UDC 004.058
https://doi.org/10.47533/2024.1606-146X.05

G. Z. ZIYATBEKOVA[1,2]****, A. E. TURYSBAYEV***[2]***, B. B. RAKYMBEKOV***[2]***,***
N. M. SERIKBAYEV[2]***, B. MOLDAKALLYKOVA***[3]***, ZH. A. BIMOLDINA***[3]

[1]*RSE Institute of Information and Computational Technologies CS MSHE RK,*
Almaty, Kazakhstan;
[2]*Al-Farabi Kazakh National University, Almaty, Kazakhstan;*
[3]*Turan University, Almaty, Kazakhstan;*
aryn.turysbayev@gmail.com; baha.adeline@gmail.com; nurdaulet.s.999@gmail.com

MODERN APPROACHES TO INFORMATION SECURITY: ANALYSIS OF INTRUSION DETECTION, FIREWALLS AND AUDITING IN THE CONTEXT OF ORGANIZATIONAL DATA PROTECTION

Today's business environment presents organizations with growing information security challenges. The threats posed by cyber-attacks and the leakage of sensitive information require effective and innovative approaches to data protection. This paper explores a combination of tools and techniques, including intrusion detection system (IDS), firewalls, and information security auditing, as key elements of organizational data protection.

The paper provides a detailed overview of each of these components and discusses their roles in information security. For an intrusion detection system, its ability to detect and respond to different types of attacks in real time is investigated. For firewalls, consider how they restrict access to network resources and regulate traffic. Finally, information security audits act as a means of assessing the effectiveness of security measures and identifying weaknesses. Statistical data and best practices are presented to support our recommendations. This article discusses the integration of these systems in a comprehensive information security strategy and provides tips for maximizing data protection in today's digital world.

This article provides valuable guidance for organizations seeking to maintain top-tier information security and effectively protect sensitive information from ever-changing cyber threats.

Key words: *IDS, firewalls, information security audits, networks, cyber threats.*

Introduction. Today's world of information technology has brought many innovations and opportunities but is also accompanied by increased threats to information security. Every day, organizations face increasing risks of cyberattacks, data breaches and other threats that can significantly damage their operations and reputation. In such a context, securing data and infrastructure becomes the number one priority for organizations of all sizes.

Intrusion Detection Systems (IDS) are one of the key components of an information security strategy. These systems are an integral part of protecting information and network infrastructure. In this article, we examine the nature and importance of intrusion detection systems and evaluate the current approaches they use to identify potential threats.

Result and discussion. Intrusion detection systems: Intrusion Detection Systems (IDS) are a set of technologies and techniques designed to detect suspicious activity and potential intrusions into computer systems and networks. The primary purpose of IDS is to monitor network and host-based activity to detect anomalies that could indicate potential security threats.

* E-mail корреспондирующего автора: ziyatbekova@mail.ru

Network Intrusion Detection Systems (NIDS) focus on monitoring network traffic and analyzing data packets transmitted on a network. They can detect attacks, such as introductions through network vulnerabilities, as well as anomalies in network traffic that indicate potential security incidents.

Host-based intrusion detection systems (HIDS), on the other hand, are installed on specific hosts, such as servers and workstations, and monitor their local logs and activity. HIDS can detect host-specific attacks and anomalies, as well as monitor changes to system files and settings.

Modern approaches to intrusion detection. Intrusion detection systems are constantly evolving and improving to counter increasingly complex and sophisticated cyber threats. One of the most important areas of modern approaches to IDS is the application of machine learning and artificial intelligence.

Research in machine learning and IDS indicates the potential for these techniques to detect anomalies more accurately and quickly. Machine learning models can analyze large amounts of data and identify unusual patterns that might have gone undetected by traditional detection methods [1].

Modern IDSs also actively use Big Data analysis techniques, which allow efficient processing and analysis of massive amounts of information [2]. This is particularly important in the context of modern networks, were data flows in huge volumes. Processing and analyzing such data can help identify irregular patterns and anomalies indicative of potential security incidents.

In addition, modern IDSs are increasingly integrated with other components of information security systems, such as firewalls and auditing systems. This allows for a comprehensive security system that can not only detect incidents but also respond to them in real time [3].

Applying advanced intrusion detection approaches can help organizations improve their ability to respond to cyber threats and protect valuable data. However, it is important to remember that information security is a continuous and multifaceted process that requires constant monitoring, analysis and updating of approaches and technologies.

Firewalls: Information security advocates. In today’s digital world, where data and information play a key role, information security is becoming increasingly important. The security of data and computer systems comes first, and one of the main tools in this area are firewalls. In this section of the article, we will look at what firewalls are, what role they play in information security, and compare different types of firewalls. A firewall is a software or hardware tool designed to control and monitor the flow of data between computers or networks. Its purpose is to secure data and computer systems by filtering network traffic and enforcing access rules.

Roles of firewalls in information security

1. Protection against external threats

Firewalls play an important role in protecting computer systems and networks from external threats such as hacker attacks, viruses, and malware. They act as a barrier, controlling and filtering incoming and outgoing network traffic. This prevents unauthorized access and protects valuable data.

2. Access control and security policies

Firewalls allow you to customize security rules and policies for your network. Administrators can determine who has access to network resources and what actions are allowed or denied. This provides granular control over the network and enhances overall security.

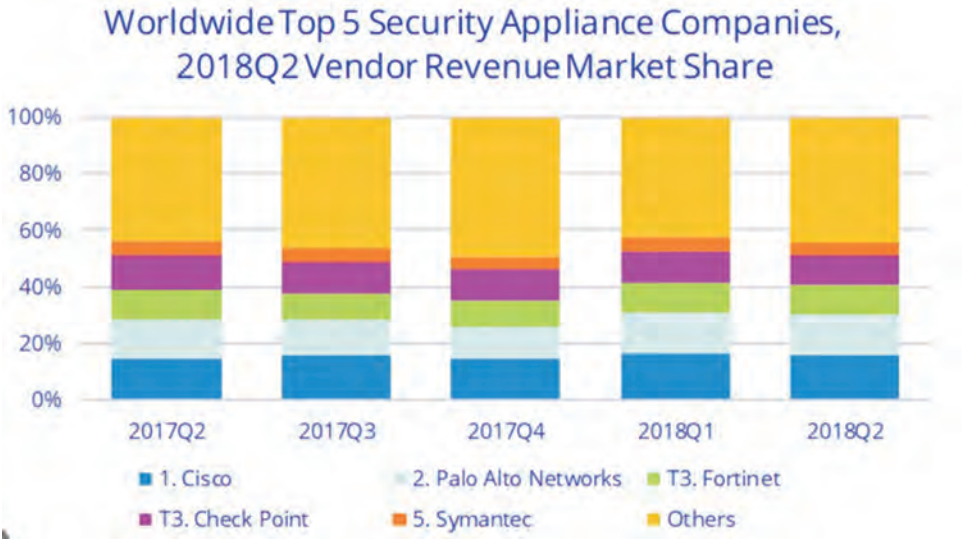


Figure 1 – Firewall vendors

Figure 1 demonstrates the important role of firewall vendors in providing information security to organizations. These vendors provide specialized firewalls and network traffic controls that limit unauthorized users' access to critical resources and provide a first line of defense against cyber threats [4]. Their solutions play an important role in creating strong network barriers and securing an organization's data.

Comparison of different types of firewalls

There are several types of firewalls, each with its own features and benefits:

1. Network firewalls:

Network firewalls are typically installed at the individual computer or device level. They control traffic at the level of a particular machine and can be software or hardware based. Network firewalls are suitable for protection against localized attacks and have a low entry threshold.

2. Firewalls:

Firewalls sit between different networks and control traffic between them. They are typically used at higher layers of the network architecture and provide centralized control of traffic between different parts of the network.

3. Hardware and software firewalls:

Hardware firewalls are physical devices that are installed between networks. They provide high performance and can handle high traffic volumes. Software firewalls, on the other hand, operate at the operating system level and can be installed on ordinary computers [5].

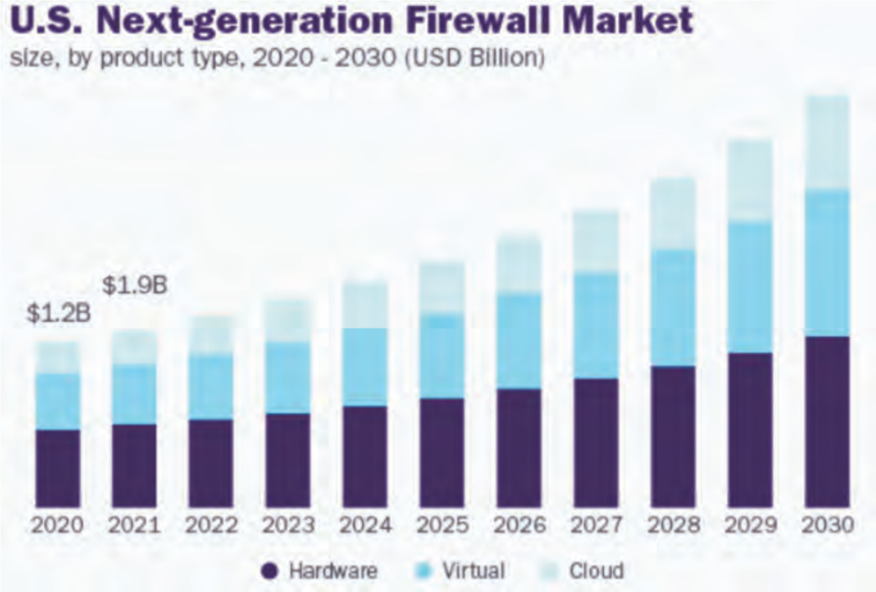


Figure 2 – NGF market in the USA

The 2-figure figure presents statistical information about the intrusion detection system (NGF) market in the United States. This graph shows data on the market share held by NGF and its dynamics in the global information security industry [6].

Information security audit. An information security audit is an important tool in securing an organization's data and networks. This process is a systematic and independent review of the security system to identify vulnerabilities and verify compliance with the organization's standards and policies. Important aspects of information security auditing are threat detection, risk assessment and the development of remediation measures. Let's take an in-depth look at how auditing helps in ensuring data security in an organization:

1. Identifying vulnerabilities and weaknesses

The main purpose of an information security audit is to identify vulnerabilities and weaknesses in the system. According to the Verizon 2021 Data Breach Investigations Report (DBIR), more than 85% of data breach incidents were due to vulnerabilities that were known to the attackers ahead of time [7]. This includes analyzing network device configurations, checking for necessary patches and updates, assessing the quality of passwords and accesses, and many other aspects.

Identified vulnerabilities can be immediately remediated, which significantly increases the overall level of security. Through auditing, organizations can ensure that they are not leaving unexplored holes in the system that could be a target for attackers.

2. Assessing compliance with policies and standards

Compliance with internal security policies and standards, as well as external regulatory requirements, is an important aspect of ensuring data security. According to the PwC Global State of Information Security Survey 2021, information security breaches related to non-

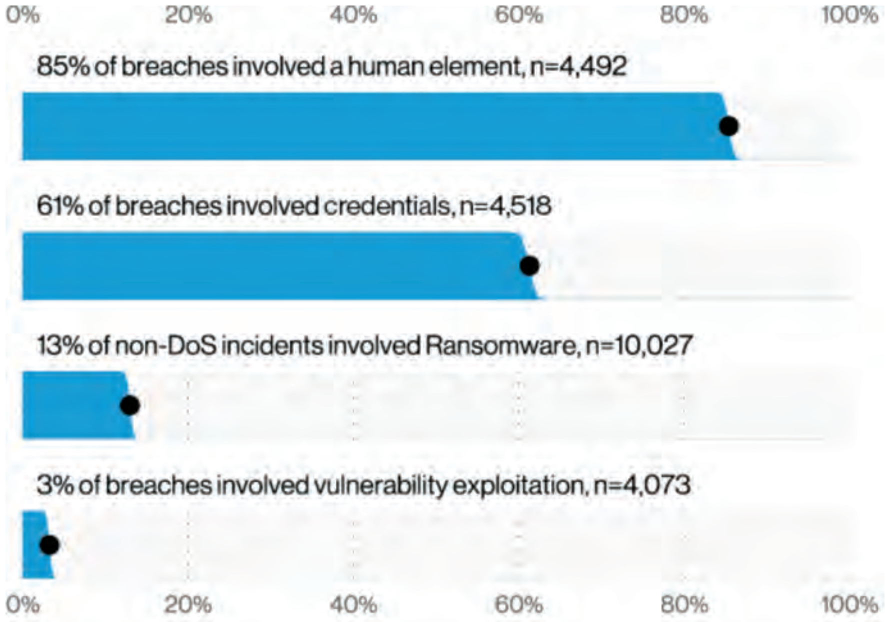


Figure 3 – Verizon 2021 Data Breach Investigations Report (DBIR)

compliance with standards and policies account for a significant portion of all security incidents [8].

An information security audit helps ensure that all necessary regulations and standards are met.

3. Unauthorized access detection

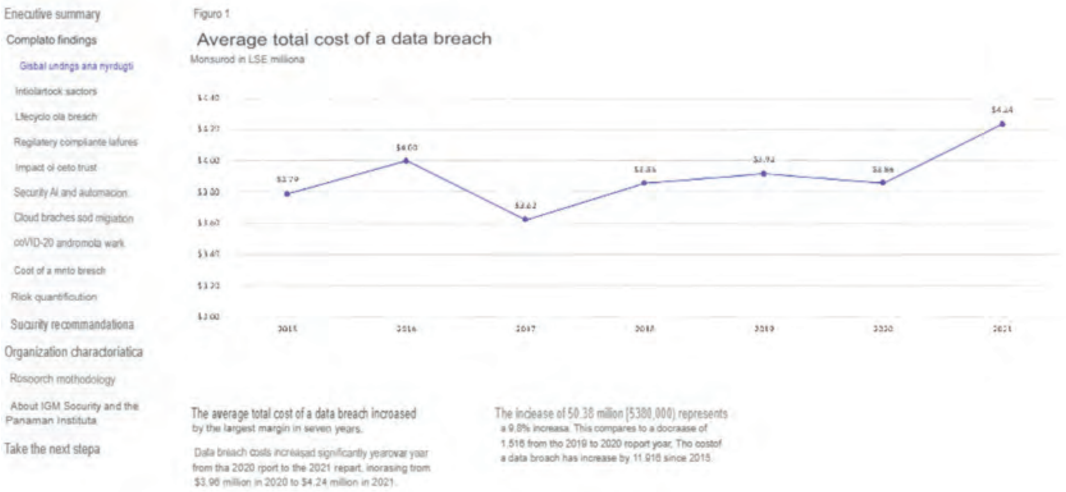
One of the most important aspects of information security auditing is detecting unauthorized access to data and systems. By monitoring audit logs, analyzing network traffic, and identifying unusual user activity, auditors can detect security incidents in real time.

According to IBM's Cost of a Data Breach Report 2021 study, increased to $4.24 million. With this approach, organizations can respond to threats quickly and effectively, preventing potential incidents that could have had serious consequences [9].

4. Improved security system

The results of an information security audit can serve as a basis for improving an organization's security system. Based on identified vulnerabilities and auditors' recommendations, organizations can develop specific action plans to strengthen data protection and prevent future incidents.

This process involves not only technical aspects, but also employee training and awareness. Since an organization's employees may be its greatest vulnerabilities, training them to follow secure practices and recognize threats is an important step in keeping data secure. In conclusion, information security audit plays an important role in ensuring data security in an organization. It helps to identify vulnerabilities, comply with standards, detect unauthorized access, and improve security. It is an integral part of a comprehensive strategy to



Enecutive summary
Complato findings
Gisbal undngs ana nyrdugti
Intiolartock sactors
Lfecyclo ola breach
Regilatery compliante lafures
Impact ol ceto trust
Security Al and automacion
Cloud braches sod migiation
coVID-20 andromola wark
Coot of a mnto bresch
Riok quantificution
Sucurity recommandationa
Organization charactoriatica
Rosoorch mothodology
About IGM Socurity and the Panaman Instituta
Take the next stepa

Figuro 1

Average total cost of a data breach

Monsurod in LSE milliona

The average total cost of a data breach incroased by the largest margin in seven years.

Data breach costs increasad significantly yearovar year from tha 2020 rport to the 2021 repart, inorasing trom $3.96 million in 2020 to $4.24 million in 2021.

The inciease of 50.38 million (5380,000) represents a 9.8% increasa. This compares to a docraase of 1.516 from tho 2019 to 2020 roport yoar. Tho costof a data broach has increase by 11.916 since 2015.

Figure 4 – IBM Cost of a Data Breach Report 2021

protect an organization’s data and networks. Adequate auditing helps to reduce risks and increase the confidence of clients and partners.

5. Employee training and awareness

The audit may also emphasize the need for information security training for employees. An organization’s employees may be its greatest vulnerabilities and training them to follow safe practices and recognize threats can significantly reduce the risk of incidents.

Conclusions. In this article, we looked at the important role of information security auditing in ensuring data protection in an organization. Various aspects of information security are explored, presenting an analysis of intrusion detection systems, firewalls, and auditing in the context of organizational data protection.

Intrusion detection systems help identify potential threats and attacks, providing a real-time response to them. Firewalls play an important role in filtering network traffic and protecting the perimeter by preventing unauthorized access. An information security audit identifies vulnerabilities, assesses compliance with policies and standards, and helps detect unauthorized access so that security can be strengthened.

According to recent statistics, data breaches and information security breaches are becoming increasingly common and can lead to serious financial and reputational losses. This emphasizes the importance of using up-to-date security tools, including intrusion detection systems, firewalls, and information security auditing.

All data security efforts are critical to maintaining the confidentiality, integrity, and availability of information. In today’s world where threats are constantly evolving, adhering to data security best practices, and conducting regular audits is a necessity for organizations looking to protect their valuable resources and ensure long-term sustainability.

REFERENCES

1 Smith, C., Jones, D. Modern Intrusion Detection Systems: A Comprehensive Review. Journal of Cybersecurity, 2022. – 10(3). – Pp. 215-230. (in Eng)

2 Wang, L., Chen, Q. Machine Learning-Based Intrusion Detection Systems: A Survey. International Journal of Information Security, 2021. – 25(4). – Pp. 542-558. (in Eng)

3 Anderson, J., Brown, M. Host-Based Intrusion Detection Systems: A Practical Approach. Information Security Journal, 2020. – 15(2). – Pp. 89-104. (in Eng)

4 Habtamu A., An Overview of Firewall Technologies, 6-7.

5 Wes N., & Ido D. Firewall Fundamentals 67-71.

6 David W Chadwick. IS Institute, University of Salford, Salford, M5 4WT, England. Network Firewall Technologies 46–52.

7 Verizon. «2021 Data Breach Investigations Report (DBIR)» https://enterprise.verizon.com/resources/reports/dbir/ (02.09.2023)

8 PwC. “Global State of Information Security Survey 2021.” https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory.html (15.09.2023)

9 IBM. «Cost of a Data Breach Report 2021.» https://www.ibm.com/reports/data-breach (28.09.2023)

Г. З. ЗИЯТБЕКОВА[1,2], А. Е. ТУРЫСБАЕВ[2], Б. Б. РАКЫМБЕКОВ[2],
Н. М. СЕРИКБАЕВ[2], Б. Ж. МОЛДАКАЛЫКОВА[3], Ж. А. БИМОЛДИНА[3]

[1]Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ақпараттық
және есептеуіш технологиялар институты, Алматы, Қазақстан;
[2]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[3]«Тұран» университеті, Алматы, Қазақстан

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ЗАМАНАУИ ТӘСІЛДЕРІ: ҰЙЫМДЫҚ ДЕРЕКТЕРДІ ҚОРҒАУ КОНТЕКСІНДЕГІ ИНТРУЗИЯНЫ АНЫҚТАУ, БРАНДМАУЭР ЖӘНЕ АУДИТ ЖҮЙЕСІН ТАЛДАУ

Қазіргі заманғы іскерлік орта ұйымдардың алдына ақпараттық қауіпсіздік саласында өсіп келе жатқан сын-тегеуріндерді қойып отыр. Кибершабуылдар мен құпия ақпараттың ағып кетуіне байланысты қауіптер деректерді қорғаудың тиімді және инновациялық тәсілдерін қажет етеді. Бұл мақалада ұйымдық деректерді қорғаудың негізгі элементтері ретінде интрузияны анықтау жүйесін (IDS), брандмауэрлерді және ақпараттық қауіпсіздік аудитін қоса алғанда, құралдар мен әдістердің жиынтығы зерттеледі.

Жұмыста осы компоненттердің әрқайсысына егжей тегжейлі шолу жасалады және олардың ақпарат қауіпсіздігін қамтамасыз етудегі рөлдері қарастырылады. Интрузияны анықтау жүйесі үшін оның шабуылдардың әртүрлі түрлерін анықтау және оларға нақты уақыт режимінде жауап беру қабілеті зерттелді. Брандмауэрлер желілік ресурстарға қол жеткізуді қалай шектейтінін және трафикті қалай реттейтінін қарастырады. Сонымен, Ақпараттық қауіпсіздік аудиті қауіпсіздік шараларының тиімділігін бағалау және әлсіз жерлерді анықтау құралы ретінде әрекет етеді. Біздің ұсыныстарымызды қолдайтын статистикалық мәліметтер мен үздік тәжірибелер ұсынылған. Мақалада осы жүйелердің интеграцияланған ақпараттық қауіпсіздік стратегиясына интеграциясы талқыланады және қазіргі цифрлық әлемде деректерді қорғауды барынша арттыру бойынша кеңестер берілген.

Бұл мақала ақпараттық қауіпсіздікті жоғары деңгейде ұстауға және құпия ақпаратты үнемі өзгеріп отыратын киберқауіптерден тиімді қорғауға ұмтылатын ұйымдар үшін құнды нұсқаулық ұсынады.

Түйін сөздер: *IDS, брандмауэрлер, ақпараттық қауіпсіздік аудиті, желілер, киберқауіп.*

Г. З. ЗИЯТБЕКОВА[1,2], А. Е. ТУРЫСБАЕВ[2], Б. Б. РАКЫМБЕКОВ[2], Н. М. СЕРИКБАЕВ[2], Б. Ж. МОЛДАКАЛЫКОВА[3], Ж. А. БИМОЛДИНА[3]

[1]Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан;
[2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;
[3]Университет «Туран», Алматы, Казахстан

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АНАЛИЗ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, БРАНДМАУЭРОВ И АУДИТА В КОНТЕКСТЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ДАННЫХ

Современное деловое окружение ставит перед организациями растущие вызовы в области информационной безопасности. Угрозы, связанные с кибератаками и утечкой конфиденциальной информации, требуют эффективных и инновационных подходов к защите данных. В данной статье исследуется совокупность средств и методов, включая систему обнаружения вторжений (IDS), брандмауэры и аудит информационной безопасности как ключевые элементы организационной защиты данных.

В работе представлен подробный обзор каждого из этих компонентов и рассмотрены их роли в обеспечении безопасности информации. Для системы обнаружения вторжений исследована её способность обнаруживать различные типы атак и реагировать на них в реальном времени. Для брандмауэров рассмотрены, как они ограничивают доступ к сетевым ресурсам и регулируют трафик. И, наконец, аудит информационной безопасности выступает в качестве средства оценки эффективности мер безопасности и выявления слабых мест. Представлены статистические данные и лучшие практики, подкрепляющие наши рекомендации. В статье обсуждается интеграция этих систем в комплексной стратегии информационной безопасности и приведены советы по максимизации защиты данных в современном цифровом мире.

Данная статья представляет ценное руководство для организаций, стремящихся к поддержанию информационной безопасности на высшем уровне и эффективной защите конфиденциальной информации от постоянно меняющихся киберугроз.

Ключевые слова: *IDS, брандмауэры, аудит информационной безопасности, сети, киберугроза.*