DOI: 10.15587/978-617-7319-98-5.CH2

Svitlana Onyshchenko, Alina Yanko,
Alina Hlushko, Oleksandra Maslii

CHAPTER 2

ECONOMIC CYBER SECURITY OF BUSINESS IN UKRAINE: STRATEGIC DIRECTIONS AND IMPLEMENTATION MECHANISM

ABSTRACT

The study is devoted to the determination of strategic directions for ensuring the economic cyber security of business in Ukraine. The importance of information protection in the context of the development of the digital economy has been updated. The place of economic cyber security in the national security system is determined. A thorough analysis of the dynamics of cyber incidents in the world in recent years has been conducted. The specifics of the manifestation of cyber threats at the macro and micro levels are outlined. Qualitative changes in the state policy of Ukraine in the aspect of ensuring information and cyber security have been studied. A number of the most relevant risks and threats to the economic cyber security of business in 2023 have been identified. The need for business entities to develop an effective internal policy of cyber protection of computer networks against attacks, intrusions and unauthorized access is proven. The modern trends of cyber threats are studied and the cyber security policy strategy of business entities in Ukraine is described.

Special attention is paid to the intrusion detection process. The working principles of modern intrusion detection and prevention systems have been studied in detail. Behavioral analytics of UEBA users and objects were considered to detect violations in the field of security. On the basis of Microsoft's Advanced Threat Analytics (ATA), the process of monitoring network traffic of domain controllers was considered, with the aim of detecting cyber-attacks. Using Azure Security Center as an example, it explores intelligent security tools and expanding analytics to detect threats faster and reduce the number of false security alerts. Using the proposed cybersecurity policy recommendations will significantly increase the level of business information security (confidentiality, integrity, and availability).

KEYWORDS

Economic cyber security, information security, national economy, business, cyber security infrastructure, computer network, intrusion detection systems, unauthorized access, intrusion prevention system, cyber security strategy, security center.

The global processes of information technology development have become a determinant of the development of the digital economy and a powerful tool for global economic growth. On the one hand, the digitalization of all spheres of public life allowed maximizing the benefits of the state, business and citizens in connection with increasing the efficiency and effectiveness of operations, information exchange, but on the other hand, it caused an increase in risks associated with receiving financial and reputational losses as a result cybercriminal activities. The urgency of the problem of protecting cyberspace in the context of the development of artificial intelligence systems is due to the growth of cyber incidents both in the national and in the global information space. Interference and destabilization of information systems, theft of confidential information are cyber threats that are modified every day and require business entities to build effective protection systems. In this regard, the need to develop a cyber security policy and a mechanism for its implementation at the micro level, which will minimize cyber security risks for business in Ukraine, is gaining indisputable relevance.

The research was supported by the Ministry of Education and Science of Ukraine and performed the results of the project 0122U001749 "The formation of organizational and economic principles for the prevention of threats to the social and economic security of Ukraine in the conditions of a pandemic".

2.1 RISKS AND THREATS TO ECONOMIC CYBER SECURITY OF BUSINESS

The development of the digital economy in recent decades is a strategic direction of the world's leading countries. In this regard, the current stage of society's development is characterized by the integration of security aspects of economic and information processes, which requires the transition of the management system at both the macro and micro levels to a qualitatively new level.

The digital economy is a type of economy in which digital data are the key factors of production. Their use as a resource makes it possible to significantly increase the efficiency, productivity, value of services and goods, to build a digital society.

To date, the size of the digital economy, according to various estimates, is from 15.5 % to 17.5 % of world GDP. Almost 40 % of the added value created in the global sector of information and communication technologies is accounted for by the United States and China. It is predicted that by 2030 the share of the digital economy in the GDP of the world's largest countries will reach 50–60 % [1, 2].

One of the indicators that characterizes the development of the digital economy is the International Digital Economy and Society Index (I-DESI), which is based on a comparative analysis of the digital efficiency indicators of EU member states and 19 other countries of the world (Australia, Albania, Bosnia and Herzegovina, Brazil, Canada, Chile, Iceland, Israel, Japan, Mexico, Montenegro, North Macedonia, Norway, Serbia, South Korea, Switzerland, Turkey, United Kingdom, and the United States) [3]. According to the results of 2022, the EU-27 member states are in the first five positions out of the 10 TOP in the I-DESI index. Overall index scores remain higher for non-EU countries than for EU-27 member states in each year. Denmark had the highest I-DESI score. It was also the leading country in the EU according to the 2021 DESI index. Iceland became the leading country outside the EU (**Fig. 2.1**).

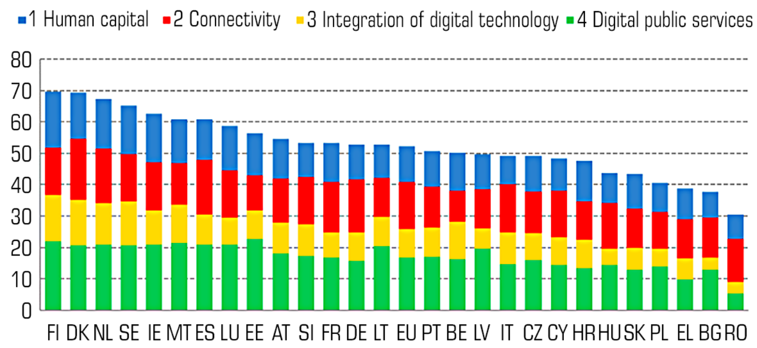


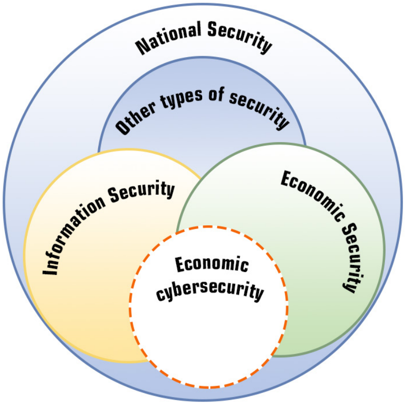
Fig. 2.1 Digital Economy and Society Index, 2022
Note: compiled by the authors according to [4]

In general, in developed countries, the level of cyber security and indicators of the development of the digital economy are on average higher than in developing countries.

Regarding the level of digitization of the economy of Ukraine, it is possible to note a significant difference in various industries. In particular, in the field of financial services, communication services, and logistics, national business entities use digital technologies on a par with global competitors [5]. Along with a number of advantages, this creates new risks for Ukrainian business, including threats to cyber security, and requires an appropriate response and a systemic approach from both the state and business entities.

State policy is usually manifested in two main aspects – state support for development (concepts, strategies, doctrines, state programs) and state regulation of relations (legislative acts) [6]. It is appropriate to note that starting from 2021, from the moment of adoption of the Information Security Strategy of Ukraine and the Cyber Security Strategy of Ukraine, the foundations were laid for the development of effective mechanisms for countering threats to the national economy in the information sphere, including in cyberspace. The information security strategy of Ukraine outlines the need to strengthen the capabilities to ensure the information security of the state, its information space, support with information means and measures of social and political stability, state defense, protection of state sovereignty, territorial integrity of Ukraine [7]. The cyber security strategy defines Ukraine's urgent need to ensure socio-economic development in the digital world, which requires the acquisition of the ability to effectively deter destructive actions in cyberspace, the achievement of cyber resilience at all levels, and the interaction of all cyber security actors [8].

Taking into account the provisions of the strategies and other legal acts, it is legitimate to outline the place of cyber security of the economic sphere in the national security system (**Fig. 2.2**).



⬡ **Fig. 2.2** Economic cyber security in the national security system

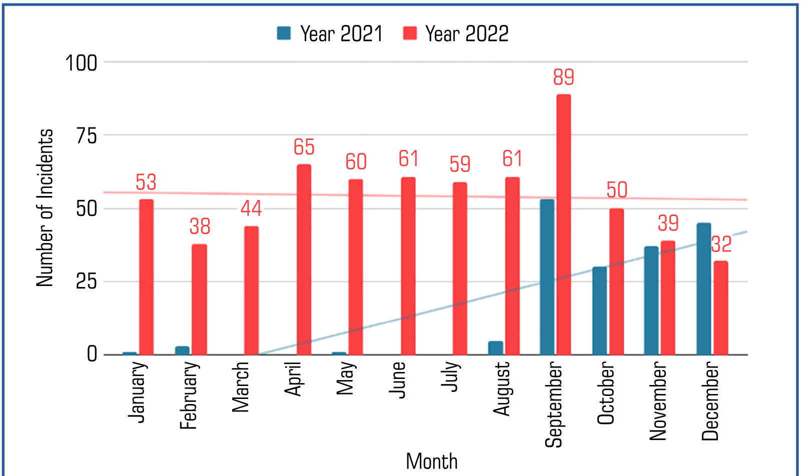
Therefore, national security must be considered taking into account the processes of digitalization, which have radically changed the paradigm of socio-economic development. The latest economic processes in cyberspace require adequate security measures. Economic cyber security occupies a special place in the national security system, because cybercrimes in the form of cyber espionage (theft of information about the latest technological developments, financial transactions, etc.) and cyber-attacks can cause irreparable damage to strategically important objects of both the public and private sectors. This is confirmed by official static data.

The public sector became the main target for cybercriminals in 2022: the number of attacks on this sector increased by 95 % in the second half of 2022 compared to the same period in 2021 (**Fig. 2.3**).

The increase in digitalization brought about by COVID-19 has not only increased the attack surface for attackers, but has also allowed countries to use cyberwarfare as a tool to attack other countries.

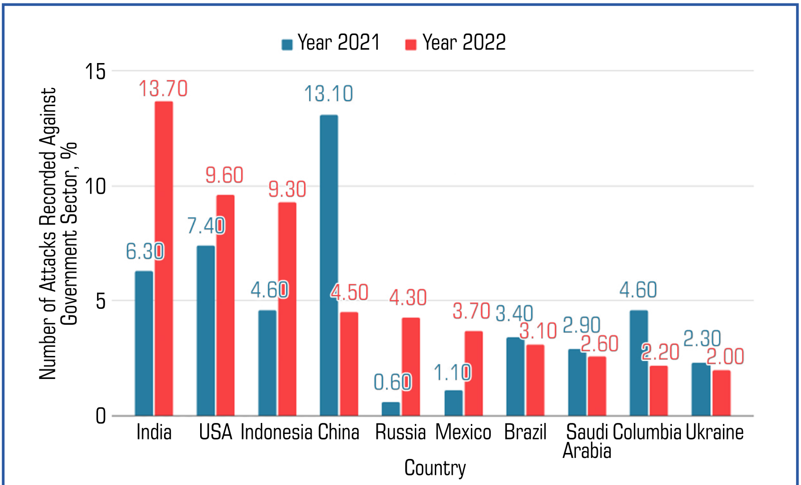
In recent years, India, the USA, Indonesia and China have remained the main target countries for cyber-attacks (**Fig. 2.4**). Together, these four countries account for about 40 % of the total number of public sector incident reports.

The Russian Federation's full-scale invasion of Ukraine was accompanied by coordinated cyber-attacks on state institutions and critical infrastructure facilities. At the same time, the number of cyberattacks against Russia increased by more than 600 % in support of Ukraine by activists.



⬡ **Fig. 2.3** Number of cyber incidents targeting the government sector recorded in the past two years by month

Note: compiled by the authors according to [9, 10]



⬡ **Fig. 2.4** Number of cyber incidents targeting the government sector recorded in the past two years by country

Note: compiled by the authors according to [9, 10]

The high level of development of cyberspace and the organization of cyber threats indicates the need to change the paradigm of cyber security strategy: it should be based not on responding to the fact, but on the principles of forecasting and planning protection against future actions of cybercriminals. For this, it is necessary to constantly analyze modern trends in economic cyber threats [11].

At the macro level, the most dangerous trend is the use of cyber weapons in conflicts between countries, which is taking on new forms. Cyberactivity plays a leading role in this destructive dialogue. Attacks on critical infrastructure and purposeful destabilization of the Internet in certain countries open a new era of cyber-attacks.

The main cyber threats to business, i.e. the micro level, can rightly be identified as the following:

1. Phishing is one of the most common types of cybercrime, which leads to countless financial losses every year. The goal is to steal sensitive data and credentials, such as login credentials or credit card details, and trick people into allowing malware to be installed.

2. Malware – hackers develop malware to have persistent backdoor access to company devices that is difficult to detect. They can then remotely control the device and use it to steal data, explore the local network, or send spam from the infected device. 91 % of cyber-attacks start with a phishing email, so phishing and malware are closely related.

3. Ransomware – this form of malware can cause catastrophic damage to a business. Ransomware blocks a firm's information system and deprives it of access to critical data until a ransom is paid to return sensitive information and regain control of the systems. Ransomware presents businesses with a difficult choice: pay the attackers or lose data and access to it. Most companies choose to pay hackers, but even when business owners pay the ransom, they don't always get access to their data.

4. Compromise of corporate e-mail (BEC – Business Email Compromise) is one of the most expensive cybercrimes. The process begins with criminals hacking business systems in order to gain access to information about their payment systems. They then deceive employees and encourage them to make payments to bogus bank accounts instead of real ones. Fake payment requests can be difficult to identify because they look almost identical to genuine requests. BEC can result in huge financial losses for a business and it can take months to track down and recover payment amounts, if at all.

5. Internal threats – some of the company's employees have access to confidential information. Whether they are current or former employees, partners or contractors, 25 % of data breaches are caused by insider threats. Unscrupulous employees act out of greed, or sometimes disgruntled employees act out of bitterness. In any case, their dissemination of important information can cause significant financial losses.

6. Inadvertent disclosure – employees may accidentally disclose confidential information and cause financial damage to the company. A mistake could be as simple as accidentally sending an email to everyone in the company. Companies with a large number of employees are at particular risk if employees have access to core databases.

7. Storage intelligence – companies store huge amounts of data in the cloud and believe that it is automatically protected. However, this is not always the case. Cybercriminals look to unsecured cloud storage to access and exploit data. Cloud interfaces are not always supported by

secure systems, making them easy prey for cybercriminals. Probably the most famous example of this is the breach of an unsecured cloud S3 bucket containing vast amounts of classified National Security Agency data. The data was breached in 2017 with serious consequences. Companies should be aware that the storage of confidential information can be risky if appropriate precautions are not taken.

8. Social engineering – involves the creation of fictitious persons and profiles by cybercriminals on social networks in order to gain the trust of their victims and obtain the information necessary to complete the operation. These relationships are used to achieve the ultimate goals of phishing and installing malware to disrupt businesses, gain access to company data, and gain financial gain. Any form of social interaction designed with the ultimate goal of deceiving a business can be classified as social engineering [12, 13].

Fig. 2.5 schematically presents threats to the cyber security of business entities according to the 2022 report on global IT risks from Cisco Talos. The main causes of the most expensive data leaks are related to the mentioned cyber-attacks [14].

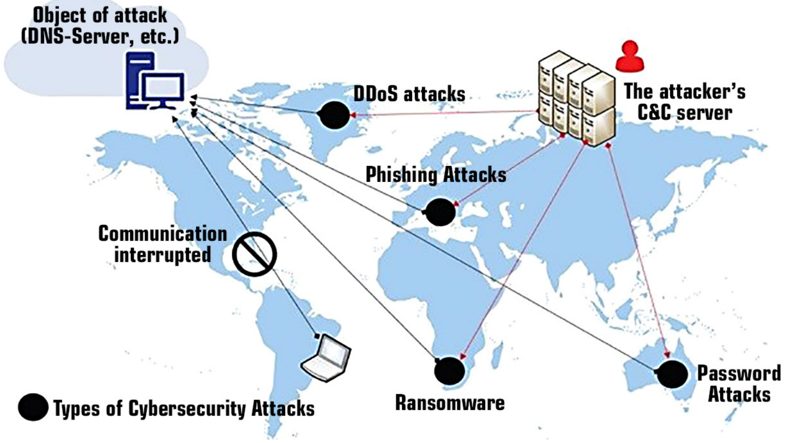


Fig. 2.5 The most common types of cyber attacks

Financial losses from cyber-attacks are difficult to estimate. However, according to approximate estimates of experts, the world economy will experience losses measured in trillions of US dollars. However, the greatest danger is not in the amount of money, but in the threat to the business. So, every fifth company that was subjected to a cyber-attack was forced to close its business. 48 % of companies experienced data or equipment loss, and of the 42 % that paid the ransom, a quarter did not receive the promised data [15].

The outlined risks and threats to the economic security of business require the implementation of effective mechanisms for their prevention and neutralization both at the level of the state [16] and at the level of business entities.

Taking into account the improvement of national legislation in the field of information and cyber security, it should also be noted that in February 2023, the Protective DNS system was implemented in Ukraine. It provides filtering of phishing sites, thus hindering the activities of cybercriminals, and Ukrainians have received additional protection from fraudsters on the Internet. When trying to go to a phishing site, Protective DNS redirects users to a page with a warning about the threat and recommendations on cyber hygiene. More than 320 Ukrainian providers have already joined the system, which are responsible for the security of their customers. Among them are the largest market players – Kyivstar, Lifecell, Vodafone, Ukrtelecom, Datagrup and Volya. In the first month of the system's operation, there are significant results – the volume of phishing fraud in monetary terms fell by approximately 40–50 %, and the number of appeals from defrauded citizens – by 30–40 %. In general, these are tens or even hundreds of millions of hryvnias every month, which Ukrainians will not lose thanks to the operation of the system [17].

Thus, in the aspect of ensuring economic cyber security, it is necessary to establish an exchange of information about cyber incidents and develop close cooperation of the state with scientific institutions and private companies, as well as international organizations. At the same time, at the level of business entities, it is necessary to develop individual cyber security strategies and mechanisms for their implementation.

2.2 CYBER SECURITY POLICY STRATEGY OF BUSINESS OF UKRAINE

The concept of security of any system is a complex concept that can be considered from different aspects and implemented in many ways and methods, but all active actions must be aimed at the constant security of both the system as a whole and its individual elements, which ensures the sustainable development of the system, timely detection, prevention and neutralization of real and potential threats. Today, in the era of digitalization of almost all spheres of the economy, it is necessary to pay special attention to the cyber security policy of economic entities [18]. In modern conditions, the problem of economic cyber security of Ukraine is intensifying in connection with military actions in the country, as well as the activation of European integration processes. This requires a review of existing concepts of cyber security at the level of business entities and improvement of priority ways of ensuring it. Since there are international standards that must be met if it is planned to become part of the EU in the future, for example, in 2016, the European Parliament adopted the General Data Protection Regulation (GDPR) [19]. Starting from the spring of 2018, according to the GDPR, companies are obliged to:

– report information leaks;

– appoint a person responsible for data protection;

– ask for user permission for data processing;

– make the data anonymous to preserve privacy [20].

All organizations operating on the territory of the European Union must comply with these standards.

Business security in the information space is most necessary to be considered from the point of view of protection against various types of attacks and prevention of existing cyber threats, that is, against unauthorized access.

An analysis of current trends shows that over time, hacker attacks have proven to cyber security experts that attackers (hackers) can be persistent, more creative and increasingly sophisticated in their attacks. Attackers have learned to adapt to changes in the IT landscape in order to always act effectively when launching an attack. Although there is no Moore's Law or its equivalent in the context of cyberattacks, it can be said that hacking methods are becoming more sophisticated every year.

In the last few years, there has been a trend towards better attacks and methods of their implementation, therefore the internal information and cyber security policy of any business entity must be effective, flexible and dynamically adapt to existing cyber threats.

According to Verizon's 2022 Information Security Incident Investigation Report, the relationship between a threat actor, their motivations, and their modus operandi varies by industry. Nevertheless, the report states that the main attack vector is the state financial structures and the banking sector. On January 25, specialists of the cyber security company Proofpoint published a detailed analysis of ART TA444, which focuses on financial crimes in the interests of the leadership of North Korea, the main targets of this cyber-attack: banks, financial institutions of many countries around the world, as well as the circulation of cryptocurrencies. Therefore, there is an urgent need for information protection of elements of the economic system of countries, including: websites of state and private economic institutions, network equipment of computer systems, methods of authentication and authorization, etc. Because, as a rule, business entities are focused on profits, and often forget about compliance with cybersecurity policies.

On January 24, the cybersecurity company Cisco Talos released its final report on the state of cybersecurity in 2022. In addition to the pronounced impact of the Russian-Ukrainian cyber confrontation, the company's specialists note several other important trends:

– dual purpose cyber security tools allow malicious actors to remain undetected in the affected environment;

– criminals actively use legitimate utilities/systems (such as PowerShell) for their purposes;

– expanding the scope of using the traditional form of spreading viruses via USB [21].

Guidelines from cybersecurity infrastructures such as the International Organization for Standardization (SOC) 2700 or the National Institute of Standards and Technology (NIST) should be used when creating the cybersecurity policy of economic entities. Many organizations, including Microsoft, are implementing a zero-trust security strategy to protect remote and hybrid workers (network users) who need secure access to company resources from anywhere. But any chosen cybersecurity policy strategy includes the core functions of protection, detection, response, prevention, and recovery. Based on the main functions of modern cyber security strategies, the main attention should be focused on methods of detecting and preventing intrusions.

Of course, in the issue of protecting the economy from cyberattacks on a national scale, under the conditions of informatization, digitalization, and computerization, it is necessary to consider the economic system at the level of each economic entity [22]. The network of any institution is a complex system of communication between various elements of the economic structure, which is implemented on the basis of computer systems of various functional purposes and network equipment. From the point of view of information security, it is necessary to consider them as a computer network, since most of the existing threats and attacks in cyberspace are carried out precisely from the global Internet network to which all economic structures are connected (**Fig. 2.6**).

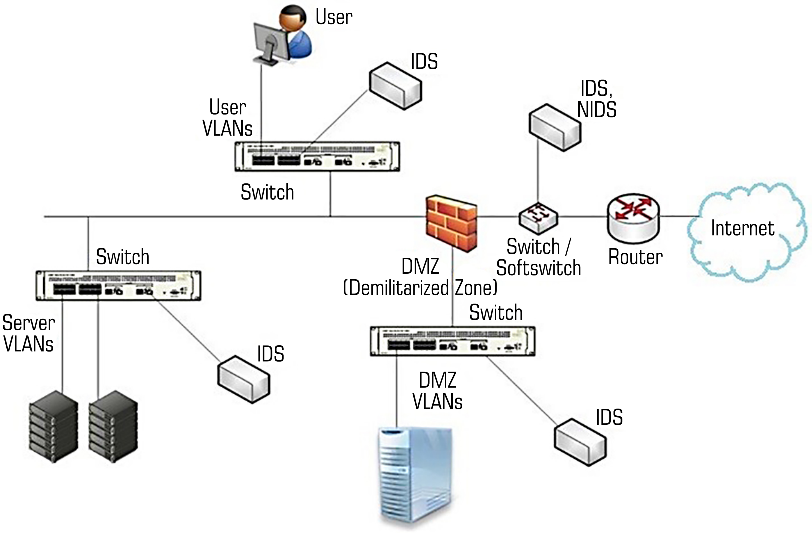


Fig. 2.6 Example of placing IDS in the network

Detection of network attacks is currently one of the most acute problems of the secure use of corporate networks. Large-scale epidemics of network worms, automated means of finding network vulnerabilities – all this makes ensuring the security of local networks of any enterprise a very time-consuming task. Now it is difficult to find a network that does not have such active means of preventing attacks as an antivirus, a brandmauer or a firewall, etc. However, active attack detection tools alone are not enough, because in cyber-attacks of any scale, the attacker scans the network using specially prepared scripts that identify potentially weak nodes. Selected nodes are attacked, which consists in sending certain bits (packets, frames, etc.), and the attacker gains administrative rights to them. Trojans (again certain types of active data attack prevention tools) are installed on hijacked nodes and run in the background. Therefore, the process of scanning data with the help of certain network scanners and sensors (which are included in the SBB, or are installed separately for additional monitoring) is one of the key factors in protecting against hacker attacks, since hacking mechanisms and all scenarios of cyber-attacks, regardless of their type (DoS, DDoS attacks, etc.) consists first in the possibility of access, and then in the acquisition, blocking, editing or destruction of data. In other words, when attacking a network, hackers send disguised data, usually as service information, which are actually parts of hacking code. Therefore, a very important element of information security of the economic sector is the development of effective monitoring of cyber security system events, which consists primarily of filtering traffic (network data). Currently, there are many information security monitoring systems based on Zabbix, DellFoglight, and Microsoft SCOM, among others, but the algorithm of their actions is well known to criminals, and the hacking of such a system is a matter of time [18].

Based on the above, it is necessary to actively monitor suspicious actions and threats and take action. Any security strategy will not be complete if there is no detection system, which means the presence of the necessary sensors of the intrusion detection system (IDS), which are distributed over the network and monitor actions (**Fig. 2.6**). Cybersecurity professionals must take advantage of today's detection technologies that profile users and computer systems to better understand anomalies and deviations from normal behavior and take preventive measures.

Therefore, the presence of a reliable and effective mechanism for detecting and preventing intrusions, which are the main elements of monitoring, are quite important, as they are one of the tools for building effective information security of financial institutions [23]. That is why this section will consider such questions as:

– detection capabilities;

– intrusion detection systems (IDS – Intrusion Detection System);

– intrusion prevention systems (IPS – Intrusion Prevention System);

– behavioral analytics within the organization;

– behavioral analytics in the hybrid cloud;

– placement of IDS in the network.

Intrusion detection process

The current threat landscape requires a new approach to detection systems that relies on the traditional complexity of fine-tuning initial rules, thresholds, and baselines. Dealing with multiple false positives becomes unacceptable for many organizations. When preparing to defend against attackers, the cybersecurity team should use a number of methods, which include:

– correlation of data from several sources;

– profiling;

– behavioral analytics;

– detection of anomalies;
– assessment of activity;
– machine learning.

It is important to emphasize that some traditional security controls, such as protocol analysis and signature-based antivirus software, still have their niche in the defense line, but are designed to combat legacy threats. Of course, it is not necessary to remove antivirus software that to use just because it doesn't have machine learning capabilities. This is still your host's security level.

On the other hand, the traditional mindset of cyber security professionals, which focuses only on monitoring high-powered users, is over and can no longer be that approach. To identify current threats, it is necessary to view all user accounts, profile them, and understand common behavior. Active threat actors will attempt to compromise the average user, remain on the network, and continue the intrusion through further propagation and privilege escalation. For this reason, there must be detection mechanisms that can identify such behavior across devices, in different locations, and generate alerts based on data correlation, as shown in **Fig. 2.7** [24].

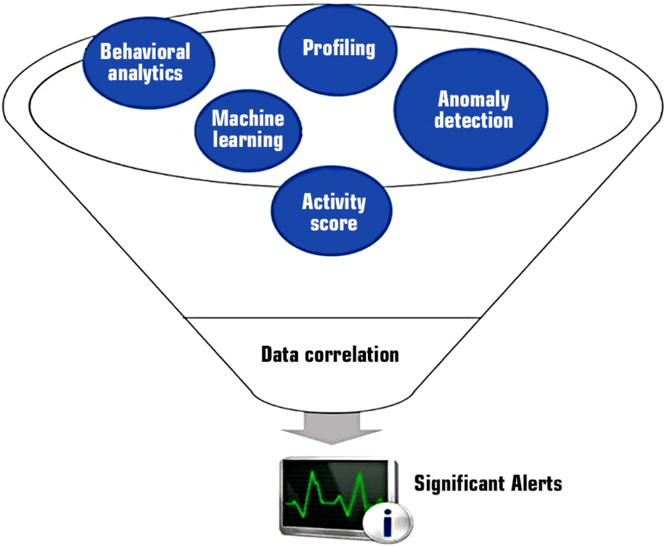


Fig. 2.7 Data correlation and notification process

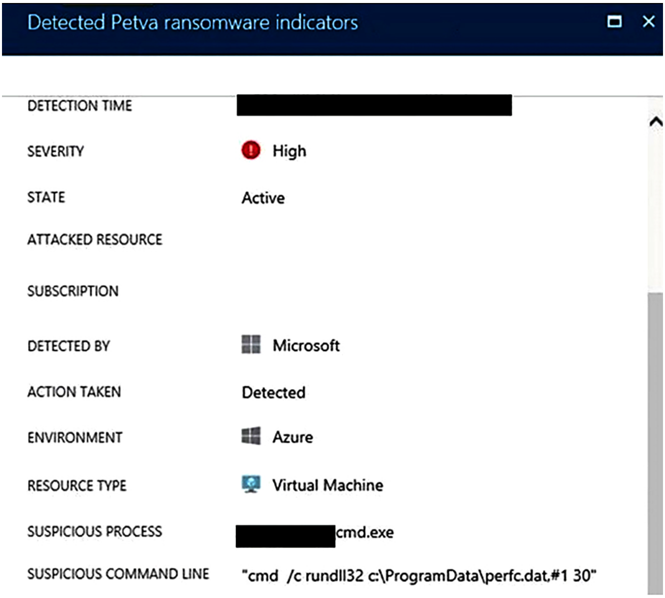
When data is contextualized, the number of false positives is naturally reduced, which has a significant impact on the security system.

Speaking of detection, it is important to mention indicators of compromise (Indicator of Compromise, IoC). When new threats appear in the natural environment, they usually have some kind of behavioral pattern and leave their mark on the victim's system.

For example, in June 2017, a large-scale cyberattack on various businesses and organizations, including a large number of financial institutions, was carried out using the Petya ransomware [25], which executed the following commands on the target system to reschedule the restart:

schtasks /Create /SC once /TN «» /TR «<systemfolder>shutdown.exe /r /f» /ST <time> cmd.exe /c schtasks /RU «SYSTEM» /Create /SC once /TN «» /TR «C:Windowssystem32shutdown.exe /r /f» /ST <time>

Another indicator of the activity of this program is the scanning of the local network through TCP ports 139 and TCP 445. These are important signs that the target system is under attack and the culprit is Petya. Discovery systems will be able to collect these indicators of compromise and issue alerts when an attack occurs. Using Azure Security Center as an example, some time after detecting the Petya threat, the center automatically updates its security mechanism and can alert users that their computer has been compromised, as shown in **Fig. 2.8** [24].



Detected Petva ransomware indicators

DETECTION TIME	[redacted]
SEVERITY	● High
STATE	Active
ATTACKED RESOURCE	
SUBSCRIPTION	
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
SUSPICIOUS PROCESS	[redacted]cmd.exe
SUSPICIOUS COMMAND LINE	"cmd /c rundll32 c:\ProgramData\perfc.dat,#1 30"

Fig. 2.8 Detecting the Petya virus using Azure Security Center

One of the options for using cyber security infrastructures in this aspect is the possibility to register on the OpenIOC website (http://openioc.org) to receive information about new indicators, as well as to contribute to the security of cyberspace based on previous experiences. Using the IoC Editor (see the help section for the URL from which it can be downloaded), it is possible to create your own indicator or browse an existing one. The cyber security team must always be aware of the latest threats and IoC.

Intrusion detection and prevention systems

An intrusion detection system (IDS) is a software or hardware tool designed to detect unauthorized access to or control of a computer system or network (mainly via the Internet). An IDS is one of the most important cyber security considerations that can detect intrusions before and/or after an attack [26]. As the name suggests, IDS is responsible for detecting a potential intrusion and initiating an alert. What can be done with this alert depends on the policy of the detection system [27]. In other words, IDS registers suspicious activities on the network and informs the person responsible for information security about them. Simplified, it can be imagined in the form of the scheme presented in **Fig. 2.9**.

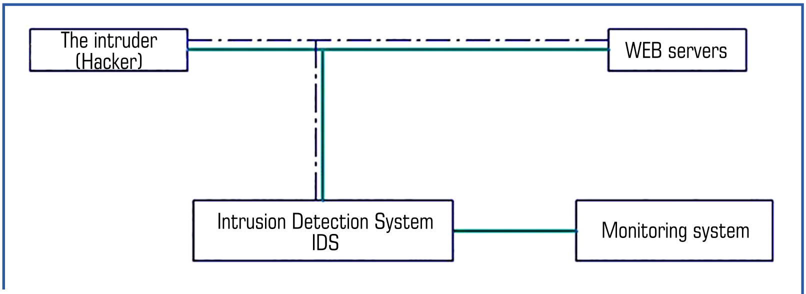


Fig. 2.9 Schematic representation of IDS interaction

When creating an IDS policy, the following step-by-step steps must be taken into account:

– determine those responsible for IDS control and availability of IDS administrator rights;

– determine the procedure for processing incidents based on alerts generated by IDS;

– determine the IDS update policy;

– determine the location of the IDS in the network.

These are just a few examples of the primary steps that should help in planning and implementing an IDS.

There are various variants of IDS classification, for example, IDS can be classified based on their, Detection methods, Deployment method, and Response method [28]. IDS can be divided into: network intrusion detection systems (NIDS) and host-based systems (HIDS) (**Fig. 2.10**).

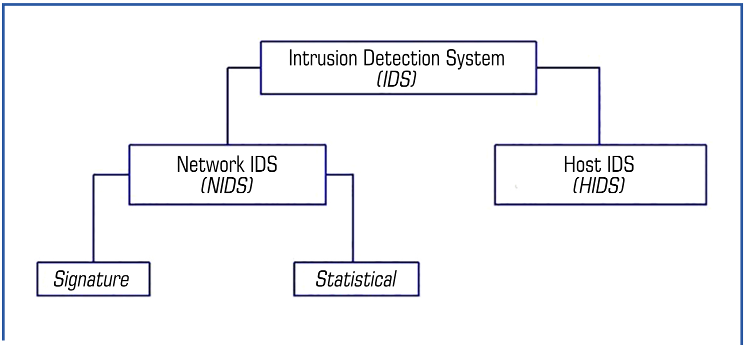


Fig. 2.10 Types of existing IDS

A HIDS node-based system is installed on each computer in the network to analyze and monitor traffic coming to the respective node, and from there HIDS also monitors and controls local file changes and possible changes due to unauthorized access.

NIDS analyzes traffic to detect known attacks based on existing rule sets. NIDS detects intrusions for the network segment in which it is installed. This means that in the case of NIDS, placement becomes critical to garnering valuable traffic. This is where the cybersecurity team must work closely with the IT infrastructure team to ensure IDSs are installed in strategically important locations throughout the network. When planning NIDS placement, prioritize the following network segments:

– Demilitarized Zone (DMZ);
– main corporate network;
– wireless network;
– virtualization network;
– other critical network segments.

Sensors that are part of the NIDS look at network traffic or logs and pass them to analyzers that look for information of a malicious nature in the received data and, in case of successful detection, send the results to the monitoring system. If the network sensors listen (analyze) traffic, that means they won't consume too much network bandwidth. Let's note that in the IDS deployment shown in **Fig. 2.6**, a detection system (which is actually a NIDS in this case) has been added to each segment (using a SPAN port on the network switch).

NIDS, in turn, fall into two broad categories, signature and statistical.

A signature-based intrusion detection system will query a database of signatures (traces) of already known attacks and known system vulnerabilities to check whether what has been detected is a threat and whether an alert should be triggered. Signature methods describe an intrusion using a formal model – it can be a character string, a semantic expression, etc. Signature analysis was the first method used for intrusion detection. This method checks whether the sequences match the signature. A signature is a signature, a pattern, for example, it can be a characteristic string of a program that indicates malicious traffic. The signature may contain a key phrase or command that is associated with the intrusion. If a match is found, an alarm is raised. The signature method protects against a hacker or virus attack only if its signature (for example, a fragment of the virus body) is known in advance. The advantages of signature intrusion detection methods are low computational complexity and low cost of deployment and application. The disadvantages of signature methods include the low efficiency of detecting unknown attacks and the problem of the aging of signature databases. Since it is the database of these signatures, it requires constant updating to have the latest version available. A behavior-based IDS works by creating basic patterns based on what it learns from the system. By learning normal behavior, it becomes easier to detect deviations.

Statistical methods are widely used to detect anomalies and are based on the construction of a statistical profile of the system's behavior during the training stage. System behavior should be normal during training. Further, for each parameter of the system functioning, it is necessary to form an interval of acceptable values using some known law of probability distribution. Statistical intrusion detection systems use a statistical approach and, after installation, are "learned" by the administrator, who sets the policy of the detection system, corresponding to normal activity in the network – types of traffic, connections between nodes, used protocols and ports. When detecting network intrusions or significant traffic differences from the typical in a particular system, IDS notifies the administrator. The statistical approach is highly sensitive to the correctness of the recognition rules. As a result, if the rules are set incorrectly, the system may trigger a false positive and differ in the complexity of the settings.

An effective IDS must be both signature and statistical, because some attacks have a pronounced signature, while others do not, but they cause deviations in the lower levels of the protocol stack (TCP/IP), which is exactly what a statistical IDS can detect. In wireless networks, the task of detecting intrusions is complicated by radio interference, refraction reflection, and signal scattering.

Regardless of the chosen one, a typical IDS has the capabilities shown in **Fig. 2.11**. In addition to the functions of constant monitoring and analysis of what is happening, IDS systems perform the following functions:

– collection and recording of information;

– notification of network administrators about the changes that have occurred;

– creation of reports for summarizing logs.

While these are the basic capabilities, the number of features will actually depend on the vendor of the security tool (software and/or hardware) and the method used by the IDS. The implemented IDS should be based on various detection methods and technologies, as well as flexibly integrated with the general cooperative structure of the enterprise network [29]. IDS has got many developments through its datasets, new technologies and methods but as the technologies increases, the threats of attacking the system and data breaches also increases, so in order to overcome this problem a hybrid framework for the intrusion detection has to be developed to detect the intrusions from the intruder [28].

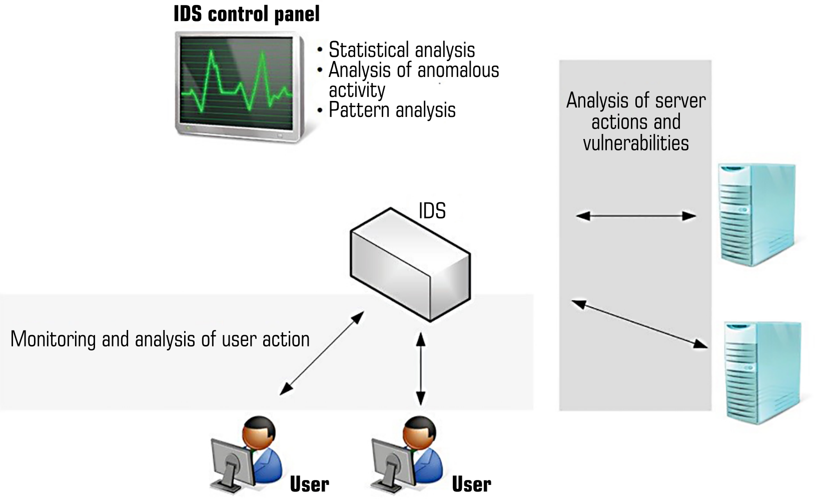

IDS control panel
• Statistical analysis
• Analysis of anomalous activity
• Pattern analysis
Analysis of server actions and vulnerabilities
IDS
Monitoring and analysis of user action
User
User

Fig. 2.11 Scheme of a typical IDS

An Intrusion Prevention System (IPS) uses the same concept as an IDS, but as the name suggests, it prevents intrusions by taking corrective actions. These actions will be debugged by the IPS administrator. It is worth noting that IPS is a subclass of IDS (active IDS) and is therefore based on its attack detection methods. The ability to prevent attacks is realized due to the fact that the network IPS is usually built into the network gap and passes traffic through it further if it is recognized as safe [30]. IPS works, of course, slower than ordinary IDS, because it is necessary to analyze and immediately pass traffic. IPS technology, in turn, in addition to the IDS functions listed above, is able not only to identify the threat and its source, but also to block them. This indicates the extended functionality of such a solution. IPS is able to perform the following actions:

– terminate malicious sessions and prevent access to the most important resources;

– change the configuration of the "protected" environment;

– perform actions on attack tools (for example, delete infected files).

Just as IDS is host-based (HIDS) and network-based (NIDS), IPS is host-based (HIPS) and network-based (NIPS). Placing NIPS on the network is critical, and the same guidelines as previously mentioned apply here. Consideration should also be given to positioning NIPS according to traffic so that corrective actions can be taken if necessary.

IPS can typically operate in one or more of the following modes:

– based on the rules;

– based on the anomalies.

Rule-based detection. When operating in this mode, IPS compares traffic against a set of rules and attempts to verify that the traffic matches the rule. This is very useful when it is necessary to deploy a new rule to block an attempt to exploit vulnerabilities. NIPS systems such as Snort are capable of blocking threats using rule-based detection [30]. For example, the Snort rule Sid 1-42329 is able to detect the Win.Trojan.Doublepulsar variant. Snort rules can be found here: etc/snort/rules, and other rules can be downloaded from the official site.

Sometimes multiple rules are needed to neutralize a threat. For example, rules 42340 (Anonymous SMB session IPC access attempt), 41978 (SMB remote code execution attempt), and 42329-42332 (Win.Trojan.Doublepulsar variant) can be used to detect the WannaCry ransomware.

The advantage of using an open source NIPS such as Snort is that when a new threat becomes available on the network, the community usually reacts quite quickly by publishing a new rule to detect the threat. For example, when the Petya ransomware was discovered, the community created a rule and posted it on GitHub. Although vendors and the security community are really quick to publish new rules, it's still up to cybersecurity professionals to keep an eye out for new indicators of compromise and create NIPS rules based on them.

Anomaly based detection. In this case, the anomaly is based on what the IPS classifies as anomalous. This classification is usually based on heuristics or summation of rules. One of the options is statistical anomaly detection, in which samples of network traffic are taken at random moments of time and a comparison is made with the baseline state. If this sample deviates from the baseline, an alert is triggered with further action.

It is worth noting that the UTM firewall, network sensors and any modern intrusion detection and prevention systems are the optimal combination of IDS and IPS technologies.

The method of detecting malicious activity (malicious activity) as a behavioral and analytical mechanism of cyber security

For the vast majority of companies on the market today, the core business is still conducted within the organization. It's where mission-critical data resides, where most users work, and where key resources reside. There are many attacker attack strategy scenarios, but they all have common steps: infiltrate the local network, spread further, elevate privileges, and maintain communication with the command-and-control server until that server can complete its mission. For this reason, the presence of behavioral analytics is required to quickly break the attack lifecycle [24].

According to Gartner, it is very important to understand how users behave. By monitoring legitimate processes, organizations can use User and Entity Behavior Analytics (UEBA) to detect security breaches. There are many benefits to using UEBA's behavioral analysis system to detect attacks, but one of the most important is the ability to detect attacks at an early stage and take corrective measures to contain the attack.

Fig. 2.12 shows an example of how UEBA looks at different objects to decide whether an intrusion alert should be triggered or not.

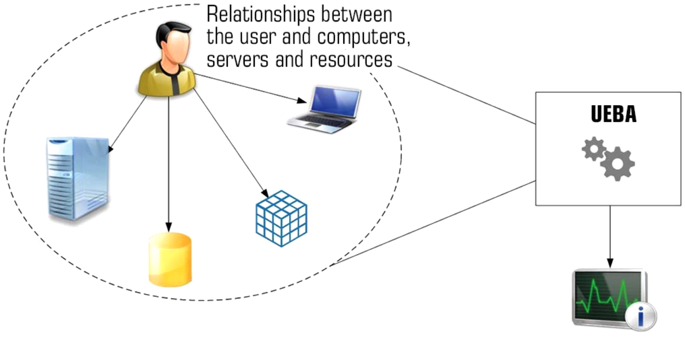
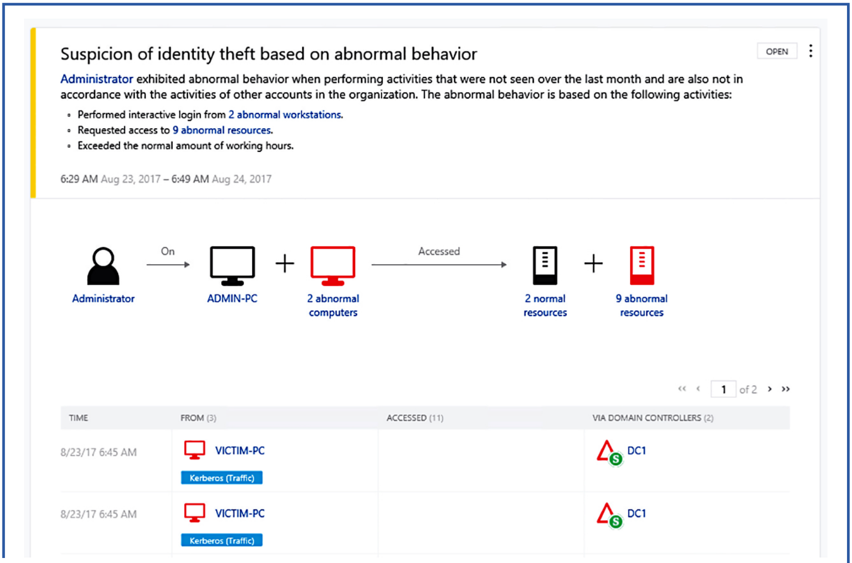


Fig. 2.12 Principle of UEBA operation

Without a system that can look at all the data at scale and make correlations not only by traffic pattern, but also by user profile, the chances of false positives for security tools increase. For example, when there is a UEBA system within the organization, which serves as the main tool for detecting malicious activity through the analysis of the behavior of users and objects in the network. The UEBA system knows which servers' users usually access, which resources they visit, which operating system is used to access these resources, and it also knows the geographic location of users. **Fig. 2.13** shows an example of this type of detection from Microsoft's Advanced Threat Analytics (ATA), which uses behavioral analytics to detect suspicious behavior. Let's note that in this case the message is quite clear. It says that the administrator did not perform these actions last month, as a result the data does not correlate with other accounts in the organization. This warning cannot be ignored because it is contextualized, which means that it analyzes the data collected from different angles to perform a comparison and decide whether to issue an alert or not.

The UEBA system within an organization can help the security team be more proactive and gain more tangible data for accurate response. The UEBA system consists of several modules, and another module is advanced threat detection, which looks for known vulnerabilities and attack patterns. **Fig. 2.14** shows how Microsoft ATA detects a Pass-the-ticket attack.

Because there are different ways to perform this attack, advanced threat detection cannot only look for the signature, it must look for the attack pattern and what the attacker is trying to do. This is much more efficient than using a signature-based system. It also looks for suspicious behavior that comes from normal users who shouldn't be performing certain tasks. For example, if a normal user tries to run NetSess.exe in the local domain, Microsoft ATA treats this as traversal of SMB sessions, which, from the attacker's point of view, is usually done during the reconnaissance phase. For this reason, Microsoft ATA issues a warning when the user attempts to run NetSess.exe.



Suspicion of identity theft based on abnormal behavior

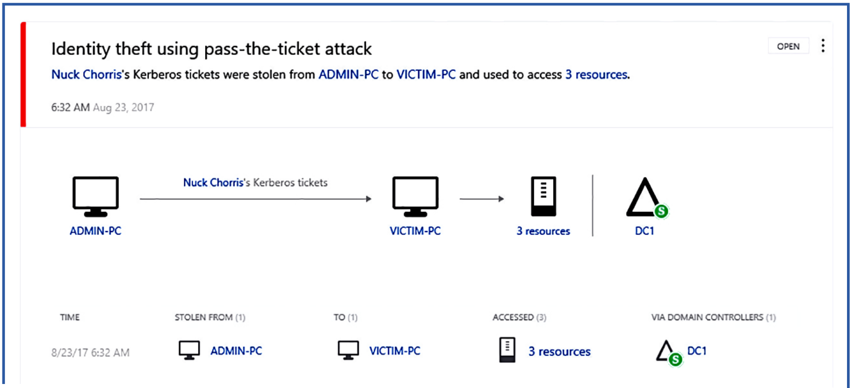
Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 2 abnormal workstations.
- Requested access to 9 abnormal resources.
- Exceeded the normal amount of working hours.

6:29 AM Aug 23, 2017 – 6:49 AM Aug 24, 2017

TIME	FROM (3)	ACCESSED (11)	VIA DOMAIN CONTROLLERS (2)
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1

Fig. 2.13 Detection of suspicious behavior of a network user



Identity theft using pass-the-ticket attack

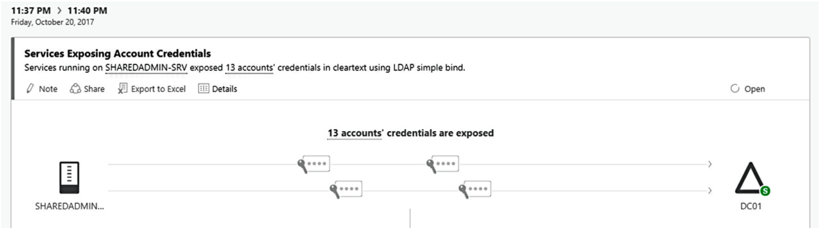
Nuck Chorris's Kerberos tickets were stolen from ADMIN-PC to VICTIM-PC and used to access 3 resources.

6:32 AM Aug 23, 2017

TIME	STOLEN FROM (1)	TO (1)	ACCESSED (3)	VIA DOMAIN CONTROLLERS (1)
8/23/17 6:32 AM	ADMIN-PC	VICTIM-PC	3 resources	DC1

Fig. 2.14 Pass-the-ticket attack detection using Microsoft ATA

Attackers will not only exploit vulnerabilities, but also take advantage of misconfigurations in the targeted system, such as incorrect protocol implementation and lack of protection. For this reason, UEBA will also detect systems that lack a secure configuration. **Fig. 2.15** shows how Microsoft ATA detects a service that provides access to account credentials because it uses the LDAP protocol without encryption.



11:37 PM > 11:40 PM
Friday, October 20, 2017

Services Exposing Account Credentials
Services running on SHAREDADMIN-SRV exposed 13 accounts' credentials in cleartext using LDAP simple bind.

Fig. 2.15 Microsoft ATA warning to account credentials

Using the same principles previously discussed when looking at IDS, where to install UEBA will vary depending on your company's needs and vendor requirements. Microsoft ATA, which was used in the examples described in the section, requires the use of traffic mirroring with a domain controller (traffic mirroring with a domain controller). ATA will not affect network throughput as it will only listen to controller traffic.

When cybersecurity professionals need to take countermeasures to protect a hybrid environment, they should expand their understanding of the current threat landscape and perform an assessment to verify the ability to continuously connect to the cloud and assess the impact on the overall security posture. In the hybrid cloud, most companies prefer to use the IaaS model [31]. Although the adoption of this model is increasing, according to the Oracle study, the security aspect is still a major concern. According to an Oracle report, long-term users of IaaS believe that the technology will ultimately affect security. It actually has a positive impact, and this is where the cyber defense team should focus their efforts to improve the overall detection process. The goal is to use the power of the hybrid cloud to contribute to the overall security concept. The first steps are establishing a good partnership with the deployed cloud provider and understanding what security capabilities the provider offers and how those capabilities can be leveraged in a hybrid environment. This is important because some capabilities are only available in the cloud and not on-premises.

Azure Security Center

The reason for considering using Azure Security Center to monitor a hybrid environment is that the center agent can be installed on a local computer (Windows or Linux), on a virtual machine running on Azure or on AWS, which is quite relevant Today. This flexibility is important, and centralized management is important for a cyber defense team. Security Center uses intelligent security tools and advanced analytics to detect threats faster and reduce the number of false positives. Ideally, using a single window system to visualize alerts and suspicious activity across all workloads, the basic topology looks similar to that shown in **Fig. 2.16**.

When Security Center is installed on work computers, it will collect ETW (Event Tracing for Windows), operating system log events, running processes, computer name, IP addresses, and registered users. These events go to Azure and are stored in the personal workspace storage.

Security Center will analyze this data using methods such as:

– cyber intelligence;

– behavioral analytics;

– detection of anomalies.

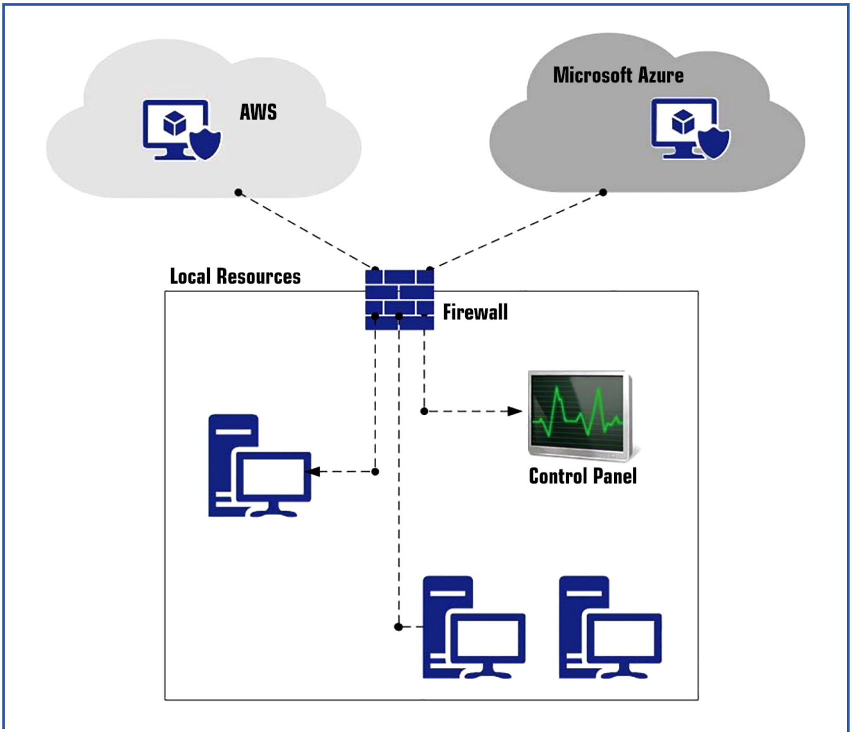
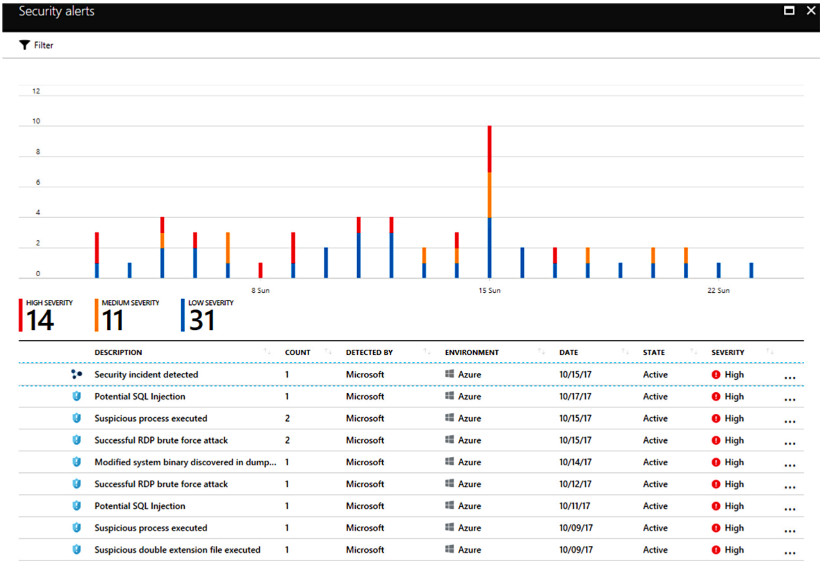


Fig. 2.16 Communication structure with the security center

After evaluating this data, the security center will trigger an alert based on the priority and add it to the monitoring dashboard as shown in the **Fig. 2.17**.

Let's note that the first alert has a different icon and is called Security Incident Detected. This is because it has been identified, and two or more attacks are part of the same command and control server (the attackers' C&C server) directed against a certain resource. This means that, when the security center collects data in order to find the relationship between events, it does this automatically and provides relevant alerts for analysis. When to click on this notification, the following window will appear (**Fig. 2.18**).



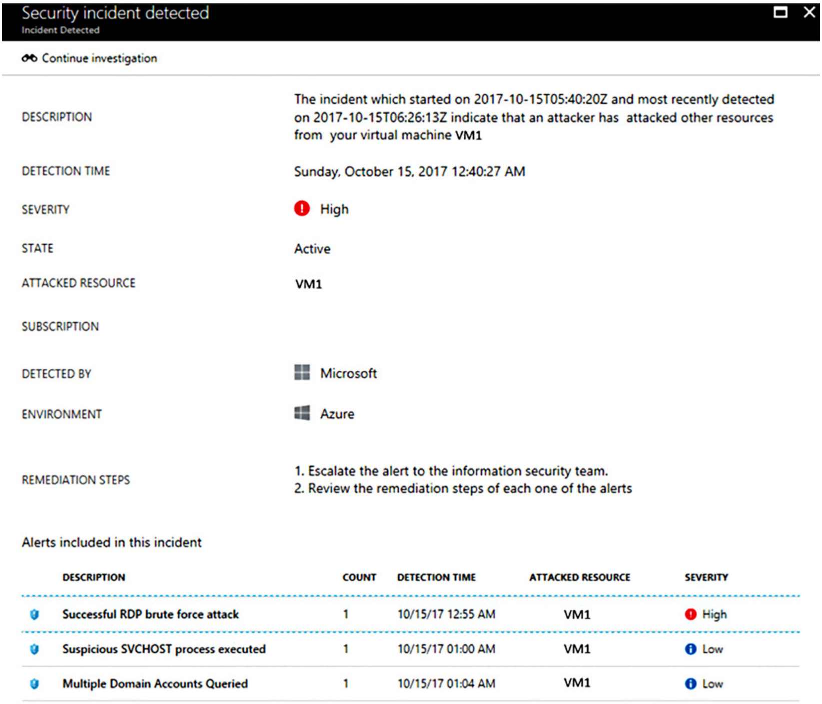
DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	Azure	10/15/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/17/17	Active	High
Suspicious process executed	2	Microsoft	Azure	10/15/17	Active	High
Successful RDP brute force attack	2	Microsoft	Azure	10/15/17	Active	High
Modified system binary discovered in dump...	1	Microsoft	Azure	10/14/17	Active	High
Successful RDP brute force attack	1	Microsoft	Azure	10/12/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/11/17	Active	High
Suspicious process executed	1	Microsoft	Azure	10/09/17	Active	High
Suspicious double extension file executed	1	Microsoft	Azure	10/09/17	Active	High

Fig. 2.17 Microsoft Azure Security Center Notification Panel

In the lower part of this page in **Fig. 2.18** shows all three attacks (in order of occurrence) on the attacked resource VM1 and the severity level assigned by the Microsoft Azure Security Center. Here is one important observation regarding the benefits of using behavioral analytics for threat detection. This is the third notification (**Fig. 2.18**) Multiple Domain Accounts Queried. The command that was executed to issue this alert is: netuser<username> /domain. However, to decide that this looks suspicious, it is necessary to look at the normal behavior of the user who executed the command and compare that information with other data that, when analyzed in context, would be categorized as suspicious.

As it is possible to see from this example, hackers use built-in system tools and a "native" command-line interface to carry out their attack. For this reason, it is extremely important to have a command line call logging tool available.

The security center will also use statistical profiling to build traditional baselines and anomaly alerts that match the potential attack vector. This is useful in many scenarios. A typical example is a deviation from normal activity. For example, suppose a host initiates an RDP connection 3 times a day, but on a given day hundreds of attempts are made. When such a deviation occurs, an alert should be issued to warn of it.



Security incident detected
Incident Detected

Continue investigation

DESCRIPTION	The incident which started on 2017-10-15T05:40:20Z and most recently detected on 2017-10-15T06:26:13Z indicate that an attacker has attacked other resources from your virtual machine **VM1**
DETECTION TIME	Sunday, October 15, 2017 12:40:27 AM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	**VM1**
SUBSCRIPTION	
DETECTED BY	Microsoft
ENVIRONMENT	Azure
REMEDIATION STEPS	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts

Alerts included in this incident

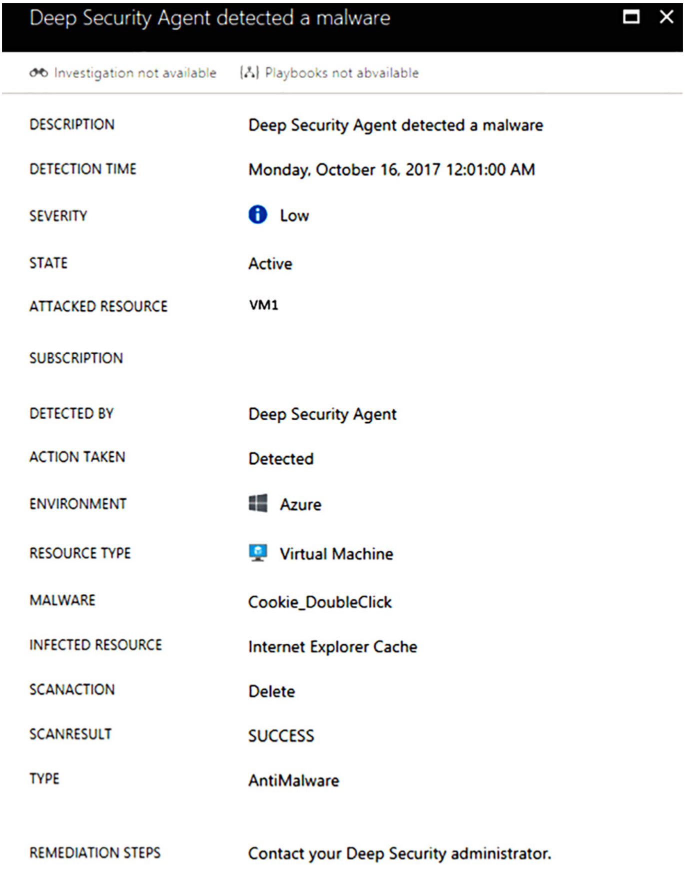
DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Successful RDP brute force attack	1	10/15/17 12:55 AM	VM1	High
Suspicious SVCHOST process executed	1	10/15/17 01:00 AM	VM1	Low
Multiple Domain Accounts Queried	1	10/15/17 01:04 AM	VM1	Low

Fig. 2.18 Microsoft Azure Security Center Notification Panel (analysis)

Another important aspect of working with a cloud service is built-in integration with other providers. Security Center can integrate with many other solutions such as Barracuda, F5, Imperva and Fortinet for Web Application Firewall, among others for endpoint protection, vulnerability assessment and next generation firewall. The image below shows an example of such integration (**Fig. 2.19**).

Let's note that this alert was generated by the Deep Security Agent, and since it is integrated with Security Center, it will appear on the same dashboard as other events detected by Security Center.

It should be remembered that the security center is not the only solution that will monitor systems and integrate with other security system providers. There are many Security Information and Event Management (SIEM) solutions for information security and event management, such as Splunk and LogRhythm, that will perform a similar type of monitoring.



Deep Security Agent detected a malware

Investigation not available Playbooks not abvailable

DESCRIPTION	Deep Security Agent detected a malware
DETECTION TIME	Monday, October 16, 2017 12:01:00 AM
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	VM1
SUBSCRIPTION	
DETECTED BY	Deep Security Agent
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
MALWARE	Cookie_DoubleClick
INFECTED RESOURCE	Internet Explorer Cache
SCANACTION	Delete
SCANRESULT	SUCCESS
TYPE	AntiMalware
REMEDIATION STEPS	Contact your Deep Security administrator.

Fig. 2.19 Alert generated by Deep Security Agent

CONCLUSIONS

The principles of information security management according to the international standard ISO/IEC 27001 state that an organization must develop, implement and maintain a coherent set of policies, processes and systems to manage risks and threats to its information assets, thus ensuring acceptable levels of information security risk. According to this standard, it is necessary to develop an effective security policy for each enterprise depending on many factors (field of activity, network configuration, software, etc.).

Although cybercrime is quite an actual problem, protecting information in terms of confidentiality, availability and integrity is not as easy as it might seem at first glance. It is important to constantly use new methods of protection, because criminals are constantly working and looking for new ways. That is why this section discusses modern and effective cyber protection tools for business entities. Methods and algorithms of security systems against unauthorized intrusions are usually developed for a specific object of protection. But regardless of the object of protection, it will be a large commercial network, a state-level server or a mobile device of a simple user, there is one common goal, which is to protect data as the main element of information security. To protect any system, it is necessary to first detect an intrusion (attack), regardless of the type, it will be viruses (classic file viruses or Ransomware), phishing, DDoS attacks, botnets, backdoors or other hacking attempts, this is the task of intrusion detection systems. The next stage is to decide how to eliminate this cyber-attack and, based on this experience, to create a reliable protection algorithm against threats of this type, this is the task of intrusion prevention systems. There are different operating practices of intrusion detection and prevention systems, but, as a rule, the algorithm is the same, when detecting and eliminating attacks, the task of security systems is also to create patterns of potential threats. In the further process of continuous monitoring and data scanning, data is constantly compared with templates of user and service information, as well as with templates and indicators of threats based on previous experience, not only one's own, within the local network or system, but also on a global scale [18]. That is, detection and prevention of network attacks is one of the most important tasks of the company's network cyber security policy. That is why this article considered various types of intrusion detection mechanisms and indicated the advantages of their use. Intrusion prevention systems that work on the basis of rules and anomalies are also analyzed in detail. Currently, there are various cyber protection systems (Acunetix, Azure Security Center, Invicti (formerly Netsparker), ManageEngine Vulnerability Manager Plus, System Mechanic Ultimate Defense, Microsoft Advanced Threat Analytics, SecPod SanerNow, Solar Winds Security Event Manager) with a template database of all threats, which were discovered earlier in the world. There are also many sites where it is possible to get information about new indicators and patterns, as well as contribute to the cyber security IT community by sharing your attack types if they are not available on this platform. It is very important that cyber-attack protection systems compare all data on a wide scale and make correlations not only by the traffic pattern, but also by the user profile, because otherwise the chances of false positives increase [18].

In this section, Microsoft ATA and Azure Security Center were used as an example, which was used as a hybrid solution for behavioral analysis of computer network users. Based on the considered concept of detection and prevention of intrusions, it is possible to build an effective notification system for network protection, which is the basis of a cyber security strategy according to international standards.

Therefore, creating an effective cyber security policy and managing it is a rather complex process that requires a combination of various tools, methods and specialists. First, identify resources and assess risks, then create processes to address cybersecurity threats. Develop a plan to help the cybersecurity team respond to security breaches. Track your goals and assess your security level with the specialized solution outlined in this section.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Ukraina 2030E – kraina z rozvinutoyu cifrovoyu ekonomikoyu. Available at: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html
2. Onyshchenko, S., Skryl, V., Hlushko, A., Maslii, O.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Inclusive Development Index. Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 779–790. doi: https://doi.org/10.1007/978-3-031-17385-1_66
3. European Commission. International Digital Economy and Society Index 2022 – Executive Summary. Available at: https://nqa.gov.ua/news/indeks-cifrovoi-ekonomiki-2022-zvit-evropejskoi-komisii/
4. European Commission. Digital Economy and Society Index (DESI) 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022
5. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. International Journal of Engineering & Technology, 7 (3.2), 447–452. doi: https://doi.org/10.14419/ijet.v7i3.2.14569
6. Glushko, A. D. (2013). Directions of Efficiency of State Regulatory Policy in Ukrain. World Applied Sciences Journal. Pakistan: International Digital Organization for Scientific Information, 27 (4), 448–453.
7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky". Ukaz Prezydenta Ukrainy No. 685/2021. 28.12.2021. Available at: https://zakon.rada.gov.ua/laws/show/en/685/2021#Text
8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy". Ukaz Prezydenta Ukrainy No. 447/2021. 26.08.2021. Available at: https://www.president.gov.ua/documents/4472021-40013
9. Saxena, H., Mittal, A. (2022). Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022. Available at: https://www.cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022

10. Onyshchenko, S., Hlushko, A. (2022). Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats. Economics and Region, 1 (84), 13–20. doi: https://doi.org/10.26906/EiR.2022.1(84).2540
11. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 749–760. doi: https://doi.org/10.1007/978-3-031-17385-1_63
12. Borenkov, A. (2023). TOP 10 Cybersecurity Threats to Businesses in 2023. Available at: https://www.bdo.ua/en-gb/insights-1/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023
13. Onyshchenko, S., Bilko, S., Yanko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Business Information Security Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 769–778. doi: https://doi.org/10.1007/978-3-031-17385-1_65
14. Nayak, Mr. P., Sufiyan, M., Monisha, N. S., Bhaskar, M. G., Raju, M. (2022). Review Paper on Cyber Security and Types of Cyber Attacks. International Journal of Advanced Research in Science, Communication and Technology, 2 (1), 732–735. doi: https://doi.org/10.48175/IJARSCT-7043
15. Fedor, O. (2022). 93 Must-Know Ransomware Statistics. Available at: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/
16. Glushko, A., Marchyshynets, O. (2018). Institutional Provision of the State Regulatory Policy in Ukraine. Journal of Advanced Research in Law and Economics, 9 (3), 941–948. doi: https://doi.org/10.14505/jarle.v93(33).18
17. Za pershyi misiats roboty systemy Protective DNS na ponad 30% zmenshylys vtraty ukraintsiv vid finansovoho fishynhu. Available at: https://inshe.tv/suspilstvo/2023-03-16/747356/
18. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
19. Zhao, J., Yue, X., Feng, C., Zhang, J., Li, Y., Wang N. et. al (2022). Survey of Data Privacy Security Based on General Data Protection Regulation. Journal of Computer Research and Development, 59 (10), 2130–2163. doi: https://doi.org/10.7544/issn1000-1239.20220800
20. Schütze, B.; Hübner, U. H., Wilson, G. M., Morawski, T. S., Ball, M. J. (Eds.) (2022). Data Protection and Data Security in the EU: the European General Data Protection Regulation. Nursing Informatics. Cham: Springer, 437–451. doi: https://doi.org/10.1007/978-3-030-91237-6_29
21. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12 (6), 1333. doi: https://doi.org/10.3390/electronics12061333

22. Onyshchenko, S., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Risks and Threats to Economic Security of Enterprises in the Construction Industry Under Pandemic Conditions. Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181. Cham: Springer, 711–724. doi: https://doi.org/10.1007/978-3-030-85043-2_66
23. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Increasing Information Protection in the Information Security Management System of the Enterprise. Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181. Cham: Springer, 725–738. doi: https://doi.org/10.1007/978-3-030-85043-2_67
24. Makarenko, O., Yanko, A. (2022). Concept of the system of detection and prevention of networks. Control, Navigation and Communication Systems, 2 (68), 59–67. doi: https://doi.org/10.26906/SUNZ.2022.2
25. Diogenes, Y., Ozkaya, E. (2019). Cybersecurity Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals. Packt Publishing Ltd.
26. Othman, S. M., Alsohybe, N. T., Ba-Alwi, F. M., Zahary, A. T. (2018). Survey on Intrusion Detection System Types. International Journal of Cyber-Security and Digital Forensics, 7 (4), 444–462. doi: http://dx.doi.org/10.17781/P002525
27. Northcutt, S., Novak, J. (2002). Network Intrusion Detection: An Analyst's Handbook. Indianapolis: New Riders Publishing, 478.
28. Kalaivani, A., Pugazendi, R. (2023). A Review on Intrusion Detection System and its Techniques. Data Analytics and Artificial Intelligence, 3 (2), 132–137. doi: https://doi.org/10.46632/daai/3/2/24
29. Li, J. (2022). Network Intrusion Detection Algorithm and Simulation of Complex System in Internet Environment. 2022 4th International Conference on Inventive Research in Computing Applications, Coimbatore: IEEE, 520–523. doi: https://doi.org/10.1109/ICIRCA54612.2022.9985720
30. Collins, M. (2017). Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc.
31. Chowdhury, P., Paul, S., Rudra, R., Ghosh, R.; Joshi, A., Mahmud, M., Ragel, R.G. (Eds.) (2023). Cyber-Attack in ICT Cloud Computing System. Information and Communication Technology for Competitive Strategies. Lecture Notes in Networks and Systems Vol. 400. Singapore: Springer,115–121. doi: https://doi.org/10.1007/978-981-19-0095-2_12