DOI:
UDC: 141.7: [355.014: 172]

Serhii Lysenko,
Doctor of Law, Professor, PJSC "Higher Education Institution "Interregional Academy of Personnel Management", Head of the cathedra of Jurisprudence by Severodonetsk Institute, Kyiv, Ukraine,
e-mail: sl-bezpeka@iapm.edu.ua,
ORCID: 0000-0002-7050-5536

MODERN INFORMATION SECURITY ANALYSIS: INTEGRATION OF BEST PRACTICES AND TECHNOLOGIES INTO ADMINISTRATIVE AND LEGAL MEASURES

The article is devoted to modern approaches to the analysis of information security and the search for the most effective practices and technologies for countering threats using administrative and legal measures. The article proposes an information security concept based on several advanced administrative and legal measures, which includes an examination of a number of threat response cycles and with a direct attack on the protected object.

Given the high dynamics of modern information processes and the accompanying information threats, it is necessary to have such a complex of measures to counter threats, which would allow not only to respond to threats, but also to predict them. The author, referring to the approaches of the Nobel laureate in economics Daniel Kahneman, on the distribution of decisions into "fast" and "slow", suggests combining the response to attacks with the accumulation of information, for the subsequent identification of the most unprotected elements and predicting future attacks. In particular, the proposed process of responding to attacks, which consists of the following stages of administrative and legal measures: preparation; identification and analysis; localization, elimination of the threat; recovery of activity after an incident. Attention is focused on the need, after the expiration of this four-step algorithm, to consider the initial data for subsequent use in each appropriate period when repeating the cycle.

Special attention is devoted to the importance of transmitting data on unlawful attacks to the information collection system, which requires careful planning and coordination between numerous operations and structures. Such a process usually occurs due to well-coordinated administrative and legal measures in organizations, regulated by corporate norms, based on current legislation.

Keywords: *information security, information threats, administrative and legal measures, forecasting information threats, information and analytical activities.*

Анотація. Лисенко С.О. Сучасний аналіз безпеки: інтеграція кращих практик і технологій в адміністративні та законодавчі заходи. *Стаття присвячена сучасним підходам до аналізу інформаційної безпеки та пошуку най-*

більш дієвих практик і технологій протидії загрозам із застосуванням адміністративно-правових заходів. У статті запропоновано концепцію інформаційної безпеки, засновану на кількох передових адміністративно-правових заходах, яка включає огляд ряду циклів реагування на загрози та при безпосередньому нападі на об'єкт захисту.

З огляду на високу динаміку сучасних інформаційних процесів та супутніх їм інформаційних загроз, необхідним є такий комплекс заходів протидії загрозам, який дозволяв би не тільки реагувати на загрози, але й прогнозувати їх. Автор, посилаючись на підходи Нобелівського лауреата з економіки Даніела Канемана, щодо розподілу рішень на «швидкі» та «повільні», пропонує поєднати реакцію на атаки з накопиченням інформації, для подальшого виявлення найбільш незахищених елементів та прогнозування майбутніх атак. Зокрема, запропоновано процес реагування на атаки, який складається з наступних етапів адміністративно-правових заходів: підготовка; виявлення і аналіз; локалізація та ліквідація загрози; відновлення діяльності після події. Акцентовано увагу на необхідність, після закінчення цього чотириступінчастого алгоритму, врахування вихідних даних для подальшого використання у кожному відповідному періоді при повторі циклу.

Окрему увагу присвячено важливості передачі даних про протиправні напади до системи збору інформації, що вимагає ретельного планування і координації між численними операціями і структурами. Такий процес зазвичай відбувається завдяки злагодженим адміністративно-правовим заходам в організаціях, які регламентуються корпоративними нормами, на основі діючого законодавства.

Ключові слова: *інформаційна безпека, інформаційні загрози, адміністративно-правові заходи, прогнозування інформаційних загроз, інформаційно-аналітична діяльність.*

Relevance of the research topic

The modern threat scene is more complex and dynamic than ever before. Organizations are often attacked by aggressors with different skills, using a different set of tools that are improved daily. Control measures aimed at protecting the organization, which worked so well yesterday, may not be able to prevent the attack of the same attackers the next day, because weaknesses and strengths are not static, and are often the result of an attack when it is too late to counter. In such a complex environment, it would seem that it would be possible to abandon attempts to create a list of priorities for protection, to recognize the fallacy of this approach to "protection of priorities" and try to protect everything at once.

However, those who practice risk analysis will quite rightly say that there is an advantage in nuances, namely in the priority of information assets that are protected, because there are always too many things to keep and too few administrative and legal mechanisms through which they can be protected. Even exceptionally large financial institutions, with virtually unlimited budgets, are still forced to compete with other organizations for specialists, and time for them, unfortunately, will always remain a

limited resource[1] [1]. This truth is verified by centuries of research by theorists of philosophy, politics, and military thought. "He who protects everything does not protect anything," said King Frederick II of Prussia. It has always been and will always be necessary to identify the priorities that need to be protected and to determine the scope and content of the resources needed for such protection.

Setting the tasks

Against this background, organizations, for more effective risk management, first it is advantageous to introduce such administrative and legal measures aimed at the use of data on threats possessed by information security services. Similar measures will better train professionals in the collection of external information, which, among other things, may be better suited to protect the organization if they use data on probable risks collected in advance. Such a combination of collected data on threats and risks, in our opinion, should form the basis of a model of administrative and legal measures to combat them. Such a model should be the result of a combination of several different algorithms that differ in their goals but have so much in common that their interaction is mutually beneficial.

Analysis of recent research and publications

The process of responding to attacks consists of the following stages of administrative and legal measures: preparation; detection and analysis; localization, threat elimination; resumption of activities after the event. At the end of this four-step algorithm, the original data should be considered for further use in each period when repeating the cycle. Interestingly, this cycle is somewhat reminiscent of the classical understanding of management functions. At one time, M. Mescon, M. Albert and F. Hedouri proposed to consider four main functions of management: planning, organization, motivation, and control[2] [2, p. 131]. At the same time, it can be only about the interpenetration of these stages of administrative and legal measures and management functions, but not about their duplication. After all, say, control is a necessary component of success in the process of preparation, detection, and analysis, and during localization, elimination and resumption of activities after the event.

Responding to attacks is one of those administrative and legal processes that benefits from proper planning, and it is the first phase that describes it very accurately. In this case, the organization, according to the administrative and legal measures taken, will develop the resources needed for a proper response. This may include acquiring the right technology to aid, setting up computing assets to provide appropriate evidence in the event of an attack, and setting the right signals to alert personnel that an attack has occurred. Finally, this stage of the administrative process includes the involvement and training of relevant personnel to use administrative and legal resources, opportunities, and processes in the event of a confirmed attack[3] [3]. It is the first stage, in our opinion, is the most important, because its successful implementation

[1] Varenko, V.M. (2014). Information and analytical activities. Kyiv: University "Ukraine".

[2] Vologin, Y. (2011). Formation and development of management as a science in modern market economy. Youth and the Market, 8 (79), 129-133.

[3] Kai-fu, Lee. AI. (2020). Superpowers of artificial intelligence. Kyiv, BookChef.

allows you to take the most advantageous position, thereby increasing the probability of success of subsequent stages. Instead, the failure of the first stage, or the lack of response at this stage is exceedingly difficult, and sometimes impossible to compensate in the future.

Presentation of the main materials of the study

The second phase - "detection and analysis" - regulates the need for early information about the threat in the organization. First, this requires the presence of people who collect information and technicians who are able to analyze the information selected by a number of reference indicators, to determine the priority of action at each subsequent stage. A characteristic feature of the stage is the relatively high degree of both positive and negative results that can be obtained from monitoring and making administrative and legal decisions. In this case, the most developed organizations set a priority rating scale that allows you to quickly classify the information obtained and respond quickly to certain changes in indicators. Such prioritization is an excellent opportunity for administrative and legal regulation of the risk analysis process, as knowledge of the correct risk-based priorities at an early stage of response to attacks is crucial for further management optimization.

The third phase of the algorithm involves the implementation of administrative and legal measures aimed at localization and complete cessation of the attack. This means, first of all, restricting the spread of the attack, stopping the attacker, his equipment and malware from accessing the objects of protection, as well as stopping the exchange of data that have been attacked and could be damaged. Of course, the most typical situations are when it comes to data theft (personal information, financial details, information with limited access, etc.), or the destruction of valuable information. However, it should be noted that one of the causes of the attack may be the infliction of indirect damage to the object. For example - it may be a substitution of certain data (statistical reporting, information that can be further analyzed) to further mislead the management of the institution, or, in general - to draw attention to a particular data set. It is easy to simulate a situation in which attackers first launch an "information bomb" (for example, misinformation about the activities of valuable employees or partner organizations, true or fictitious compromising information on them), and only then, in another way, inspire an attack on related datasets. . In this case, the purpose of the attack will not be to steal any information (which can be done to distract the security service, giving its experts a false sense of understanding the situation) but to draw the attention of both security and management to a pre-prepared "surprise". At the same time, the double or even triple benefit of such an attack cannot be ruled out (for example, an attack can steal valuable information, damage other important information and at the same time draw the attention of the management of the "object of attack" to pre-posted misinformation).

This stage of action also involves restoring the information security system and returning it to the state in which it was before the attack. At this stage of the algorithm, data and evidence should be collected for possible transfer to law enforcement

agencies or human resources departments and legal services to decide on further administrative and legal measures.

The final phase of the attack response algorithm tunes in for integration with other participants. In this regard, you should carefully collect data and prepare the information for use. This may also include a forecast that can be used by other professionals to determine exactly where weaknesses are found in the organization and, accordingly, similar attacks can be expected in the future. The preventive component of the final phase involves planning further administrative and legal measures that will help prevent the recurrence of such events.

These algorithms in practice are designed not only to minimize the threat of attack, but also to turn it into a set of information for further optimization of the administrative-legal scheme. The level to which activities are achieved in the organization may mean eliminating technical details but will always include a description that summarizes what happened, turning it into material that helps decision-makers understand what happened. Due to this, the statements of analysts about the necessary administrative and legal actions are gaining due credibility. The information can and should be used as baseline input to help prepare for repelling the next attack. This in-house intelligence on threats can also be used, along with similar externally generated information on potential threats, as a critical contribution to the next cycle of attacks. Sometimes such information is included in the array of collection and processing of information security data of the organization [3].

Threat analysis is a systemic process, as Nobel laureate Daniel Kahneman points out in his book, Think Fast and Slow. To summarize the researcher, in this book he describes in detail the types of decisions made by people, and groups them into two categories: 1) quick decisions that protect us from harm and meet the needs of a lower level in the hierarchy of Maslow's needs; 2) slow (thoughtful) decisions that come as a result of spending time thinking about the causes and consequences, the application of the correct model of information security to analyse the results[4] [4]. The thinking of the first category is so simple and fast that we often resort to it subconsciously, which helps to escape when we are directly under threat. Such a model of action can lead to a poor choice of administrative and legal measures at best, and to conflict and devastating consequences at worst. However, when quick decisions are needed, a situation often arises where even the wrong quick decision will be less harmful than inaction. However, strategically, without a doubt, threat investigation should be aimed at eliminating bias in the process of gathering information, which will allow to come to the most accurate and correct balanced (slow) decision.

The general threat intelligence algorithm proposed by Crisan at the Joint Military Intelligence College of the United States provides us with an algorithm designed to ensure a continuous process of developing administrative and legal decisions on urgent issues5 [5]. The first step in this algorithm is to fully understand what questions need

[4] Daniel Kahneman (2017). Thinking fast and slow. Kyiv: Our format.

[5] Levchuk, N. (2018). Development of economic competence of undergraduate officers of the State Border Guard Service of Ukraine. Dissertation. Khmelnytskyi.

to be answered during threat intelligence and why. Next, you need expert judgment as to what data needs to be collected to answer these questions. This phase should be well known to any researcher, as it precedes any research project.

The second step is simply collecting certain data or, sometimes, even simply identifying where that data may come from, and launching the technologies and processes needed to generate and collect that data. At this stage, as soon as the necessary data are collected, the specialist analyses them, processes, and converts this source data into information that can be used in practice [5]. In fact, this means the introduction of administrative and legal measures based on different media. By analogy with the attack response algorithm, this involves identifying facts, conclusions, and predictions about what to expect next. After all, this information is disseminated in various places, including by risk and threat analysts. In our scheme, this algorithm is between the stage of responding to the attack and the stage of risk analysis, and therefore it contributes to each of them. This allows us to manage threats and risks separately, but at the same time provide each administrative and legal measure with the information necessary for the smooth operation of information security of the organization. The relevance of this approach will continue to grow, given the spread of e-government technologies6 [6]. Even today, it is possible to practically guarantee the interest of criminals in this area of activity.

In general, risk analysis is less sensitive to administrative and legal measures to protect against threats than intelligence. The main reason for this, in our opinion, is that despite the possibility of the existence of different and numerous ways in which a spy can find his way into the information environment of the organization, the risk is usually more fixed.

For example, an attacker's ability to exploit vulnerabilities in an organization's outlet information systems may change over time, but the outcome is likely to be the same. There are several variables that are needed for risk analysis (especially quantitative variables), and they are included in our review. In general, it is useful to think of the risk analysis phase as an abstraction of the details required for the daily implementation of administrative and legal measures in solving information security problems.

Added threat information is used as input required for risk analysis. This information is characterized by two variables that are often used by attackers when it comes to internal personnel. The first is information about how often they make mistakes and when they do it. And secondly - what resources they can use in case of error, to avoid liability. A concomitant variable can be a community profile, which serves as a universal tool for communication in the organization. It helps to determine detailed information about the goals and objectives of the attackers.

For example, if aggressors can threaten their attacks in terms of time, skills, and resources, they can be said to be the most dangerous (say - 99%). Thus, the danger in them will be 99%. These values should also be stored along with threat data so that

[6] Romanenko, Y. O., & Chaplay, I. V. (2016). Marketing communication system within public administration mechanisms. Actual Problems of Economics, 178 (4), 69-78.

professionals can clearly and timely communicate what these attackers are to their organizations. It is important to note that attribution is not a prerequisite for creating threat profiles for risk analysis. Indeed, establishing attribution is an incredibly difficult and relatively unnecessary task for risk analysis purposes. It is more important to rely on the assessment, which states that a certain type of attack was correlated with the level of information security of the organization. The only valuable question is whether this type of attack is part of the actions of a broader, abstract group of attackers.

After completing several cycles of risk analysis, the organization will receive a list of options for the highest threats. It is important to note that they are formed when there is complete information about losses, including threats, weaknesses in control and the type of economic impact (according to CIA guidelines). These predictions of maximum losses can be used in conjunction with attack data to focus the organization on the main actions by which attackers or insiders can carry out their attacks[7] [7].

In summary, it should be noted that each of the previous algorithms has its advantages and usefulness for different administrative and legal measures of information security of the organization. Combining them together allows us to see the big picture from the organization's data collection. It is possible to observe how exactly these algorithms interact and what administrative and legal measures can be mutually beneficial for each of the specific management decisions.

Conclusions

Most often, there is a certain distance between management functions, risks, taking administrative and legal measures and information collection specialists. And this is no accident. Each function is quite different in nature. However, only a comprehensive interaction of all these components of information security allows us to better understand the role of each of them, and better understand the reality of the threats that everyone deals with in everyday life.

Risk management teams need both professionals in the legal field and specialists in threat and risk assessment. The use of the information attack data collection system as an administrative measure gives each group clear rights and responsibilities. This can stimulate interaction where it may not have been before and create professional commitments that will allow for more effective collaboration and, as a result, improve the quality of the team's information products.

Many organizations are working to improve their information security reporting to their management and boards of directors. For these organizations, finding the right administrative and legal measures that can lead to a good result, as well as neutralizing potential losses in the information space, is one of the key tasks. Tight regulation of instructions and certain steps of participants by corporate norms, and finally - the adoption of administrative and legal measures and the exchange of data between performers, can not only help to summarize and optimize approaches to their daily

[7] Lysenko, S. (2019). Information security: the genesis of principles and approaches on the example of studies of the classics of military thought. International Scientific Journal "Rule of Law", 2, 184-192.

activities, but also bring the greatest effectiveness of measures. In addition, it should be borne in mind that the implemented administrative and legal measures must comply with the principles of balance and equilibrium between the actions of state bodies and the organization's own information security specialists.

References

Varenko, V.M. (2014). Information and analytical activities. Kyiv: University "Ukraine".

Vologin, Y. (2011). Formation and development of management as a science in modern market economy. Youth and the Market, 8 (79), 129-133.

Kai-fu, Lee. AI. (2020). Superpowers of artificial intelligence. Kyiv, BookChef.

Daniel Kahneman (2017). Thinking fast and slow. Kyiv: Our format.

Levchuk, N. (2018). Development of economic competence of undergraduate officers of the State Border Guard Service of Ukraine. Dissertation. Khmelnytskyi.

Romanenko, Y. O., & Chaplay, I. V. (2016). Marketing communication system within public administration mechanisms. Actual Problems of Economics, 178 (4), 69-78.

Lysenko, S. (2019). Information security: the genesis of principles and approaches on the example of studies of the classics of military thought. International Scientific Journal "Rule of Law", 2, 184-192.