ECONOMICS COLLEGE IN STALOWA WOLA

ENGINEERING SCIENCES: DEVELOPMENT PROSPECTS IN COUNTRIES OF EUROPE AT THE BEGINNING OF THE THIRD MILLENNIUM

Collective monograph

Volume 1

Stalowa Wola, Poland
2018

Recommended for publication
by the Academic Council of Economics College in Stalowa Wola

Responsible for release: dr Małgorzata Korecka, rector
(Economics College in Stalowa Wola)

Engineering sciences: development prospects in countries of Europe at the beginning of the third millennium: Collective monograph. Volume 1. Riga : Izdevnieciba "Baltija Publishing", 2018. 460 p.

ISBN 978-9934-571-63-3

CONTENTS

MODEL FOR CRYPTOGRAPHY PROTECTION OF CONFIDENTIAL INFORMATION

Borsukovskyi Y.V., Borsukovska V.Y.

INTRODUCTION

Appearance and development of informational and cyber spaces assisted the establishment of modern informational society and leaded to synthesis of two technologies – information and telecommunication, but besides, the issue of interstate balance and interaction within the information and cyberspaces (in contrast to such spaces as terrestrial, maritime, air and cosmic) remained open and still requiring the solution. Such state of play is explained, first of all, by unprecedented impact to modern society and its information and cyber spaces by line of expedient information and cyber operations which became lately an inherent part of domestic and foreign policy of the most states around the world.

Again, the active operations at information and cyber spaces start to play an essential role in economic and social development of highly developed states and certifies their reaching of new phase of social interaction – information and cyber confrontation.

Together with blowing increase in volume of data accessed by the ordinary citizens and its transition to cloud infrastructure, as well the invention of powerful computers and imbedded microcontrollers – all abovementioned force the world countries not only to global intellectualization and receiving of certain advantages, but also promote the appearance of certain security problems. Intellectualization of operations at cyberspace increases the number and directions of destructive actions and simultaneously significantly increases the vulnerability of critically important infrastructure assets of these countries to threats of man-made nature and natural calamities.

Initially it was officially stated in January 2017 at World Economic Forum at Davos, and in consequence underlined the political necessity in control and further regulation of relations in these spheres, as well on special actuality of process for creation by countries their own security systems, which in a close perspective will play

the extremely important role at international geopolitical competition. In 2018 the Davos Forum again in global topic “Creating a Shared Future in a Fractured World” discussed the combating the world`s cyber threats. Global landscape of threats[1] presented to the Forum is provided on Picture 1.

R-Vision Company on the basis of analysis of vendor`s forecasts (supplier companies) for informational security (IS) had concluded the TOP-10 threats in informational sphere for 2018[2]. Company’s representatives consider the following threats:

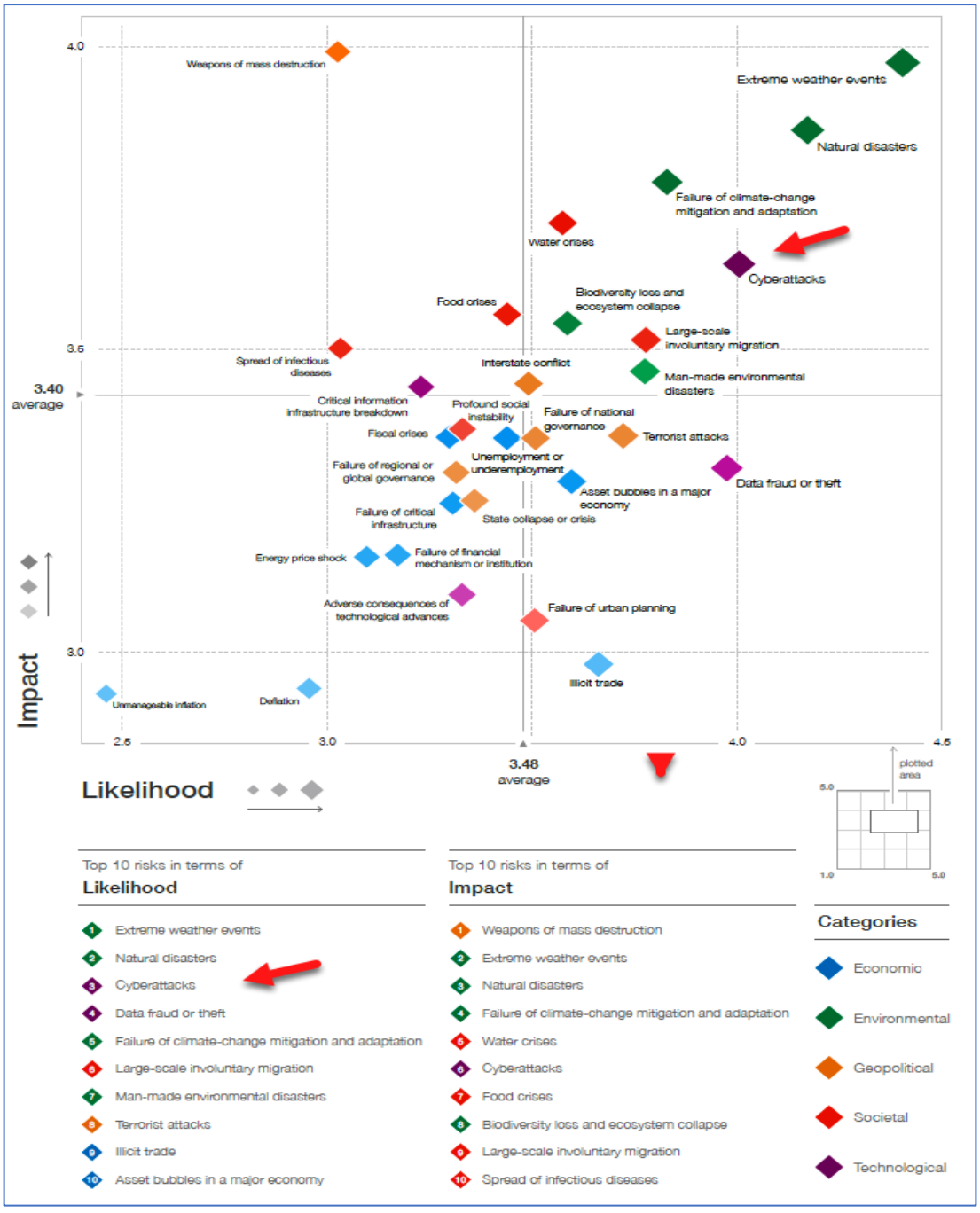
- *use of machine learning and artificial intellect* – applied for automated search of threats, increase of attacks accuracy, execution of sophisticated fishing attacks;
- *further development of ransomware* – such programs remains a key component in 2018 landscape of threats, its families will increase, and hacker’s focus will move to mobile devices;
- *IoT vulnerabilities* will be used more often, considering the numerous devices are produces without any security rules and any industry standards;
- *Hacking of mass media and social networks accounts to share the false information* – shall mean the impact to stock market quotes, manipulation with public opinion, negative impact to the reputation, propaganda via hacked channels, etc.;
- *Increase in attacks to manufacturing facilities* – spin up in preparation and realization of complex cyberattacks in manufacturing facilities by means of cyber espionage and expert knowledges of Computer-Assisted Management of Technical Processes and industry specifics;
- *Attack of ghost and light viruses* – ghost malware does not write to hard drive the files and execute all its actions in memory, and during the system

[1] World Economic Forum, „Reports 2018“ [Electronic resource]. Access mode: www3.weforum.org/docs/WEF_GRR18_Report.pdf

[2.] 2018 Informational Security Forecasts: [Electronic resource]. – Access mode: https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/.

restart the virus is vanished, but it already damaged the system, and detect, trace or stop such an attack is extremely hard;

- *Attacks on mobile applications.* The main targets are Android and iOS platforms – increase in attacks frequency and improvement of prevention technologies will cause the appearance of more complicated APT-malwares for mobile platforms;



Picture 1 - Global landscape of threats 2018

- *Attacks on the cloud infrastructure and storages* – leak of data from public cloud storages which may lead to access for private keys, passwords, private information and even intellectual property.

World Economic Forum experts consider the world to face the exact crucial period when the focus of the world`s critical energy is directed especially to incitement of hatred. Mass cases of fraud with data and/or its theft cause not only the economic damage, but also cause geopolitical intensity and loss of confidence in Internet that automatically may lead to essential social unrest with unpredicted consequences[3]. Besides, the development and dissemination of perspective informational systems and technologies promote the new forms of cyber-attacks which expose the governmental and corporate resources to threats with which they are not ready deal with.

RESEARCH THEORETICAL BACKGROUND

Cryptography protection of confidential information, including the scientific and technical information, allows ensuring the additional level of information security with restricted access, by means of creation of additional protection at local and network information resources and during information transmission through the open channels. Today, IT-experts consider the cryptography protection as the most efficient way to secure information from unauthorized access.

Considering the current landscape of information and cyber threats, the cryptography protection of information now is reasonable to use for all data essential for business and security of state. Such data could be processed and stored at hard disks, portable units, in electronic letters, files, folders and other places. We can formulate the line of specific threats to information resources for which timely prevention is reasonable to use the encryption of confidential information[4]:

[3] Euronews - Davos 2018: Global Threats Response: [Electronic resource]. – Access mode: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic.
[4] Access Controls. [Electronic resource]. Access mode: TechNet - Microsoft (https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx)

1. **Computer equipment theft.**

At theft and loss of computer technics the confidential data that stored at unencrypted disks and other data storages, could be easily reached by intruder and sold to interested person, including to competitors. Moreover, in case of unexpected inspections and seizure of computer equipment by representatives of the state agencies the confidential information may become known to other persons.

2. **Business espionage.**

Business espionage incidents which lately became more often are connected with high level of financial losses. Anyone, even the most “reliable” person, may be an intruder. It can get the access to resources where stored the unencrypted business critical and important data. Besides, one should remember that system and applications administrators have, *a priori*, the full access to any information that is stored at computers, servers and different data storage devises.

3. **Compromising materials.**

With physical access to computer or server the intruder may place there any negative information and inform on it the interested persons. At that, the consequences for business may be quite unexpected.

4. **Negligence of subjects.**

If the subject suddenly left its working place and forgot to block computer, the information may become available to other persons and may be used to inflict the serious damage to information owner. Moreover, the subject may inaccurately send the confidential information to untrusted addressee.

The separate problem at cyberspace become, *de facto*, realization of cyber strategies at the level of the state policies that clearly declare the possibility to ensure competitive intelligence in favor of own producers, as well the further enhancement of technical capabilities of criminal structures.

The volume of threats related to business and state confidential information just increase each year. According to the latest researches of Fortinet Company the number of attacks on one organization had increased at 82% during last quarter of

2017[5]. When WikiLeaks published the documents and files of high-security network situated inside the CIA's Center for Cyber Intelligence in Langley – actually the cyber arms elements – in a short term the means and practices of the state agency were effectively used for criminal purposes[6].

Main advantages in use of cryptography protection tools for confidential information:

- secure protection of confidential information that regularly used in electronic format;
- possibility to protect from unauthorized access to data bases, corporate e-mails and other restricted information;
- granting access to confidential data only to reliable subjects;
- existence of tools for urgent block of access to confidential data;
- protection from unauthorized copying of confidential data by disloyal or corrupted subject who may have the physical access to computer and server equipment;
- reduction of risk of direct and indirect financial losses caused by unauthorized leakage of business critical information;
- increase in level of trust of clients and partners;
- increase in level of corporate business-ethics in external and internal information exchange with electronic messages;
- assure in solid security of confidential information.

Consequently, the introduction of cryptography protection tools for confidential information provide the reduction of confidential information leakage risks and increase the competitiveness of enterprises and national safety in general. Obviously that use of cryptography protection tools for confidential information require the development of relevant model and it also require the formalization of its main components in order to create relevant procedures and instruction for deployment,

[5] Fortinet. [Electronic resource]. Access mode: https://www.itweek.ru/security/news-company/detail.php?ID=199637
[6] WikiLeaks (@wikileaks). [Electronic resource]. March 7, 2017

exploitation and efficient management of cryptography protection tools for confidential information[7].

RESEARCH RESULTS

Considering the rise in information and cyber threats we should identify few main positions in approach to development of model for cryptography protection of confidential information (hereinafter referred as model).

1. General Provisions

In order to ensure the protection of confidential information from unauthorized access, leakage, intentional or undeliberate integrity violation, or accessibility or other threats to information and cyber security, the model for cryptography protection of confidential information should include the functional and organizational requirements to information cryptography protection tools.

Information cryptography protection tools should ensure the encryption of disks at working stations, information at portable storage devices, e-mail and files at corporate network; as well ensure the work with encrypted e-mail at fixed and mobile devices.

2. Model Role

The model is developed to regulate the use of information cryptography protection tools to secure the confidentiality, authenticity and integrity of confidential information, as well to support information security in storage and exchange of confidential information with internal and external partners.

The acting model should define:

- main functional and organizational provisions for work with information cryptography protection tools;
- information security requirements for information cryptography protection tools;
- responsibility at work with information cryptography protection tools.

[7] Borsukovskyi Y.V., Borsukovska V.Y. «Defining Current Requirements to Policy for Use of Information cryptography Protection at Enterprise». Modern Information Protection, №1, 2018, p. 74–81.

3. Model scope

Model shall cover all subjects (or users) and third parties who are engaged to electronic workflow, and all its provisions and requirements are obligatory for all subjects and third parties, with no exceptions.

All exceptions from the acting provisions and requirements of the model shall be agreed with information security department.

4. General requirements of the model for use of information cryptography protection tools

In development, implementation and use of confidential information cryptography protection tools should be obligatory considered the provisions and requirements of the shaped model.

Information security department shall define the list of approved information cryptography protection tools according to the provisions and requirements of the shaped model.

Information cryptography protection tools shall be used for:

- encryption of confidential information that is used and transmitted;
- ensure its integrity and/or authentic;
- non-repudiation of taken actions with use of cryptography methods of receiving evidences of existence, absence of incident or action.

With use of encrypted file folders of general access, additionally should be delimited the user access modes at system level and provided only to subjects who have the relevant access authorization to such folders[4,8].

All local and portable disks at computers of subjects (users) should be encrypted.

In order to boot operational systems of computers with encrypted disks at model should be used the procedure for additional pre-boot authentication.

For portable storage devices should be used the procedure of enforced encryption for any data recording, except for devices included to the list and which

[8] Role Based Access Control for IBM Systems Director Console. [Electronic resource]. Access mode: http://www.ibm.com/support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm.

could contain the exposure information. The acting list of such devices shall be approved by information security department on written request of head of organizational unit.

The received or generated cryptography keys at confidential information protection model shall be subject to protection measures related to its loss, change or damage. Private keys shall be protected from unauthorized access or disclosure.

Public users' cryptography keys shall have a certain validity term and be available to all participants of information exchange.

Confirmation of users` cryptography keys validity shall be automated with model scheduled interval.

In case of user inactivity with cryptography key during the defined period, the key should be automatically blocked for further search at information cryptography protection tool.

Passphrase (if required) shall conform with model requirements to password quality assessment, generally fixed at information cryptography protection tool (if any). The recommended minimum length for passphrase for model of information cryptography protection shall constitute at least 15 symbols. Spaces are not recommended for passphrases.

In case of subject dismissal, the model should consider that private keys shall be stored at keys archive storage of information security department and canceled for use by information cryptography protection tools.

In case of private keys compromise and/or key information the model should consider the actions to suspend any operations with such keys and key information, as well the actions on change of encryption keys and key information.

All actions related to management of cryptography keys shall be registered with keys management system and if such function is unavailable – at paper form.

In model the formalization of management process of cryptography protection tools shall be ensured according to exploitation and technical documentation, instruction for use (provided procedures and regulations).

The procedure for functioning of information cryptography protection tools, responsibilities of subjects who ensure its performance, work rules of subjects who use the information cryptography protection tools shall be specified in the model with relevant job instructions, procedures and regulations.

5. Model`s requirements to confidential information cryptography protection

The model in part related to procedure on transfer and storage of documents containing confidential information should consider the obligatory use of information cryptography protection tools (electronic documents should be obligatory encrypted).

The model for cryptography protection of confidential information regarding the subjects who use the information cryptography protection tools shall categorically forbid the users to:

- provide to anyone the private cryptography key;
- disclose the access password (PIN-code) to private cryptography key, including the direct supervisor;
- inform anyone that he/she is an owner of private cryptography key;
- use the private cryptography key at obviously damaged reader, broken personal computer, laptop, mobile device, server, etc.;
- violate the requirements of documents that provide rules for receiving/storage/work with information cryptography protection tool.

7. Model`s requirements for set hierarchy of cryptography keys

In order to ensure the confidentiality and authentic of information, prevention leakage, intentional or undeliberate integrity violation, accessibility, as well as other threats to information security in model shall be defined and approved the requirements on cryptography keys hierarchy.

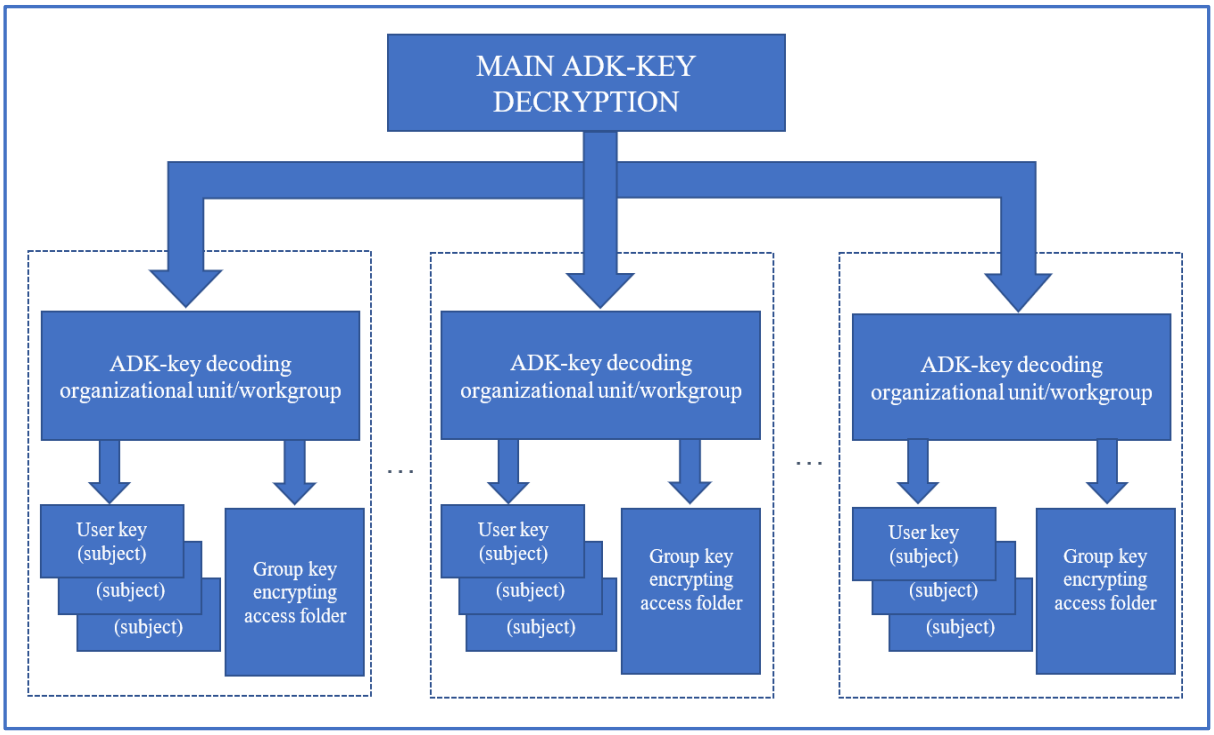
Such requirements define the acting hierarchy of encryption keys and additional decryption keys to support the information security in storage and information exchange.

The provisions shall define:

- hierarchy of additional decryption keys (ADK keys);

- requirements for ADK keys name;
- responsibilities in working with ADK keys.

The possible variant of hierarchy for encryption/decryption keys is provided at Picture 2.



Picture 2. Hierarchy for encryption/decryption keys

where:

Main ADK-key decryption – the key which is added to each encryption process which runs within subordination (Picture 2).

ADK- key decryption of organizational unit – key which is added to each encryption process executed within organizational unit and/or working group.

User key (subject) – personal key which is used by user for encryption/decoding of information used in execution of its service tasks (Picture 2).

Group key encrypting access folder – key which is used by the group of users for encryption of shared folders and further access to encrypted information in it (Picture 2).

Organizational unit – group of users which is created on the basis of assignment of users to certain structural units and/or working groups (department, division, sector, working group).

8. Scope of cryptography keys hierarchy

In model the scope of cryptography keys hierarchy and additional decoding keys shall cover the keys of all users with relevant rights for receiving/storage/work with cryptography keys.

All the exceptions from the provision of model on acting hierarchy of cryptography keys should be agreed with information security department.

9. Requirements of the model to ADK-keys structure

The model should provide the multi-level structure for additional decoding keys (maximum two levels recommended) which ensure the alarm possibility to access the encrypted information in special cases provided in the model by provisions and requirements related to keys hierarchy (Picture 2).

Additional decoding keys should be included to all cryptography keys which are used by subjects to protect the confidential information.

10. Requirements of the model for decryption keys name

Model shall include the requirements and templates for decryption keys names.

11. Responsibility for implementation and execution of provisions and requirements of the model

Model for cryptography protection of confidential information should formalize the requirements to responsibility for installation, customization, working capacity and maintenance of information cryptography protection tools.

Generally, the information security department is responsible for management of cryptography keys.

Responsibility for adherence by subjects of the requirements of acting information security policies, as well the control over physical integrity of users (subjects) key information storages (private keys, certificates etc.) is assigned to their direct supervisors.

Information security department is responsible for model maintenance.

Regarding subjects who violate the information security requirements, the model should formalize the disciplinary measures, including admonition and dismissal for serious violation of information security requirements.

12. Model`s history

All changes and modifications to acting model of cryptography protection of confidential information are subject to protocol stating the content of changes, date, background and person responsible for implementation of relevant changes and modifications.

Summarizing the abovementioned requirements for creation of model for cryptography protection of confidential information we could provide an example of its practical use for protection of authentication data of subject (user) of information resources.

Well known, that today the user should remember numerous passwords. It means password to computer, e-mail, local network, home web-page, FTP access, passwords for Internet-services (Internet-banking, accounts at forums, web-sites, messengers) etc. This list may be continued endlessly.

On the one hand, if one has complex and numerous passwords, they could be hardly remembered. On the other hand, if carefully follow the security provisions and requirements provided in model for confidential information protection, then user, and administrator as well, besides the requirements should receive the instrument which enable easy creation and storage of passwords for equipment, applications and services in protected mode and simultaneously enable its easy operation.

In such cases the use of cloud services for passwords storage is not always appropriate and comfortable, and, also, not very secure – lately increased the messages on hacking of cloud services for passwords storage. Correspondingly, information security department should undertake the mission to steer the middle course for triple requirements to this instrument – “security-functionality-costs”.

Considering abovementioned conditions, the minimal requirements to model for cryptography protection of authentication data may be formulated as follows:

1. Essential to ensure cryptography protection of all authentication data of subject from unauthorized access.
2. The subject has to have the convenient and operational access to authentication data.
3. All authentication data (logins, passwords, URL etc.) should be stored at secure data base.
4. All authentication data should be stored in encrypted form; data base should be completely encrypted.
5. For access to data base should be used the master-password and additional firewalls.
6. As additional element of protection the data base should be placed at environment secured with firewalls.
7. Solution cost should be at consumer grade.

Of course, here are the simplified requirements to development of model of cryptography protection of all authentication data of subject, and we also should consider at model construction the first security principle "If you had run the program of intruder at your computer – it is not your computer anymore"[9]. These require supplementing the description of model with additional security facilities to create protection barriers in case of attacks on information resources.

In general terms the model could be presented as follows:

$$\mathbf{M_A(CC, FC, MC, SN, GS) = CC(PW_{CC,}\, C_{KC}, P_{KC}) + FC(PW_{FC}, CP_{AES256}) + MC(PW_{MC}, C_{MC}, P_{MC}) + SN(PW_{SN}, C_{KC}, C_{MC}) + GS(C_{MC})}$$

where:

CC - cryptographic container;

FC - USB-flash drive with hardware cryptographic protection;

MC - cryptographic certificate;

SN - etoken key;

GS - synchronization service;

[9] Ten Immutable Laws of Security. [Electronic resource]. Access mode: https://technet.microsoft.com/ru-ru/library/cc722487.aspx.

PWxx - password service;

Cxx - secret service key;

Pxx - public service key;

CP_{AES256} - integrated hardware encryption chip AES256.

Here is one of the possible variants for implementation of proposed model. As solution we shall use the Open Source passwords manger - KeePass[10] and USB flash disk with hardware encryption and fixed antivirus protection Safexs Protector XT[11]. This is the operational solution, quite flexible, comfortable and validated with long-term use in corporate sector and personal use.

KeePass Password Safe – ensures the storage of all passwords of subject (user) with use of one main master-password. Application supports the encryption algorithm Advanced Encryption Standard (AES 256-bit, Rijndael and Twofish). It has the portable version which does not require the installation and could be stored at flash disk, and that is important for our solution. Moreover, it has the open code of program for its analysis and program interface is provided at 40 languages. Besides, the program ensures the export of password base in different formats TXT, HTML, PDF and also import in different formats.

For additional protection of authentication database of subject the KeePass ensures the use, together with main master-password, the additional key file which is encrypted with use of private certificate (Picture 3).

The example for construction of authentication data base is provided on Picture 3, where:

Hardware Group – equipment credentials (server, commutator, routers etc).

a) IBM Subgroup – IBM equipment credentials.

b) Cisco Subgroup – Cisco equipment credentials.

c) HP Subgroup – HP equipment credentials.

[10] KeePass Password Safe. [Electronic resource]. Access mode: https://keepass.info/.

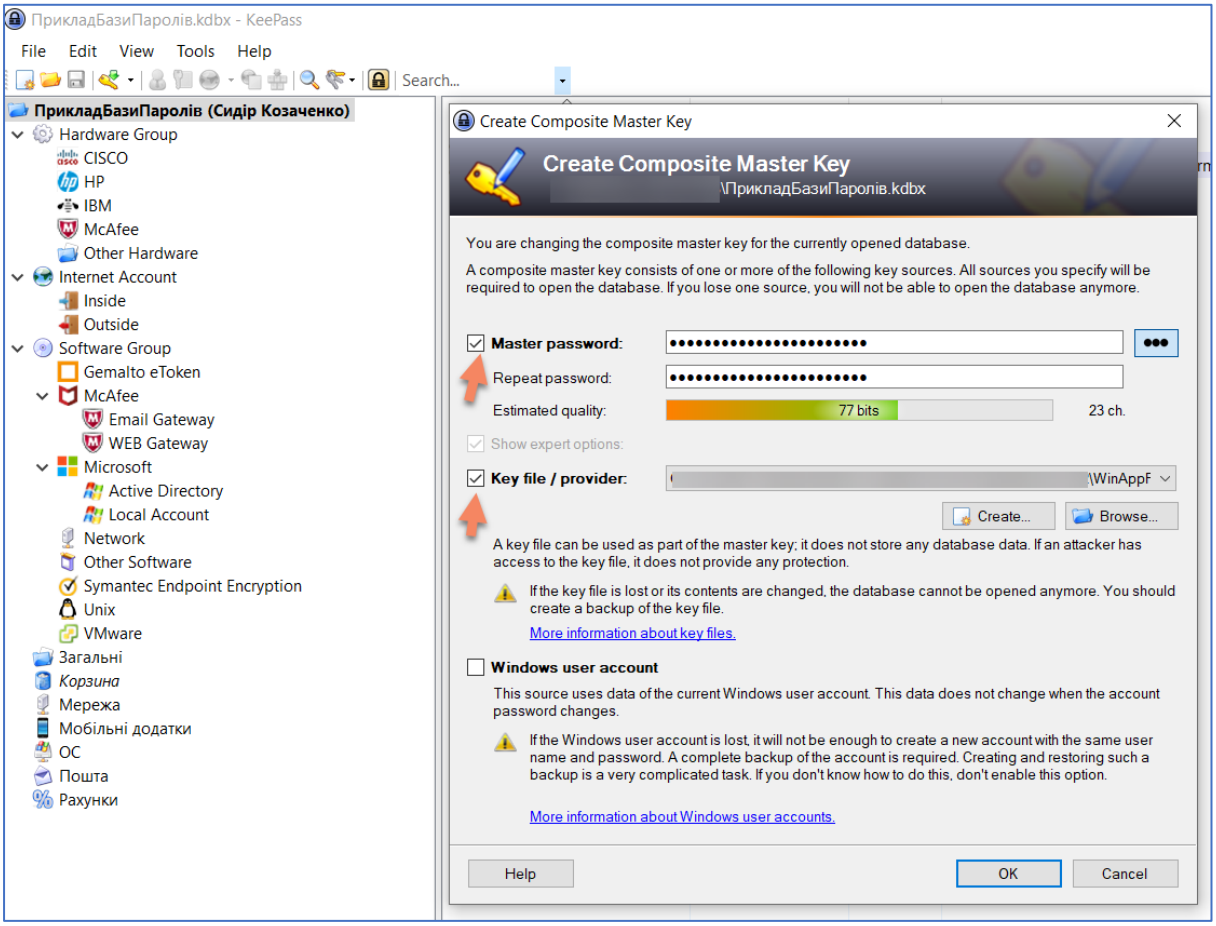
[11] Safexs Protector XT. [Electronic resource]. Access mode: http://www.safexs.info/products/protector-xt/.

Internet Account – Internet resources credentials. In this group are stored URL, logins and password to access the Internet resources, and they are conditionally separated into two categories:

a) Subgroup Outside - external resources outside the organization.

b) Subgroup Inside - internal resources inside the organization.

Software Group – credentials at various systems, applications and services … etc.



Picture 3. Example for structure of authentication data

For storage of services private key we shall use the PKI-based Multi-factor authenticator SafeNet eToken 5300[12], that provides us with additional hardware factor of pre-authentication at subject`s access to its authentication data base.

Realization of abovementioned model for cryptography protection of authentication data ensures the subject with:

[12] SafeNet eToken 5300. [Electronic resource]. Access mode: https://safenet.gemalto.com/resources/product-brief/data-protection/safenet-etoken-5300/.

1. Comfortable and secure instrument for creation and encrypted storage of authentication data for access to web-resources, network and server equipment, applications and services – sophisticated pairs (login, password), URL and etc.;
2. Possibility to create unique authentication data for each item of equipment, web-service, applications and services;
3. Possibility to keep “correct” URL for access to web-resources – decrease probability of use of fake URL;
4. Possibility to store additional confidential information (IP, configuration data etc.);
5. Adhere in full scope the requirements of password policies;
6. Ensure mobility access to confidential resources with keeping of multi-level protection of authentication data.

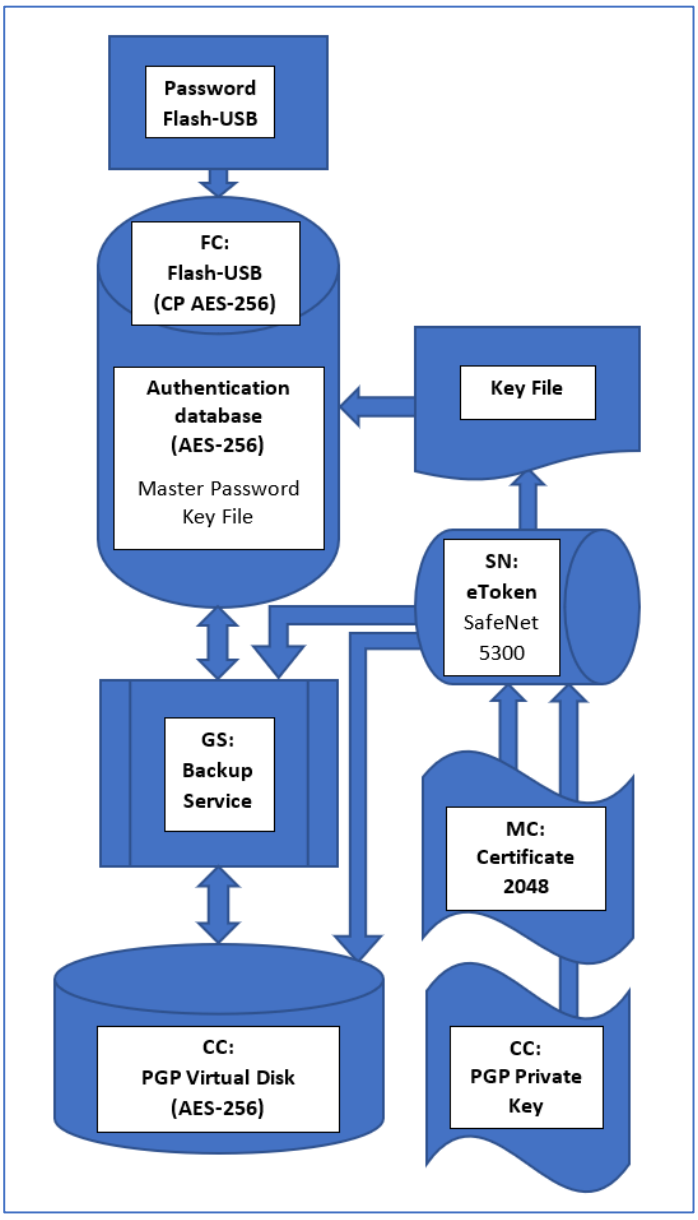
Actually, in realization of abovementioned model for cryptography protection of confidential information we ensure for the subject the following levels of hardware and software protection of authentication data:

1. Hardware cryptography protection of database where stored all authentication data;
2. Encryption of authentication data at database;
3. Separate key file to access the database encrypted with personal certificate;
4. Storage at hardware medium and hardware cryptography protection of certificates which are used to access the confidential information;
5. Hardware passwords for access to authentication data and certificates database.

So, the proposed model allows to realize the multi-level protection at subject`s access to its authentication data (base encryption, master-password, key file, certificate). The multi-levels reduce the possibility for compromising of authentication data of subject, and provide additional capabilities to use unique authentication data for each separate equipment, service or application.

Functionally the model for cryptography protection of authentication data may be provisionally presented in a form provided at Picture 4.

For the purposes of mobility and keeping of authentication data backup copies in this function we may use the cryptographic container with keys not less than 2048 byte. Cryptographic container in our case is created by means of Symantec Encryption Desktop[13] and placed, generally, at secured corporate environment.



Picture 4. Model`s functional view

In order to synchronize the main and backup authentication data base of subject is used the synchronization service GoodSync Enterprise[14] or fixed at Safexs Protector XT functional for safe backup.

CONCLUSIONS

Large scale cyberattacks, mass cases of fraud with data and/or its theft cause not only the economic damage, but also cause geopolitical intensity and loss of confidence in Internet. The main precondition for such a tendency in 2017-2018 became the increasing interest of governmental structures in receiving of information which can be used by opposing parties in world`s competitor and political fights.

[13] Symantec Encryption Desktop 10.4.x For Windows User's Guide. [Electronic resource]. Access mode: https://support.symantec.com/en_US/article.DOC9226.html.
[14] File Synchronization and Backup Software. [Electronic resource]. Access mode: https://www.goodsync.com/.

The issue of effective organization of confidential information protection became the hottest point throughout the world. Especially this is burning for enterprises of critically important infrastructure.

Development of model for cryptography protection of confidential information provides the information security departments of critical infrastructure assets with instrument to create the structured system for protection confidential information and standardize the requirements for its functioning.

The presented model is already implemented to structures of different forms of incorporation and education plans for training specialists on information and cyber security at Borys Grinchenko Kyiv University and State University of Telecommunications. In course of further researches will be processed the statistics results received from abovementioned educational institutions and introduced the correlations to the structure of model for cryptography protection of confidential information.

The proposed recommendations for basic elements at creation of model for cryptography protection provide the decrease of risks related to unauthorized access to confidential information, loss and compromising of confidential information resources etc.

Further researches should be focused on creation and implementation of standard models, procedures, regulations and instruction for deployed basic cryptography protection tools for confidential information and their exploitation, trainings with personnel on rules and practices of efficient use of systems for cryptography protection of information.

SUMMARY

Current article provides the detailed analysis of requirements for creation of model for cryptography protection of confidential information. Article defines the use of information cryptography protection tools in order to ensure the application of organizational and technical actions to prevent leakage of confidential information at critical infrastructure assets. It provides the basic requirements for the structure and functional elements of model for protection of confidential information. Formalize

requirements on creation, implementation and exploitation of preventive procedure in management of multi-level protection of confidential information. The article includes example of use of model for cryptography protection of information for creation of secure and transparent in use the authenticating data base of user. The presented model of protection ensure to have a few levels of firewalls, that, on one hand, simplifies its use in execution of acting security policies and decrease the probability of discrediting of authenticating data, and, on other hand, increase the probability to detect the criminal actions of third party by means of multi-level protection system. It considers the practical experience in creation of standard models for protection of confidential information for development, implementation and management of modern policies on information security in part of use of cryptography protection tools for confidential information at enterprises of different forms of incorporation.

Keywords: model, cryptography protection, encryption, access, policy, cybersecurity.

REFERENCES

1. World Economic Forum, „Reports 2018“ [Electronic resource]. Access mode: www3.weforum.org/docs/WEF_GRR18_Report.pdf [Checked October 11th 2018].
2. 2018 Informational Security Forecasts: [Electronic resource]. – Access mode: https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/ [Checked October 11th 2018].
3. Euronews - Davos 2018: Global Threats Response: [Electronic resource]. – Access mode: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic. [Checked October 11th 2018].
4. Access Controls. [Electronic resource]. Access mode: TechNet - Microsoft (https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx) [Checked October 11th 2018].

5. Fortinet. [Electronic resource]. Access mode: https://www.itweek.ru/security/news-company/detail.php?ID=199637. [Checked October 11th 2018].
6. WikiLeaks (@wikileaks). March 7, 2017. [Electronic resource]. Access mode: https://wikileaks.org/. [Checked October 11th 2018].
7. Borsukovskyi Y.V., Borsukovska V.Y. «Defining Current Requirements to Policy for Use of Information Cryptography Protection at Enterprise». Modern Information Protection, №1, 2018, p. 74–81. [Checked October 11th 2018].
8. Role Based Access Control for IBM Systems Director Console. [Electronic resource]. Access mode: http://www.ibm.com/support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm. [Checked October 11th 2018].
9. Ten Immutable Laws of Security. [Electronic resource]. Access mode: https://technet.microsoft.com/ru-ru/library/cc722487.aspx. [Checked October 11th 2018].
10. KeePass Password Safe. [Electronic resource]. Access mode: https://keepass.info/. [Checked October 11th 2018].
11. Safexs Protector XT. [Electronic resource]. Access mode: http://www.safexs.info/products/protector-xt/. [Checked October 11th 2018].
12. SafeNet eToken 5300. [Electronic resource]. Access mode: https://safenet.gemalto.com/resources/product-brief/data-protection/safenet-etoken-5300/. [Checked October 11th 2018].
13. Symantec Encryption Desktop 10.4.x For Windows User's Guide. [Electronic resource]. Access mode: https://support.symantec.com/en_US/article.DOC9226.html. [Checked October 11th 2018].
14. File Synchronization and Backup Software. [Electronic resource]. Access mode: https://www.goodsync.com/. [Checked October 11th 2018].

Information about author:

Borsukovskyi Y. V.,

PhD in technical Sciences, Professor of Department of Information and cyber security,

Borys Grinchenko Kyiv University,

18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine

Y.Borsukovskyi@kubg.edu.ua

ORCID ID 0000-0003-1973-2386

Borsukovska V. Y.,

PJSC ‘’Ukrsotsbank”, Security Department,

29 Kovpaka str., Kyiv, 03150, Ukraine

v.barsik@gmail.com

ORCID ID 0000-0002-4929-6987

АНОТАЦІЯ / ANNOTATION

УДК 004.056

Борсуковський Ю.В., Борсуковська В.Ю. Модель криптографічного захисту конфіденційної інформації

В даній статті проведено детальний аналіз вимог щодо формування моделі криптографічного захисту конфіденційної інформації. Розглянуто використання засобів криптографічного захисту інформації з метою реалізації організаційних та технічних заходів по запобіганню витокам конфіденційної інформації на об'єктах критичної інфраструктури. Сформульовані базові вимоги та рекомендації щодо структури та функціональних складових моделі захисту конфіденційної інформації. Формалізовані вимоги щодо створення, впровадження та експлуатації превентивних процедур управління багатоступінчатим захистом конфіденційної інформації. Наведено приклад використання моделі криптографічного захисту інформації для створення захищеної і прозорої в використанні бази аутентифікаційних даних користувача. Запропонована модель захисту дозволяє мати кілька ступенів програмного та апаратного захисту, що із однієї сторони спрощує їх використання при виконанні чинних політик безпеки і зменшує ймовірність дискредитації аутентифікаційних даних, а із іншої сторони підвищує ймовірність виявлення зловмисних дій третьої сторони за рахунок багатоступінчатої системи захисту. Враховано практичний досвід створення типових моделей захисту конфіденційної інформації для розробки, впровадження та управління сучасними політиками інформаційної безпеки щодо питань використання засобів криптографічного захисту конфіденційної інформації на підприємствах різних форми власності.

Ключові слова: модель, криптографічний захист, шифрування, доступ, політика, кібербезпека.

UDC 004.056

Borsukovskyi Y., Borsukovska V. Model for Cryptography Protection of Confidential Information

Current article provides the detailed analysis of requirements for creation of model for cryptography protection of confidential information. Article defines the use of information cryptography protection tools in order to ensure the application of organizational and technical actions to prevent leakage of confidential information at critical infrastructure assets. It provides the basic requirements for the structure and functional elements of model for protection of confidential information. Formalize requirements on creation, implementation and exploitation of preventive procedure in management of multi-level protection of confidential information. The article includes example of use of model for cryptography protection of information for creation of secure and transparent in use the authenticating data base of user. The presented model of protection ensures to have a few levels of firewalls, that, on one hand, simplifies its use in execution of acting security policies and decrease the probability of discrediting of authenticating data, and, on other hand, increase the probability to detect the criminal actions of third party by means of multi-level protection system. It considers the practical experience in creation of standard models for protection of confidential information for development, implementation and management of modern policies on information security in part of use of cryptography protection tools for confidential information at enterprises of different forms of incorporation.

Keywords: model, cryptography protection, encryption, access, policy, cybersecurity.