Vol. 1, No. 2, 2016

SECURITY OF CYBER-PHYSICAL SYSTEMS FROM CONCEPT TO COMPLEX INFORMATION SECURITY SYSTEM

Valerii Dudykevych, Galyna Mykytyn, Taras Kret, Andrii Rebets

Lviv Polytechnic National University, 12, Bandera str., Lviv, 79013, Ukraine
Author e-mail: *cosmos-zirka@ukr.net*

Submitted on 02.11.2016

Abstract: **A conception of multilevel complex security system (CSS) of cyber-physical systems (CPS) was developed; dimensional model of information-technology state (ITS) was proposed; informational model of CSS cyber-physical system "iPhone – Wi-Fi, Bluetooth – sensors" was created; software of symmetric block data encryption of "Kalyna" algorithm was realized.**

Index Terms: **block encryption algorithm "Kalyna", complex security system, concept, cyber-physical system, information, information technical state, model.**

I. INTRODUCTION

Ukrainian cyber-physical security strategy is focused on development of approaches to ensuring cyber-physical security of informational infrastructure objects of society through the complex of organizational, regulatory and legal, military, operational, technical measures and appropriate mechanisms, which are agreed with priorities of Ukrainian national security strategy, Doctrine vectors of Ukrainian information security and European institution, in particular such as European Union Agency for Network and Information Security (ENISA), which provides recommendation for development of pan-European cyber security and national cyber security strategies, researching of safe use of cloud technology, resolving of data protection issues, increasing of privacy in modern technologies and detection of cyber threats [1], [2].

Cyber-physical systems are leading in the segment of new technologies developing and applying in different subject areas in the context of effective execution of computational tasks by interaction with the physical space and making decision on the management objects and processes. The main components of CPS are divided in cybernetic space (CS), communication environment (CE), and physical space (PS), which causes their multilevelness and requires ensuring of safe information interaction between components of CPS for execution of functional tasks with data: control/handling – transmission/ receiving – control. As the part of Ukrainian cyber-physical space cyber-physical systems must be safe in their functioning and protected from cyber-physical threats. In Ukraine in this direction exists the standard ISO/IEC 15408 [3], which is focused on security structure "threats – services – mechanisms" through interconnection of profiles (tasks) of information and communication systems security: confidentiality, integrity, availability, observation, guarantees.

In the context of unification of multilevel interaction CPS component and unification of interaction one level component, relevant is a level integration [4] through communication environment which is based on principles of cloud technology, which can be the reason for effective resolution of applied problems in the plane of functional and information security.

Formulation of the problem: to develop the building concept of complex security system (CSS) CPS in the context of level integration and creation of model of information –technology state of CPS in functional space which enables building of CSS for cyber-physical system with any configuration by universal structure of integration levels "CS – CE – PS", according to the threats within the ensuring of dependability.

Purpose: development of CSS for cyber-physical system "iPhone – Wi-Fi, Bluetooth – sensors" according to space model of information-technology sate and conception of ensuring multi-information security of CPS; creation of algorithmic software for ensuring of data cryptographic protection in communication environment CPS based on block algorithm encryption.

II. THE CONCEPT OF CONSTRUCTION A MULTILEVEL SECURITY OF CYBER-PHYSICAL SYSTEMS

The concept of creating a multilevel CPS is shown in Fig. 1. Concept has the following structure: classification of threats/attack – forming of protection criteria – creation of multilevel CSS CPS – determination of security policy model – selection of methods for evaluation a protection state of CPS. Classification of threats/attacks: threats by the features; attacks by the end result, by the way of implementation; method of STRIDE threats classification by categories (substitution of the objects, data modification, authorship denial, information disclosure, service denial, privileges increasing) – creation of threats model "information/CPS – sources of threats – ways of threats realisation". Criteria of information security in CPS: architecture of confidentiality, integrity, availability, observability, guarantees. Formulation of security tasks is aimed at countering security threats and compliance security policy in area of information and communication systems through the development of complex information security system, which works on identifying detection, blocking and neutralizing the information threats.

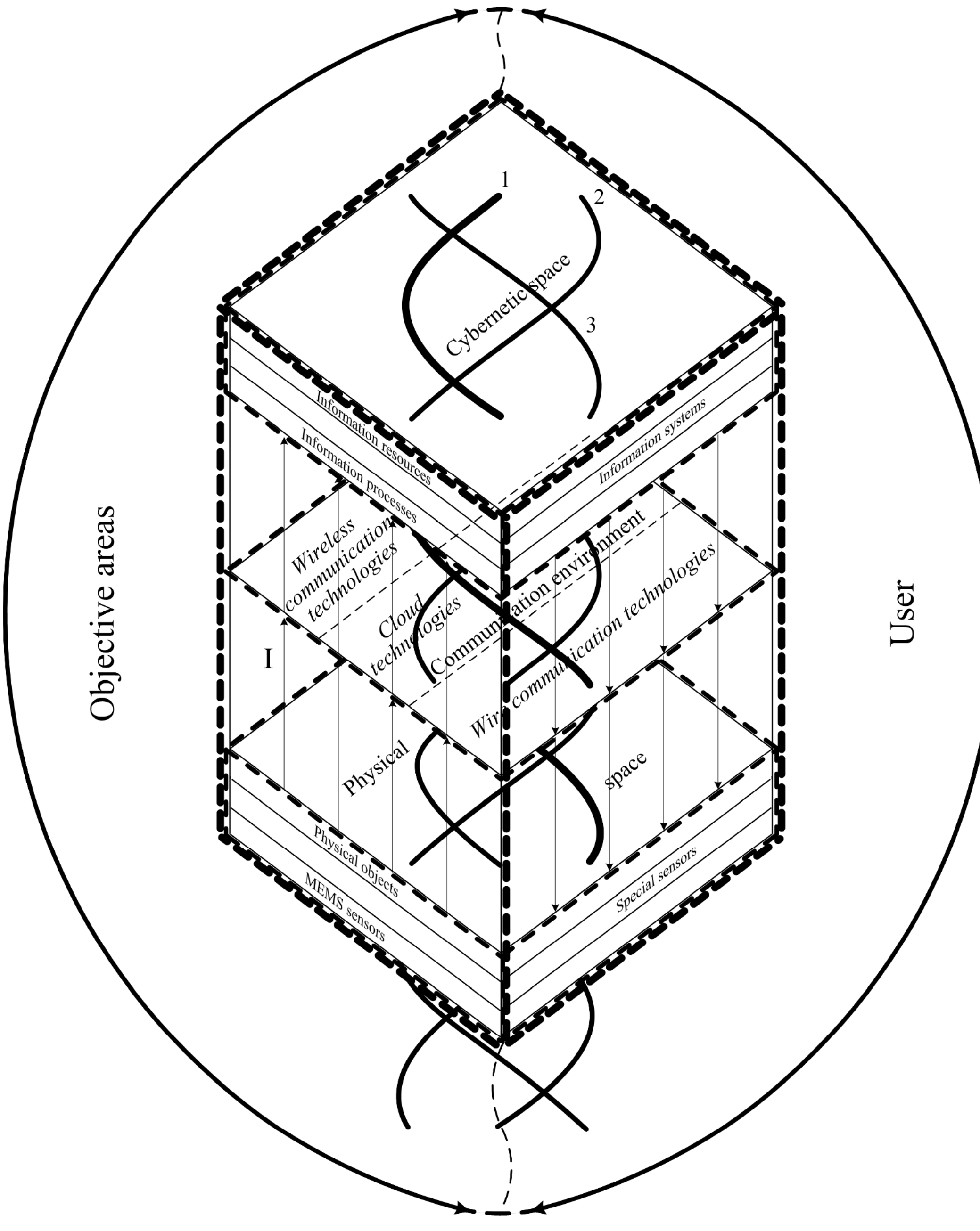


Fig. 1. The structure of the construction concept CSS of cyber-physical system in the context of integration levels
I ——► – information (selection, control); ▬ ▬ ▬ – CSS CS, CE, PS; ▬▬▬ – CSS CPS; 1.2.3 – threats for CS, CE, PS

Ensuring systems, data and resources availability: user (subject, process) has appropriate rights, may use a resource according to the rules, which are established by security policy, without waiting longer than a given period of time. Availability is aimed at maintaining the system in working condition, what provides timely and accurate functioning of mechanisms through rejection: intentional / unintentional threats, unauthorized data removal, unjustified refusal of access to the service, attempts to use the system and the data in forbidden purposes.

Integrity ensuring: data which can't be modified by unauthorized user / process during their storage, transmission and processing; system, in which any component can't be deleted, modified / added in bypass or violating a security policy.

Ensuring of data privacy and system information: is that information cannot be obtained by unauthorized users during its storage, processing and transmission.

Observability ensuring: is focused on implementing a system capabilities to register any user / processes activities, using a passive objects and identifiers installation, which are involved in certain users / processes events in order to deviate a security policy violations and be realized through: involvement mechanisms, coercion methods, faults isolation, intrusions detection, actions recovery, etc.

Guarantees ensuring, as the set of requirements, which constitute some assessment scale to determine the measure of confidence in the implementation; organizational and technical measures; protection against intentional errors of users /software; sufficient stability to intentional incursion and using of detours.

The basis for construction of multi-level CSS CPS is guidelines for the development of technical specifications for CSS creation, which is justifying the requirements to CSS in relevant protection segments against unauthorized access and guarantee. The Privacy Policy for CPS is based on models and selection criteria. In order to evaluate the level of CPS safety is used the standardized methods of dependability ensuring.

III. MODEL OF CYBER-PHYSICAL SYSTEM INFORMATION TECHNICAL STATE

Model of CPS information technical state (ITS) in functional-information space "C/P – TRSM/RCVN – M": "information selection I_S – data – information management I_M" according to dependability structure by the standard СОУ-Н НКАУ 0060:2010 [5] (Fig. 2).

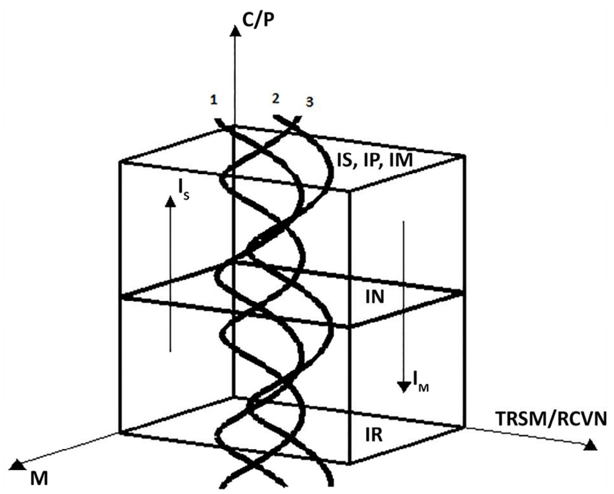


Fig. 2. Space model of information technical states in dependability context: a) functional (safe) status – NORMA

Informational and technical state of the system – is a set of properties and features as both technical and information character about the suitability of the system at a particular time. System states that are caused by influence of threats – development defects (DD), physical defects (PD) and external influences / interactions defects (ID) are classified as: a) functional (safe), b) partially functional (safe), c) incapacitated (safe), d) incapacitated (unsafe). According to conception "object – threat – protection" information is a protection object and circulates in CPS, which is presented as an universal structure – Information Systems (IS), Information Processes (IP) information management (IM), information networks (IN), Information Resources (IR). Complex of threats (1 – 2 – 3) is relevant to the influence of destabilizing factors DD, PD and ID on multilevel structure of CPS. Model (a) is basic for other models forming, what interprets ITS as: b) partially functional (safe) state – ALARM-1; c) non-functional (safe) state ALARM-2; d) non-functional (unsafe) state – AVARIA. New informational technical states (b-d) get movements of CPS universal structure anticlockwise in functional space "C/P – TRSM/RCVN – M" (Fig. 2).

It gives a reason to develop a complex system security model of CPS according to method, threats model and offender model.

IV. INFORMATION MODEL OF COMPLEX SECURITY SYSTEM OF CFS "IPHONE – WI-FI, BLUETOOTH – SENSORS"

To ensure confidentiality, integrity, availability, observability and safety of CPS data and components, let's consider a complex security system, which is formed on the basis of the construction of multilevel CSS CPS concept and allows to implement a secure process, transmission and storage of information and, accordingly, safely functioning of CPS. In structure of this CSS – protection subsystem CPS – complex security system CS, CE and PE.

Complex security system of CPS is designed based on: system approach (principle and hierarchy, structuring, integrity) and synergetic approach (property of emergency, which presupposes the existence of properties, which are typically for complex security system of CPS in general, but not inherent to its individual elements – complex security systems of CS, CE, PS).

Fig. 3 shows the model CSS of cyber-physical system "iPhone – Wi-Fi, Bluetooth – sensors". The central segments of the model are structure elements of CPS: cyber-physical space – smartphone iPhone; communication environment – Wireless communication technology Wi-Fi, Bluetooth; physical space – MEMC-sensors. The top segment is presented by threats classes using the STRIDE method, which are typically for CPS elements: CS, CE – S (object substitution), R (authorship denial), I (information disclosure), D (service denial), E (privileges increasing); PS – T, D. The lower segment of the model is CSS of cyber-physical system, which consists of subsystems – complex security systems CE, CS and PS, is generated for security problems solving of appropriate CPS segments: CS, CS – ensuring of confidentiality (C), integrity (I), availability (A), observation (O), guarantees (G); PS – I, A, G. Solving of security problems provides relevant security services based on information security technology as structure "security problem – security service – the technology of information security".

Structure of CSS cybernetic space CPS – smartphone iPhone: K – authorization – Apple ID; C – integrity control – hashing SHA; D – communication safety – TLS, DLS; S – identification – Apple ID; G – containment – Secure Enclave

Structure of CSS communication space CPS – wireless communication technology: K – protected communications – encryption: "Kalyna"; C – integrity control – MIC; D – intrusion Detection – NAC; S – Audit – MFP; G – containment – Firewalling.

Structure of CSS physical space CPS – MEMC – sensors: C – restore safe state – noiseimmunity coding; D – access management – RAC; G – containment – RAC.

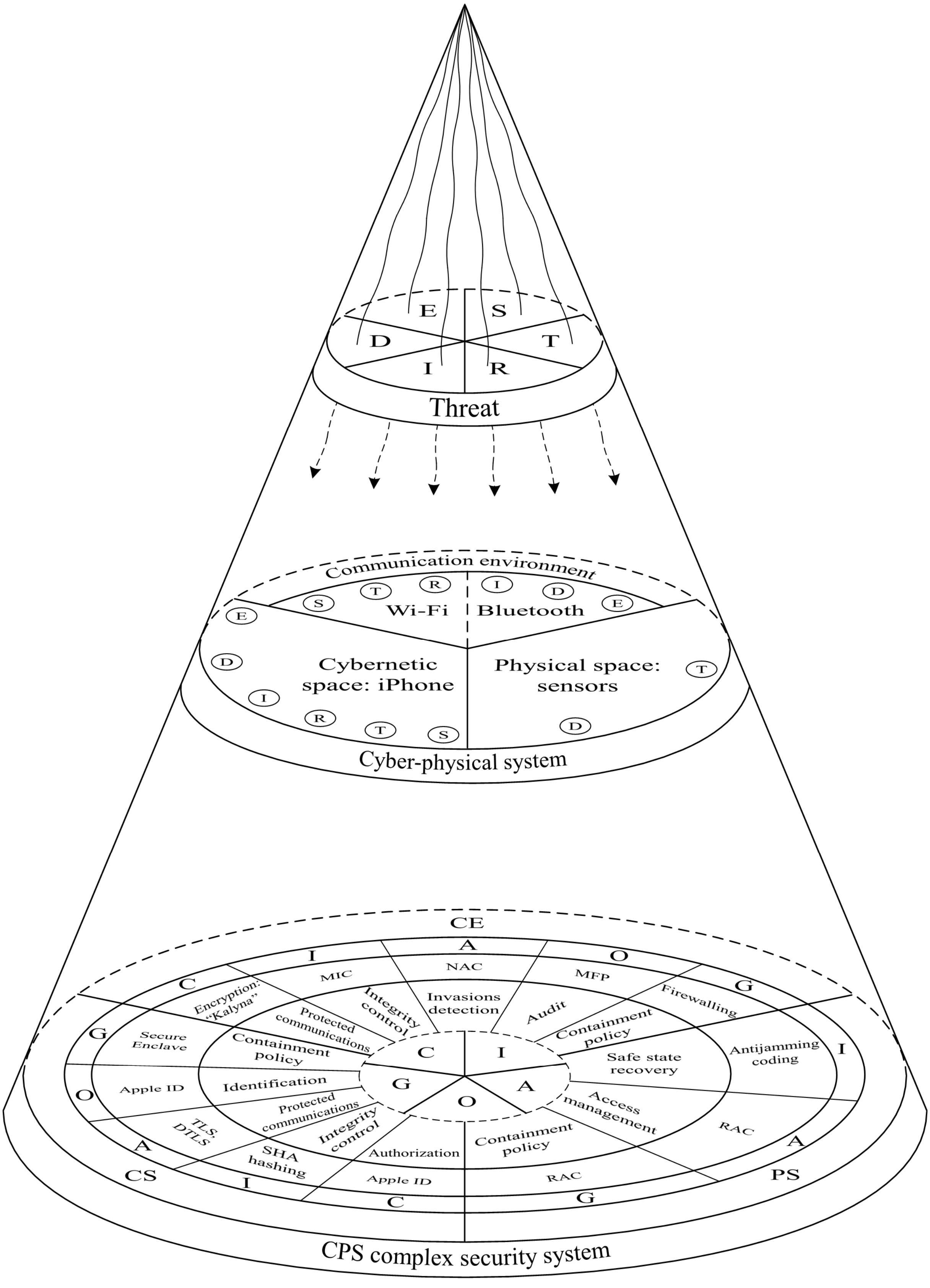


Fig. 3. Informational model of complex security system of CFS "iPhone – Wi-Fi, Bluetooth – Sensors"

A CPS complex security system was developed in context: structure CPS "iPhone – Wi-Fi, Bluetooth – sensors"; threats by the STRIDE method; protection technologies; protection profiles; regulatory support (table 1).

Table I

Complex Security System of CPS: Protection Technologies

CPS Structure		Threads: STRIDE method		Protection technologies	Protection profiles	Regulatory support
1		2		3	4	5
CS: iPhone		S	• social engineering; • substitution of signed firmware; • objects substitution	• program certification; • way of trusted device loading; • firmware SHSH certification	• Biometric Verification Mechanisms Protection Profile V1.3 (2008.11.07); • Protection Profile for Mobile Device: Fundamentals V2.0 (2014.09.17); • Application Soft-ware Protection Pro-file (ASPP) Extended Package: File	• NIST Special Publication 800-164. 2012. Guidelines on hardware-rooted security in mobile devices (draft); • NIST Special Publication 800-124. 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise; • Government Mobile
		T	• modification of access codes; • obtaining a full access to the file systems (Jailbreak); • unauthorized start of data destruction toll	• protection coding; • operation system certificates; • low-level encryption AES-256;		
		R	• replacement of digital certificates / signatures; • malicious software disguise; • unauthorized purchases through programs;	• technology of user actions fixing • parental control; • dactyloscopic sensor		
CS: iPhone		I	• unauthorized remote access; • social engineering; • unauthorized execution of software	• SSL / VPN; • remote locking of device • ARM's Execute Never	Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System V1.0 (2014.11.10); • Protection Profile for Software Full Disk Encryption V1.1 (2014.03.31)	and Wireless Security Baseline. 2013; • Mobile-Computing Device (MCD) Standards and Guidelines. A Mandatory Reference for ADS Chapter 545 2014
		D	• exploits on system kernel loader level (0x24000 Segment Overflow, usb_control_ msg(0xA1, 1) Exploit); • exploits on system kernel level (IOSurface Kernel Exploit); • unauthorized launch of device lock function	• certification Apple Root; • way of trusted device loading • Apple Sandbox		
		E	• social engineering; • substitution of digital certificates / signatures; • using of the operating system vulnerabilities	• periodic update of operating system and programs • file encryption (algorithm AES); • staged authentication		
CS:	Wi-Fi	S	• disguise as another node; • devices substitution (man-in-the-middle attack); • attacks on access passwords	• technology of authentication objects verifications; • hiding internal addresses (session gateway) • access restrictions technology	• Firewall Protection Profile V3.0 (2015.06.12); • Common Criteria Schutzprofil (Protec tion Profile). Schutzprofil 1: Anforderun-gen an den Netzkonnektor V3.2.1 (2015.04.28); • Protection Profile for IPsec Virtual Private Network (VPN) Clients V1.4 (2013.10.21)	• IEEE Std. 802.11; • ДСТУ ISO/IEC 7498-3:2004. Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing; • ISO/IEC 27033-3:2010. Information technology. Security techniques. Network security. Reference networking scenarios. Threats, design techniques and control issues; • ISO/IEC 27033-4:2014. Information technology. Security techniques. Network security
		T	• unauthorized configuration disguise; • unauthorized logs clearing; • unauthorized use of network resources	• restricting access to logs; • Remote storage of log-files; • user identification and authentication		
		R	• packet sniffing; • social engineering; • unauthorized collection of information about the network	• data encryption; • IPSEC; • VPN		
		I	• DoS\ DDoS attacks; • disabling of network elements; • obstructiveness	• packets filtering; • firewalling; • restricting access to network elements		
		D	• unauthorized access to equipment settings; • analysis of official administrative data; • unauthorized change / substitution of access permissions	• identification of sessions participants; • restricting access to equipment settings; • fixation of the settings change		
		E	• unauthorized configuration disguise; • unauthorized logs clearing; • unauthorized use of network resources	• restricting access to logs; • Remote storage of log-files; • user identification and authentication		

Continuation of Table

1	2	3	4	5	1	2
	Bluetooth	S	• devices substitution (man-in-the-middle attack); • user substitution; • interception of access codes	• equipment identification ; • authentication, user authorisation • encryption of access codes	• Certificate Issuing and Management Components Protection Profile V1.5 (2011.09.09); • Protection Profile for Network Devices V1.1 (2012.06.08); • Network Device Protection Profile (NDPP) Extended Package: SIP Server V1.1 (2014.11.05); • Common Criteria Protection Profile. Cryptographic Modules, Security Level “Low” V1.01b (2009.02.27)	• IEEE 802.15.1; • НД ТЗІ 2.5-004-99. Criteria for evaluating information security in computer systems from unauthorized access; • ДСТУ 3043-95 Information technology. Teleprocessing of data and computer networks. Terms and Definitions; • ISO/IEC 27033-5:2013. Information technology. Security techniques. Network security
		T	• unauthorized change of command; • misrepresentation; • errors in the data flow;	• hashing; • noiseimmunity coding; • preemulation		
		R	• disguise of unauthorized actions as an error; • unauthorized use of credentials • unauthorized use / change of services	• restricting access to credentials and services; • events registration; • user authentication		
		I	• interception of the data flow; • interception of access codes; • unauthorized access to account information	• data encryption; • One-time password authentication; • devices identification		
		D	• obstructiveness; • disabling of equipment;	• dynamic frequency change; • restrict access to equipment		
		E	• devices substitution (man-in-the-middle attack); • user substitution; • interception of access codes	• equipment identification ; • authentication, user authorisation • encryption of access codes		
PS: Sensors		T	• display modification	• mechanism of control measurements	• Intrusion Detection System Sensor Protection Profile V1.3 (2007.07.25)	• IEEE 2700-2014 Standard for Sensor Performance Parameter Definitions; • IEC 62047- Series. Part 1-22. Micro-Electromechanical Devices – MEMS
		D	• power outages; • exceeding of thresholds; • hardware failure	• duplication of sensor; • emergency disabling of sensor; • self-diagnosis		

To increase the resistance of cryptographic protection in CPS, it is proposed to use a blocking algorithm “Kalyna”, which can serve as a basis of adaptation encryption / decryption of data in wireless communication technology, which form a segment of CS in cyber-physical systems.

Algorithm “Kalyna” operates on the basis of variable block size and key length (128, 256, and 512). Code has SPN-structure (Rijndael-similar) with an increased size of the MDS matrix, a new set of four different S-blocks, before and after bleaching, using the sum by module 2^{64} and new construction of key schedule. Standard “Kalyna” ensures sufficient supply of reliability – 6, 7 and 9 cycles for 128, 256 and 512 bit block respectively by 10, 14 and 18 encryption cycles. For optimized versions of software implementation on 64-bit platforms algorithm shows higher performance than analogues: for 128-bit key – advantage 86-143 Mbit / s compared with AES; for 256-bit key – advantage 4 % compared with AES; performance at key size of 512 bits – at the level of 256-bit AES version. High reliability and performance of the block encryption algorithm “Kalyna” give reasons for its effective application in wireless communication technologies as part of cyber-physical system.

Let’s analyse operation of cryptographic transformation based on “Kalyna” algorithm by ДСТУ 7624: 2014 [6]. Basic transformation of encryption $T_{l,k}^{(K)}$ defined as follows:

$$T_{l,k}^{(K)} = h_l^{(K_t)} \circ y_l \circ t_l \circ p'_l \circ \prod_{n=1}^{t-1} (k_l^{(K_n)} \circ y_l \circ t_l \circ p'_l) \circ h_l^{(K_0)},$$

where K – encryption key with k bit in length; $h_l^{(K_n)}$ – sums function by module 2^{64} of internal state and round key K_n; p'_l – a layer of mutually unambiguous reflection, which processes the bytes vectors (elements V_8). It uses layer of S-blocks. Each element $g_{i,j} \in V_8$ of input state matrix is replaced by $p_{i \bmod 4}(g_{i,j})$, where $p_s \in V_8$ **a** V_8, $s \in \{0,1,2,3\}$ is defined substitutions (S-blocks); t_l – rearrangement of elements $g_{i,j} \in GF(2^8)$ of input state encryption. Performs cyclic shift to the right for rows of internal state matrix $G = (g_{i,j})$. The number of shifted elements depends on the row number $i \in \{0,1,...,7\}$, the block size $l \in \{128,256,512\}$ and is defined by the formula $d_i = \left\lceil \frac{i \cdot l}{512} \right\rceil$; y_l – linear transformation of input state elements in a finite field. During this transformation every element $g_{i,j} \in V_8$ of internal state matrix G is presented as element of finite field $GF(2^8)$, formed by irreducible polynomial $\Psi(x) = x^8 + x^4 + x^3 + x^2 + 1$ or $0x11D$ in hexadecimal form. The elements of the new state matrix $W = (w_{i,j})$ are calculated in $GF(2^8)$ by the formula $w_{i,j} = (v >>> i) \otimes G_j$, where $v = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$ – vector, which forms the circulation matrix with MDS feature, G_j – j-th column of the state matrix G; $k_l^{(K_n)}$ – sums function by module of 2 round key K_n and sate matrix. In functions p'_l, t_l and y_l input argument $x \in V_l$ and output value $c(x) \in V_l, c \in \{p'_l, t_l, y_l\}$ presented as a matrix with size $8 \times c$.

Basic decryption transformation $U_{l,k}^{(K)}$ defined as follows:

where K – encryption key with k bit in length; $-1h_l^{(K_n)}$ – subtraction function by module 2^{64} of internal state and rundown key K_n; $-1y_l$ – inverse linear transformation of input state elements in a finite field. Each element $g_{i,j} \in V_8$ of internal state matrix G is presented as element of finite field $GF(2^8)$, formed by irreducible polynomial $\Psi(x) = x^8 + x^4 + x^3 + x^2 + 1$ or $0x11D$ in hexadecimal form.

Each element of new state matrix $-1W = (-1w_{i,j})$ is calculated in $GF(2^8)$ by the formula $-1w_{i,j} = (-1v <<< i) \otimes G_j$, where $-1v = (0xAD, 0x95, 0x76, 0xA8, 0x2F, 0x49, 0xD7, 0xCA)$ – vector which forms circulated matrix MDS feature, G_j – j-th column of the state matrix G; $-1t_l$ – inverse rearrangement of elements $g_{i,j} \in GF(2^8)$ of input state encryption. It performs cyclic shift to the left for rows of internal state matrix $G = (g_{i,j})$. The number of shifted elements depends on the row number $i \in \{0,1,...,7\}$, the block size $l \in \{128, 256, 512\}$ and is defined by the formula $d_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$; $-1p'_l$ – layer of inverse mutually unambiguous reflection (layer of inverse S-block), which processes the bytes vectors (elements V_8). It uses layer of inverse S-blocks. Each element $g_{i,j} \in V_8$ of input state matrix is replaced by $-1p_{i \bmod 4}(g_{i,j})$, where $-1p_s \in V_8$ **a** V_8, $s \in \{0,1,2,3\}$ is defined substitutions (inverse S-blocks); $k_l^{(K_n)}$ – sum function by the module of 2 rundown key K_n and sate matrix (involutional function).

Algorithm "Kalyna" is implemented in the ECB mode with sizes of key and block in 512 bit and Java programming language, which ensure the highest level of reliability. On Fig. 4 and 5 are given block diagrams of the program for data encryption and generation of rundown keys.

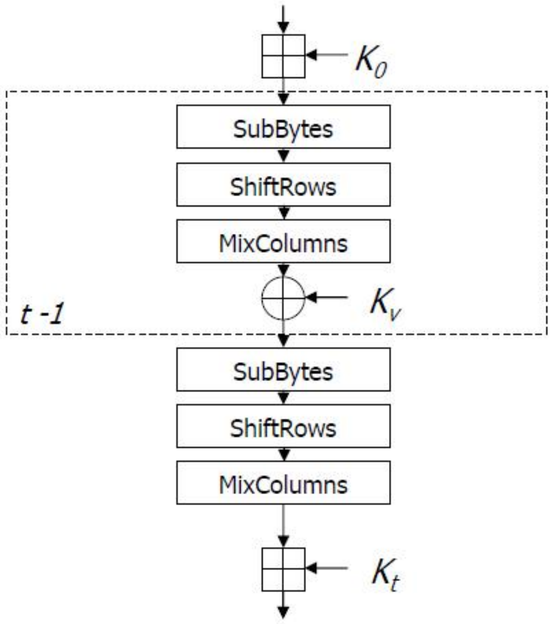


Fig. 4. Block diagram of data encryption

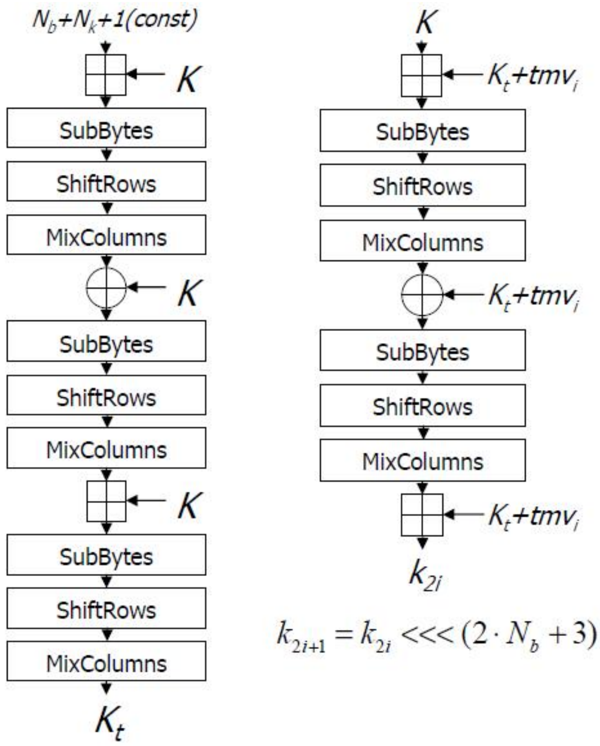


Fig. 5. Block diagram of rundown keys generation

Fig. 4 and 5: SubBytes – bytes replacement operation, ShiftRows – shift rows operation, MixColumns – mixing columns operation.

Fig. 6 shows a result of the program execution.

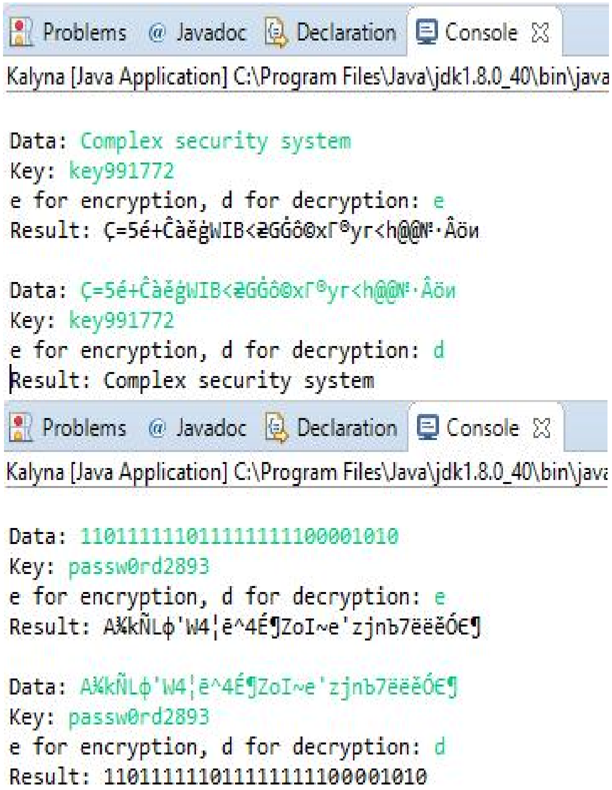


Fig. 6. The result of the program execution

V. CONCLUSION

The building concept of CSS CPS despite the integration of levels was developed, which will enable the usage of unified security measures for information's interaction between components of CPS according to the cloud technologies principles.

A model of information technology states of CPS was constructed as the basis for creation a complex security systems under the influence of threats complex.

REFERENCES

[1] Проект Стратегії кібернетичної безпеки України. – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf

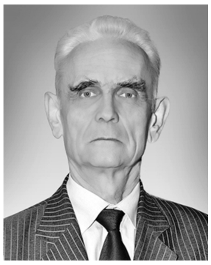
[2] The European Union Agency for Network and Information Security (ENISA). – [Online] – Available: https://www.enisa.europa.eu/

[3] Мельник А. О. Інтеграція рівнів кіберфізичної системи / А. О. Мельник // Вісник Національного університету “Львівська політехніка”, “Комп'ютерні системи та мережі”. – 2015. – № 830. – С. 61–68.

[4] Information technology. Security techniques. Evaluation criteria for IT security. Part 1–3: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008. – [Active from 2009.01.01]. – Switzerland: ISO copyright office, 2009. – 56, 161, 150 p.

[5] Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення: СОУ-Н НКАУ 0060:2010. – [Чинний від 2010-04-01]. – К. : НКАУ, 2010. – 60 с. – (Галузевий стандарт України).

[6] Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624: 2014. – [Чинний від 2015-07-01]. – К.: Держспоживстандарт, 2016. – 117 с.



Valerii Dudykevych since 2006 head of the Department of Information Security at Lviv Polytechnic National University. Graduated from Lviv Polytechnic Institute with qualification of engineer-electrician major – electrical engineering in 1963. PhD thesis was defended in Lviv Polytechnic Institute in 1971, a doctorate in 1991. Specialist in the field of information technologies, instrument-making and information. Professor, Department of automation and telemechanics of Lviv Polytechnic State University since 1992, head of the same Department since 1993. From 1992 to 2001, Dean of the faculty of automation. He founded a new scientific direction – “Theory of analysis and synthesis unit-counting specialized processors, their use in measurement systems and devices for research and production”. In particular, he developed the principles of unit-counting specialized processors converters to handle the number of pulse codes in real time. Developed the theory of structural and parametric synthesis of a number of pulse-specialized processors that optimizes their characteristics. For the parametric synthesis of the developed theory Chebyshev the best approximation with a fixed left edge. Based on the obtained theoretical results, a number of pulse-specialized processors for realization of logarithmic, power, exponential, trigonometric, and other functions was created. They were designed for independent use or as part of the means of linearization of the characteristics of transducers. Scientific results were used in the development of a number of measurement systems and devices. The scientific school, developed under his leadership, developed 6 dissertations D.Sc. and 16 Ph.D., published 3 monographs. He is currently in charge of the scientific developments in the field of information security. The results of these scientific studies and under his leadership, one D.Sc. thesis and three Ph. theses were made. D. For more than ten years, hewas: a member of the expert Council of the Higher Attestation Commission of Ukraine on computer science and engineering; a member of the expert Commission of the Ministry of Education of Ukraine; a member of the expert Council of the State Attestation Commission. Since 2010 and until now is the Chairman of the Dissertation Council D 35.052.18 for doctoral theses, constantly supervises graduate students and advises doctoral students.

Honored inventor of Ukraine (1994), honorary Professor of Lviv Polytechnic National University (2011). Since 1996 he is a member of the Institute of Electrical Engineers of England (member 1996, fellow – 1997). The author of the textbooks, dictionary, 5 monographs, 5 textbooks, 193 inventions, more than 600 scientific publications.

Galyna Mykytyn – Doctor in Technical Sciences, Professor, Professor of the Department of Information Security at Lviv Polytechnic National University. In 1986, she graduated from the radio engineering faculty of Lviv Polytechnic Institute, majoring in automatic telecommunications.

From 1986 to 1992, she worked as an engineer in Scientific production Association “Systema”. In 1988 she entered the postgraduate study in Physical and mechanical Institute national Academy of Sciences of Ukraine, where she studied until 1992. From 1992 to 2011 she worked in the Physical-mechanical Institute of NAS of Ukraine for jobs as a Junior researcher and senior researcher. From 1995 to 2007, concurrently – associate Professor of bioengineering systems and devices Ternopil national technical University Ivan Pului. From 2002 to 2011 part – time- associate Professor of the Department of software, automation and remote control, information security, Lviv Polytechnic National University.

Since 2011 to date – lecturer of the Department of information protection as Associate Professor and Professor. In 1995, she received the scientific degree of Candidate of Technical Sciences. Academic rank of associate Professor was received in 1999, the academic title of senior researcher in 2002. In 2013, she received the scientific degree of doctor of technical Sciences, specialty – information technologies. In 2016, was awarded with the academic title of Professor.

Areas of scientific research – information technology, information security of automated and communications systems. Author and co-author of 2 textbooks (1999, 2008), 1 resource manual (2001), two monographs (2012, 2013), two monographs (2015, 2016), more than 120 scientific papers.

Taras Kret – assistant of the Department of Information Security of Lviv Polytechnic National University.

In 2013, graduated from Lviv Polytechnic National University and received complete higher education in speciality "Systems of technical information security, automation of its processing" and received qualification of a professional in information security.

From 2013 to the present time, is studying at graduate school in the specialty 05.13.21 "Information Security System".

Subject of research – system of information security in a multi-level intelligent control systems. In his scientific heritage, he has 10 publications in the field of information security and participation in over 20 international scientific conferences.

Andrii Rebets – graduate student of the Department of Information Security at Lviv Polytechnic National University. In 2016, graduated from Lviv Polytechnic National University majoring in "Systems of technical information security, automation of its processing" and received complete higher education and received the degree of specialist in information security.

From 2016 up to the present time enrolled is studying at school majoring in 125 "Cybersecurity". The field of research is information security cyber physical systems. Is the co-author of 4 scientific publications and participant of 6 international scientific conferences.