СЕКЦІЯ 2

МАРКЕТИНГОВІ СТРАТЕГІЇ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ СУСПІЛЬСТВА

Karamushka O.
PhD in Economics, Associate Professor,
Acting Head of the Department of Information Systems and Technologies;
Dnipro State Agrarian and Economic University, Dnipro

INFORMATION SECURITY OF PROTECTION OF STATISTICAL INFORMATION

Information has always been a key resource in today's world. With the advent of computers and mass access to the Internet, processing, transmission and storage of information have become even more important tasks. A special place among all types of information is occupied by statistical information, as it is the basis for decision-making in many areas, such as economy, science, public health, and others. The protection of statistical information is of great importance, and information security plays an important role in ensuring the security of this information.

One of the main reasons why statistical information needs special protection is its importance for decision-making at various levels. Governments, businesses, academic institutions, and community organizations use statistical data for analysis and planning. The importance of these data is that they help make informed decisions in various areas, including resource allocation, strategic planning and social programs. Therefore, the loss or damage of statistical information can lead to serious consequences for society.

To protect statistical information, it is important to consider information security as an integral part of the overall information security strategy. *This means identifying threats, assessing risks and developing appropriate security measures. In particular, information provision should include the following aspects:*

1. Confidentiality: One of the main principles of statistical information protection is ensuring confidentiality. This means that access to the data should be restricted to those who are entitled to it. Encryption, access rights and identification are tools that help ensure the confidentiality of statistical information.

2. Integrity: Another important aspect of protecting statistical information is ensuring its integrity. This means preventing illegal changes or corruption of data. The use of digital signatures and checksums can help ensure the integrity of information.

3. Availability: It is important that statistical information is available to those who have the right to it. Protection must take into account the possibility of denial of service that may occur due to technical or natural events.

4. Audit: Information support systems must have audit tools that allow tracking access to statistical information and identifying unusual activities.

Information support for the protection of statistical information also faces various challenges. One of the biggest challenges is the ever-increasing technical capabilities of attackers. Hackers and attackers are constantly developing new attack methods and using modern technologies to bypass protection. This means that information support systems must be constantly updated and improved. In addition, information security must also consider aspects of social engineering, which may include access to confidential information through manipulation of people who have access to it. Information support for the protection of statistical information should also be laid at the level of the organization's culture. Employees must be trained in security rules and understand the importance of information protection.

Information security has become an extremely relevant topic in a world saturated with digital technologies and the growing amount of data being processed and stored. Among the different types of information, statistical information is extremely important because it is used to make decisions at different levels of management, including economic, social and political aspects. This makes the information security of statistical information a critically important task for modern societies.

The concept of information security for the protection of statistical information includes a wide range of measures aimed at ensuring the confidentiality, integrity and availability of statistical data. It is important to consider that statistical information is often confidential, as it includes personal data of citizens, commercial information and other types of sensitive information. Therefore, protecting this data becomes a critical task.

The first thing to consider is measures to ensure the confidentiality of statistical information. This includes data encryption, access control and user identification, as well as auditing and monitoring of access to information. Data encryption helps prevent unauthorized access to information and keeps it safe even if intruders break in. Access control and user identification ensure that only authorized persons have access to statistical data. Auditing and access monitoring allow you to detect unusual activity and take timely measures to protect information.

The second aspect is the integrity of information. Integrity control mechanisms and backup systems are used to ensure the integrity of statistical data. Integrity control mechanisms make it possible to detect any attempts to modify information, which can be carried out both by attackers and as a result of errors in data processing. Backup ensures that data can be recovered in the event of loss or damage.

The last important aspect is the availability of information. It is important that statistical information is available to those who are entitled to it, and this requires the development of reliable systems to ensure availability that avoid leakage or blocking of information.

Ensuring the security of statistical information also requires consideration of social and ethical aspects. For example, it is important to take into account the privacy of citizens when processing personal data and comply with regulatory requirements for information storage. In addition, it is important to train staff on the security rules and ethics of statistical data processing.

In general, information security for the protection of statistical information is a critically important task in today's digital world. It requires an integrated approach that includes technical, organizational and social aspects. Only thanks to this information can be protected from threats and remain a reliable basis for decision-making in the spheres of economy, politics and society as a whole.

Білоус Д. С.,
студентка 3 курсу факультету торгівлі та маркетингу;
Чуніхіна Т. С.,
кандидат економічних наук, доцент,
доцент кафедри маркетингу;
Державний торговельно-економічний університет, м. Київ

АВТОМАТИЗАЦІЯ ОБСЛУГОВУВАННЯ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ

Тема обслуговування без людини в бізнесі є вкрай актуальною через її потенціал в підвищення ефективності роботи, зниження витрат і забезпечення безперервності сервісу, особливо в умовах, які постійно зазнають змін. Автоматизація процесів, розвиток штучного інтелекту та роботизованих систем змінюють традиційні підходи до надання послуг, відкриваючи нові можливості для підприємств та споживачів.

Сучасний світ стоїть на порозі нової ери, де цифрові технології і штучний інтелект поступово замінюють традиційні методи задоволення потреб клієнтів. Обслуговування без участі людини, яке включає в себе використання роботизованих систем, самообслуговувальних кіосків, віртуальних асистентів і повністю автоматизованих процесів, стає новим стандартом у багатьох галузях. Переваги цих сервісів включають підвищену ефективність та продуктивність, зниження витрат на персонал, а також можливість надання послуг 24/7 без втрати якості. Особливо це стає важливим у сферах, де потрібна висока точність і швидкість, таких як банківська справа, роздрібна торгівля, транспорт та логістика.

Перспективи застосування таких систем виглядають обнадійливо, з огляду на швидкий розвиток технологій і збільшення їх доступності. Впровадження автоматизованих систем і AI може радикально змінити сценарії обслуговування, зробивши його більш персоналізованим, ефективним і зручним для клієнта. Це відкриває нові горизонти для підприємств, але не без викликів. Одним із ключових ризиків є питання конфіденційності даних. З огляду на значну залежність від даних, важливо забезпечити їх належний захист, щоб уникнути неправомірного використання особистої інформації та потенційних порушень кібербезпеки.