TECHNICAL SCIENCES AND TECHNOLOGIES
UDC 004.056.5
DOI: 10.25140/2411-5363-2018-3(13)-167-172

Volodymyr Bazylevych, Dmytro Mekhed, Volodymyr Guryev

DEVELOPMENT OF CRITERIA OF PROTECTION FROM CYBER THREATS AT SOCIAL ENTERPRISE

Urgency of the research. *The issue of creating a system of protection against cyber threats today is becoming urgent. The ever-growing number of cyberattacks is the confirmation.*

Target setting. *Most enterprises, especially small ones, cannot afford to maintain a specialized department, or even an outsourcing company for the implementation of security systems. In this context, the formulation of general protection criteria can solve this problem.*

Actual scientific researches and issues analysis. *The latest public access publications, statistics, corporations reports were reviewed.*

Uninvestigated parts of general matters defining. *Adapting criteria for protection against cyber threats for social enterprise. Are social enterprises more vulnerable to cyber threats and if so, why? Which criteria are more important and which ones can be neglected?*

The research objective. *Develop adapted criteria for protection against cyber threats, which can be used to create a system of protection at a social enterprise.*

The statement of basic materials. *The types and statistics of cyber threats are analyzed. A table of criteria has been constructed, which includes: the financial value of the information, the coefficient of value, the event, the probability of occurrence of the event, the number of resources needed to ensure complete security, the type of storage device information.*

Conclusions. *The proposed criteria allow the creation of adapted and unified security systems against cyber threats.*

Keywords: *cyber threats; social entrepreneurship; security criteria; value of information; types of data storage devices; databases.*

Fig.: 2. Table: 1. References: 6.

Urgency of the research. The issue of creating a system of protection against cyber threats today is becoming urgent. The ever-growing number of cyberattacks is the confirmation.

Target setting. Nowadays become more and more popular such words as hackers, viruses, cyber-attacks and something like this: “somebody hacked my account/e-mail” or “enterprises or web-system or something else were attacked by hackers/cyberterrorist”. So, what is cyber threats? Today there lot of different methods how “bad guys” can get access to your information.

We have three types of cyber threats, which are:

1. Unauthorized access to confidential information
2. Modification of information
3. Loss of information

So we can say that if somebody who you don’t want to get access to your information then you were attacked. Because it can influence to your finance, reputation, relations, etc.

Today we can see that numbers of cyber-attacks are slowly increasing every year, but at the same time a lot of corporation and companies are beginning to pay more and more attention to cybersecurity. Also company which developed software trying to release programs with fewer backdoors, spending more time for testing, update old software if they find some bugs in it, etc.

According to Derek Manky (Fortinet global security strategist) “Every minute, we are seeing about half a million attack attempts that are happening in cyber space” [1].

According to Symantec report 2017 [2] we can find more than 1000 breaches in cyber space every year, and because of it about 1 billion people are exposed to cyber-attacks per year.

Most of attacks are not very dangerous, but some of them could cause serious economic and political damage. For example attacks during US presidential election in 2016.

Why it is important to think about cybersecurity if you decided to start a social enterprise?

As we know “social entrepreneurship is a special form of management which purpose is to run a production function in such a way as to ensure increased value for all the parties in that function” [Sandal, 2004]. So usually, if you start a new social enterprise you responsible for everything, but at the same time you cannot be expert in all areas. For many different things, like building, plumbing, poster printing, etc., you can find outsource company, but when we are talking about confidential information, it becomes harder.

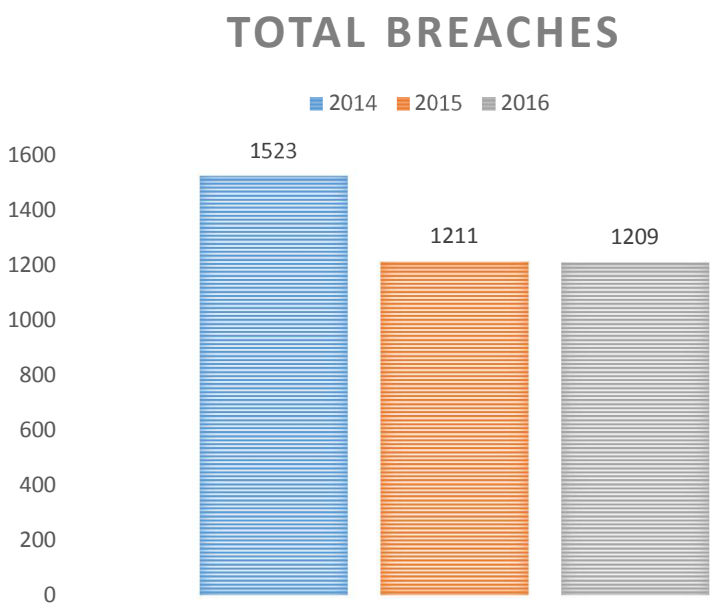

Fig. 1. Numbers of total breaches per year

Source: information from Symentec report 2017.

History knows a lot of example when company went bankrupt due to a security breach [3]. In addition, if somebody get access to the information, which is your commercial secret, you could went bankrupt in few days or at least suffer huge losses.

Actual scientific researches and issues analysis. The research of this problem was carried out by such domestic and foreign scientists as Jan-U. Sandal, Yu. O. Kovalenko, Y. M. Tkach, S. V. Kazmirchuk, D. B. Mekhed [4], S. M. Shkarlet [5] and others.

Uninvestigated parts of general matters defining. In this article, the analysis of threats will be focused on the peculiarities of social entrepreneurship. The threat analysis will be conducted using quantitative analysis and modeling of dangers.

The research objective. Analyze features of functioning and cyber threats on a social enterprise. Develop a set of criteria that are required to build a security system of the enterprise.

The statement of basic materials. We could say that organizations whose primary goal is social good may seem like unlikely targets for hackers. After all, who would want to attack the tech resources, networks, and data repositories of these groups when there are so many for-profit organizations and government agencies to prey upon? Unfortunately, the answer is many people. The reality is that social enterprises are at particularly high risk for security breach. The reason, as recently stated in a Forbes.com editorial , is that hackers' typically infiltrate their victims' networks by searching for the weakest link as the initial point of entry to their ultimate target [6].

The hackers usually looking for connections between organizations, making some kind of networks and then attacking the weakest node of this network. That is why even if it's organization with no profit and with 1 man working there it could be target.

The main question we will want to answer is what modern social entrepreneur should know about cybersecurity. We would like to start with developing of criteria of protection from cyber threats. Of course, the whole package of criteria would be depend on specific of every enterprise working, but the general idea will be the same.

What we should protect and how we can do it?

First, we should identify all types of information storage and system, which we need to protect. It could be: paper documentation; electronic documentation; web-site; database; e-mail; accounts in different web-system, social media, etc.; local computer network (both:

wired and wireless), staff, pen-drives, laptops and other electronic devices (especially if staff take this devices home after work), etc. All of this storage we can divide in two groups: **internal** storage, if you need to access inside the building to get information and **external** storage, if you can get remote access to the information.

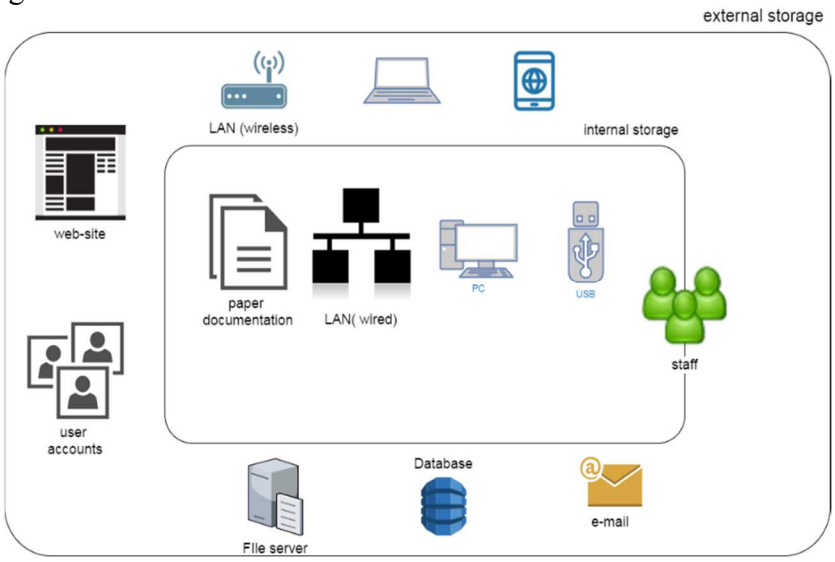

Fig. 2. Types of storage

Source: created by authors.

Then we should determine the value of information on each of this storage. For that, we should answer this simple question, what we will loss if:

1. Somebody (for example our concurrent) will get this information?
2. We just lost all this information.
3. Somebody take this information, modify it and give it to third person as original information. It`s mean that third person will have the information, which can confirm the truthfulness (for example, to receive a digital signature).

The answer should cover finance, reputation and relations side.

The most important, finance side we will count as sum of all possible losses we get if event will occur. The result will be the determination of the financial value of information as quantitative indicator (V).

After that, if it is possible, we should create coefficient of value (K) (Table) for all types of storage from 0 to 1. Where 0 – no losses in case of unauthorized access 1 – destruction of an enterprise in short period after unauthorized access. In this case, if the coefficient is close to 0, it can be neglected.

Table

Criteria for protection against cyber threats

V (finance value of information)	K coefficient of value	Event	P Probability of occurrence the event	R Resources for ensure complete safety	Type of storage
*	1	Loss all information from file server	0.1	*	internal
…	…	…	…	…	…

Next step is to determine the probability of occurrence some event (P) that could happens with every type of storage. This is the most complicated and long-term phase. To achieve our goal, we will use the concept of risk. The risk will be considered as the probability of causing loss with taking into account its severity. The economic aspect of risk is determined by the

fact that it determines the quantitative measure (probability) of causing damage (loss) as a result of the manifestation of certain dangers [4]. We plan to calculate the probability of occurrence of an event using quantitative analysis and modeling of dangers. Algorithm:

1. A quantitative analysis of dangers always begins with a preliminary study, the main purpose of which is to identify the source of danger.

2. The identification of sources of danger, the study of the development of danger and its analysis are mandatory components of the methodology, called the previous analysis of dangers (PAD).

3. Conducting the PAD in practical terms is simplified and formalized through the use of pre-prepared questionnaires, special questionnaires, tables, matrices of preliminary analysis, etc.

4. The most effective and generally accepted methods of quantitative analysis of dangers include the construction of models in the form of a tree of events (TE) and failure trees (FT).

5. When constructing TEs and FTs it is accepted to use special symbols that facilitate the perception of the analyst performed graphic constructions.

6. Event tree (TE) is a logical sequence of the most significant reactions of the physical system (technical device) to the initiating (output) events.

7. The analysis of the TE ensures the sequence of events leading to success, and at the same time, identifies an alternate sequence of events that result in the failure of the technical device and failures in the technical systems.

8. The disadvantages of the TE model are manifested when there are parallel sequences available.

Event-analysis of ACTION is not sufficiently effective in the detailed study of complex multi-element systems.

9. Tree failure (FT) - these are presented in a logical sequence possible failures, failures of the physical system (technical device), which are the causes of an unwanted major event.

10. The main undesirable event is taken to bring to the top of the tree of failure. Then, moving from the root to the top of the FT, you can detect the logical combination of events that causes the main undesirable event located at the top of the tree.

11. FT can detect all possible combinations of failures of individual elements of a complex system, the result of which is the main undesirable event.

12. The disadvantage of the FT model is too large and cumbersome construction, which requires considerable resources and time to analyze.

13. In the case of complex or multi-element systems, a qualitative analysis of hazards requires the simultaneous construction of both the model of the FT and the model of the TE. During the analysis of the dangers, the analyst performs numerous transitions from the FT to the TE and back - until both models will adequately reflect the investigated physical system (technical device).

14. FT and TE models are widely used in specially designed computer threat analysis programs.

15. The complexity of the analysis of hazards is often due to the fact that the main undesirable event is caused by a set of primary events.

For the last, we need to find how many resources we need to cover all expenses we need to ensure complete safety for all type of storage.

Conclusions. As a result, we will get the table of criteria we will use for developing system of cybersecurity at social enterprise.

References

1. Biggest cybersecurity threats in 2016 (2016). *CNBC*. Retrieved from https://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

2. Internet Security Threat Report ISTR (2017). *Symantec*. Retrieved from https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf?aid=elq_&om_sem_kw=elq_17978439&om_ext_cid=biz_email_elq_.

3. Companies that Went Out of Business Due to a Security Breach (2014). *Pro OnCall Technologies*. Retrieved from https://prooncall.com/3-companies-went-business-due-security-breach.

4. Tkach, Yu. M., Kazmirchuk, S. V., Mekhed, D. B., Bazylevych, V. M. (2017). Zastosuvannia metodu ekspertnykh otsinok do otsiniuvannia informatsiinykh ryzykiv vyshchoho navchalnoho zakladu [Application of the expert estimation method to the assessment of information risks of a higher educational institution]. *Zakhyst informatsii – Information protection, 2*, 137–142 [in Ukrainian].

5. Shkarlet, S. M. (2007). *Ekonomichna bezpeka pidpryiemstva: innovatsiinyi aspekt [Economic security of an enterprise: an innovative aspect]*. Kyiv: NAU [in Ukrainian].

6. Social Enterprises: A Hackers Favorite Target (2015). *Lunarline*. Retrieved from https://lunarline.com/blog/2015/01/social-enterprises-hackers-favorite-target.

References (in language original)

1. Biggest cybersecurity threats in 2016 [Electronic resource] // CNBC. – 2016. – Access mode : https://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

2. Internet Security Threat Report ISTR [Electronic resource] // Symantec. – 2017. – Access mode : https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf?aid=elq_&om_sem_kw=elq_17978439&om_ext_cid=biz_email_elq_.

3. Companies that Went Out of Business Due to a Security Breach [Electronic resource] // Pro OnCall Technologies. – 2014. – Access mode : https://prooncall.com/3-companies-went-business-due-security-breach.

4. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу / Ю. М. Ткач, С. В. Казмірчук, Д. Б. Мехед, В. М. Базилевич // Захист інформації. – 2017. – № 2. – С. 137–142.

5. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект : монографія / С. М. Шкарлет. – К. : Вид-во НАУ, 2007. – 436 с.

6. Social Enterprises: A Hackers Favorite Target [Electronic resource] // Lunarline. – 2015. – Access mode : https://lunarline.com/blog/2015/01/social-enterprises-hackers-favorite-target.

УДК 004.056.5

Володимир Базилевич, Дмитро Мехед, Володимир Гур'єв

РОЗРОБКА КРИТЕРІЇВ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ НА СОЦІАЛЬНОМУ ПІДПРИЄМСТВІ

Актуальність теми дослідження. *Питання створення системи захисту від кіберзагроз сьогодні стає нагальним. Постійно зростаюча кількість кібератак є цьому підтвердженням.*

Постановка проблеми. *Більшість підприємств, особливо невеликих, не можуть собі дозволити утримання спеціалізованого відділу, або навіть аутсирсингову компанію для реалізації систем захисту. У такому контексті формулювання загальних критеріїв захисту може вирішити цю проблему.*

Аналіз останніх досліджень та публікацій. *Були розглянуті останні публікації у відкритому доступі, статистичні дані, звіти корпорацій.*

Виділення недосліджених частин загальної проблеми. *Адаптування критеріїв захисту від кіберзагроз для соціального підприємства. Чи соціальні підприємства більш вразливі до кіберзагроз і якщо так, то чому? Які критерії більш важливі, а якими можна знехтувати?*

Постановка завдання. *Розробити адаптовані критерії захисту від кіберзагроз, які можуть бути використані при створенні системи захисту на соціальному підприємстві.*

Виклад основного матеріалу. *Проаналізовано типи та статистику кіберзагроз. Побудовано таблицю критеріїв, яка включає: фінансову цінність інформації, коефіцієнт цінності, подія, ймовірність настання події, кількість ресурсів, необхідних для забезпечення повної безпеки, тип пристрою зберігання інформації.*

Висновки відповідно до статті. *Запропоновані критерії дозволяють створювати адаптовані та уніфіковані системи захисту від кібрзагроз.*

Ключові слова: *кіберзагрози; соціальне підприємництво; критерії захисту; цінність інформації; типи пристроїв зберігання даних; бази даних.*

Рис.: 2. Табл.: 1. Бібл.: 6.

Bazylevych Volodymyr – PhD in Economics, Associate Professor of Department of cybersecurity and mathematical simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Базилевич Володимир Маркович – кандидат економічних наук, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: bazvlamar@gmail.com
ORCID: http://orcid.org/0000-0001-8935-446X
ResearcherID: G-5764-2014
Scopus Author ID: 57193029322

Mekhed Dmytro – PhD in Pedagogy, Associate Professor of Department of cybersecurity and mathematical simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Мехед Дмитро Борисович – кандидат педагогічних наук, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: d.mekhed@gmail.com
ORCID: http://orcid.org/0000-0003-3905-3620
ResearcherID: H-1751-2016
Scopus Author ID: 57193823626

Guryev Volodymyr – PhD in Technology, Professor of Department of cybersecurity and mathematical simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Гур'єв Володимир Іванович – кандидат технічних наук, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: bazvlamar@gmail.com
ORCID: http://orcid.org/0000-0001-9507-5408
ResearcherID: G-9807-2016