ}}(S) = 1 - \frac{N_{\mathrm{ДИВ}}^{\mathrm{Удачных}}(S)}{N_{\mathrm{ДИВ}}^{\mathrm{Общ}}(S)} \quad (8)$$

где $N_{\mathrm{ДИВ}}^{\mathrm{Общ}}(S)$ – общее количество проведенных ДИВ на всю систему S;

$N_{\mathrm{ДИВ}}^{\mathrm{Удачных}}(S)$ – количество удачных попыток реализации ДИВ на всю систему S по результатам оповещение системой фиксирования инцидентов.

Система S будет считается такой, что прошла проверку контроля на киберзащищённость, если по результатам расчета киберзащищённости по состоянию на время $t_{FДИВ1}$ при $F_{ДИВ}$ =1 удовлетворило критерии табл. 6.

Таблица 6. *Критерии оценки киберзащищённости ОКИИ по результатам penetration testing*

Критерий эффективности	Уровень	Лингвистическое описание уровня киберзащищённости
$0{,}9 < P_{КЗ}^{РТ}(S) \leq 1$	очень высокий	очень высокий уровень киберзащищённости, ДИВ практически никогда не будет проведена
$0{,}75 < P_{КЗ}^{РТ}(S) \leq 0{,}9$	высокий	высокий уровень киберзащищённости, вероятность проведения ДИВ достаточно низкая
$0{,}5 < P_{КЗ}^{РТ}(S) \leq 0{,}75$	средний	средний уровень киберзащищённости, вероятность проведения ДИВ средняя
$0{,}25 < P_{КЗ}^{РТ}(S) \leq 0{,}5$	низкий	низкий уровень киберзащищённости, вероятность проведения ДИВ скорее всего будет проведена
$0 \leq P_{КЗ}^{РТ}(S) \leq 0{,}25$	очень низкий	очень низкий уровень киберзащищённости, вероятность проведения ДИВ почти наверняка будет проведена

Обобщение результатов вычисления эффективности функционирования системы защиты информации и кибербезопасности.

Сводная таблица значений эффективности по критериям представлены в табл. 7.

Таблица 7. *Сводная таблица значений по показателям эффективности* $Э_{СЗИКБ}$

Обобщённый показатель эффективности $Э_{СЗИКБ}$	Частные показатели эффективности						
	$P_{КЗ}$	$K_{УС}$	$K_{ТГС}$	$K_{УИС}$	$K_{СА}$	$K_{ОП}$	$P_{КЗ}^{РТ}(S)$
очень низкий							
низкий							
средний							
высокий							
очень высокий							

Обобщённый показатель эффективности функционирования системы защиты информации и кибербезопасности ОКИИ предлагается определить, как средне арифметическую сумму частных показателей (9):

$$Э_{СЗИКБ} = \frac{P_{КЗ} + K_{УЗ} + K_{УИС} + K_{СА} + K_{ОП} + P_{КЗ}^{РТ}(S)}{7}. \quad (9)$$

Если по отдельному показателю не осуществлялось вычисление, то в расчётную формулу (9) не подставляются соответствующие значения, а в выводах указывается краткое обоснование почему не использовался показатель. Критерии оценки эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по обобщенном показателе представлены в табл. 8.

Таблица 8. *Критерии оценки эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по обобщенном показателю* $Э_{СЗИКБ}$

Критерий $Э_{СЗИКБ}$	Уровень	Лингвистическое описание	
$0 \le Э_{СЗИКБ} \le 0{,}25$	очень низкий	неудовлетворительный уровень эффективности	Утечка информации и кибернезахищена
$0{,}25 < Э_{СЗИКБ} \le 0{,}5$	низкий	низкий уровень эффективности	Создания условий для утечки информации и кибе рыску
$0{,}5 < Э_{СЗИКБ} \le 0{,}75$	средний	средний уровень эффективности	Обеспечения гарантированной защиты информации и кибербезопасности
$0{,}75 < Э_{СЗИКБ} \le 0{,}9$	высокий	в целом высокий уровень эффективности	
$0{,}9 < Э_{СЗИКБ} \le 1$	очень высокий	наивысший уровень эффективности	

ВЫВОДЫ

Безусловно количественная оценка эффективности функционирования системы защиты информации и кибербезопасности ОКИИ требует больших усилий, чем использование качественных методов. Однако и отдача прежде всего экономически, будет гораздо весомее, а интересы, как заказчика и разработчика системы защиты информации и кибербезопасности ОКИИ, будут заниженными более надежно.

Учитывая выше подходов и критериев на современном этапе развития видится рациональным применять не все, а наиболее показательные подходы, которые позволяют наглядно продемонстрировать эффективности функционирования системы защиты информации и кибербезопасности ОКИИ.

НАУЧНАЯ НОВИЗНА

Научная новизна полученного результата заключается в том, что предложено показатели и математические критерии возможной оценки эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Представленное исследование не исчерпывает всех аспектов обозначенной проблемы. Теоретические и практические результаты, полученные в процессе научного поиска, составляют основу для дальнейшего обоснования методики оценки эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Искусственный интеллект. 2008. № 4.С. 253 – 264.
2. Андреев К. Метод оценки экономической эффективности подразделения по защите информации // Информационная безопасность. 2010. № 5. URL: http://www.itsec.ru/ articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 7.12.2021).
3. Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Бизнес-информатика. 2015. №1(31). С. 51–57.
4. Zabara S., Kozubtsova L., Kozubtsov I. Improved method of diagnostics of cyber security of the information system taking into account disruptive cyber impacts // «Danish Scientific Journal» (DSJ). Kobenhavn. Denmark. 2020. Vol. 35(1). Pp. 68 – 74. ISSN 3375-2389.
5. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2020. Випуск № 39. С. 127 – 135.