UDC 004.77 : 004.9
DOI 10.31733/2786-491X-2023-1-152-161

Oleksandr KOSYCHENKO ©
Ph.D. (Technics),
Associate Professor
(*Dnipropetrovsk State University of Internal Affairs),*
Ukraine

Illia KLINYTSKYI ©
Ph.D. (Law)
(Silesian University),
Poland

ANALYSIS OF INFORMATION SECURITY THREATS RELATED TO THE USE OF METADATA DOCUMENTS

Abstract. The article deals with problems of a different nature that arise in any type of business activity with insufficient attention to the removal or concealment of the information contained in the metadata of various documents. Various types of documents that can contain metadata are considered, from office documents to media files. The content of metadata is analyzed, which, when accessed, can cause problems of a business, legal nature, can be used by criminals to commit financial and other crimes.

In addition, problems associated with the use of telecommunication services, such as e-mail and various instant messengers, are analyzed. Some methods of deleting metadata using various types of application tools, both online services and specific programs for various operating systems, are described. It is concluded that the analysis of metadata has already become a daily practice for specialists in developed countries. Unfortunately, the issue of metadata security in Ukraine is still in an insufficient state.

Keywords: *information, metadata, personal data, information security, fraud.*

Introduction. Any computer file has many characteristics. First of all, it is the name of the file, which consists of the name and extension. The file can then be characterized with information such as file size in bytes, creation dates, modification dates, and so on. Each file cannot appear from scratch, on its own. Files are created by people using various programs. The file must contain some information. From the point of view of an ordinary user, these are, first of all, document files, audio files, video files, photo files, and some others. Of greatest interest, of course, is the main content of the file. For example, the text of the contract, the text with the testimony of a witness, etc. The content can be consulted using the appropriate program. In recent years, it has become relevant to consider the so-called file (document) metadata. This is additional information that is created by the program and device on which this file was created.

Every day we send e-mails, some with file attachments. Each letter has not only the content, but also the date and time of sending, the title, the sender's address, and the recipient's address, the type of attachment, its volume

© Kosychenko A., 2023
ORCID ID: https://orcid.org/0000-0002-6521-0119
kosichenko-inform@meta.ua

© Klinytskyi I., 2023
ORCID ID: https://orcid.org/0000-0002-7401-8233
illia.klinicki@gmail.com

and other characteristics. This is metadata – information that accompanies the content. Every file, phone conversation, Facebook post, book, driver's license, medical record, or video has metadata. We often don't notice them. Our focus is on content. But metadata contains more valuable information than we used to think. Sometimes, using metadata, you can track down a person, get dirt on him, and completely change his life.

Researchers and experts often divide metadata into three categories:

– Descriptive metadata. A person uses them to identify and search for information. As a rule, users face them on a daily basis. Example: file name;

– Structural metadata. How information is organized, how navigation works. Example: a link between two pages of a website that allows you to display a link under article A to article B;

– Administrative metadata. Who, when, where and how information was created and processed. Example: licensing restrictions on the dissemination of information.

Although the term "metadata" is the same, the scope is different. Metadata is stored in a variety of places. For example, in music files of the popular MP3 format, metadata (here they are called ID3 tags) in special "frames" within the file itself. When you open an MP3 file in your player, you can see the artist name, song title, and even genre. The player learned this information from the metadata. An email has metadata in its header. Typically, the sender and recipient only see a subset of the metadata in their email programs. Your metadata can be accessed by a variety of people and organizations. For example, email headers are available not only to the sender and recipient, but also to email providers. The owner of the site you visit can find out not only your IP address, but also your browser and operating system versions. Very often, metadata is available to the general public and is not protected in any way, either by nature or by human negligence. Metadata can be centrally processed. It happens that the types of metadata are "mixed". One and the same information can be considered as metadata in these conditions, in others – as data (content). For example, the same e-mail header: it can be very informative. To solve professional problems, experts in different fields often develop their own, narrower categories of metadata.

Analysis of recent research and publications. Again, metadata is defined as data that describes other data. It provides information about the context, content, and structure of data, making it easier to locate and use. Several recent studies have explored the challenges and opportunities associated with metadata management in various contexts. For example, a study by Tallerås et al. (2018) examined the use of metadata in Norwegian museums and archives, highlighting the need for standardized metadata schemas and best practices for metadata creation and maintenance. Another study (Broughton et al., 2019) investigated the use of metadata in digital libraries, emphasizing the importance of user-centered approaches to metadata design and implementation. One type of metadata that has gained popularity in recent years is the Facebook pixel. The Facebook pixel is a code that can be embedded in a website to collect data on user behavior, such as page views, clicks, and conversions. This metadata is used to create targeted ads and measure the effectiveness of advertising campaigns (Facebook).

Elaborating on this, the article "Metadata Analysis of Web Images for

Source Authentication in Online Social Media" (Shaliyar et al., 2022) explores the use of metadata analysis as a means of authenticating the source of images shared on social media. The authors highlight the importance of accurate metadata in determining the authenticity of images, and describe a methodology for analyzing image metadata to identify any discrepancies that may indicate image manipulation or misattribution. The study concludes that metadata analysis can be an effective tool for source authentication in social media, and suggests that further research is needed to explore the potential of metadata analysis for other types of digital media.

There is a growing body of research on metadata that takes into account a more general perspective. Such studies aim to explore the broader implications of metadata beyond its immediate application or context, and to examine its role and impact in various domains and disciplines. For instance, researchers have investigated the ethical, legal, and social implications of metadata practices, the interoperability and standardization of metadata across different systems and platforms, and the potential of metadata for enhancing information retrieval, preservation, and access. These studies provide valuable insights and knowledge on the complex and dynamic nature of metadata, and offer new perspectives and directions for future research and practice. In "Understanding Metadata" (2017), Jenny Riley discusses several challenges associated with creating and managing metadata.

One of the main challenges she highlights is the need for standardization and interoperability across different systems and domains. This challenge is particularly relevant given the proliferation of metadata standards and the diversity of information resources that require metadata. Another challenge Riley discusses is the lack of consistent and accurate metadata. She notes that metadata creators often face difficulties in determining the appropriate level of granularity for metadata and in ensuring that metadata is consistent across different resources. Additionally, metadata quality can be compromised by errors or omissions, which can affect the discoverability and accessibility of information. Riley also addresses the challenge of metadata sustainability, which refers to the long-term management and preservation of metadata. She notes that metadata must be regularly maintained and updated to ensure that it remains relevant and usable over time. This requires ongoing investment in metadata creation, management, and preservation infrastructure, which can be a challenge for organizations with limited resources. Overall, "Understanding Metadata" highlights the complex and multifaceted nature of metadata creation and management and underscores the importance of addressing these challenges to ensure the effective use of metadata in facilitating access to information.

Diving into the local (Ukrainian) perspective, it should be noted that the basic legal acts of the information legislation of Ukraine, such as the Law of Ukraine "On Information", "On Protection of Personal Data", "On Electronic Documents and Electronic Document Management" and others do not give the concept of metadata. Documents of various departments are cited for definition metadata of a specific type, which can be easily traced using a search on the website of the Verkhovna Rada of Ukraine, however, according to Article 100 of the Civil Procedure Code of Ukraine, Article 96 of the Economic Procedure Code of Ukraine and Article 99 of the Code of Administrative Procedure. In Ukraine, electronic evidence is information in electronic (digital) in a form

containing data on circumstances relevant to the case, in particular, electronic documents (including text documents, graphic images, plans, photographs, video and sound recordings, etc.), websites (pages), text, multimedia and voices and messages, metadata, databases and other data in electronic form (Gutsalyuk et al., 2020). In other words, we can say that everywhere they talk about metadata, confirm that they have the right to be, even when they are defined, while the Law of Ukraine "On Information" does not provide a definition. In other countries, much more attention is paid to personal and metadata, their definition, legal status.

The purpose of the article is to analyze the problems and ways to solve them that arise when information is leaked in the metadata of files of various types.

Formulation of the main material. Metadata is data about data, information about information. In other words, it is technical information contained in documents of various formats, which is not visible during normal use. According to the Dublin Core Metadata Initiative (DCMI), metadata is "information that describes, explains, or provides a way to access, manage, and use resources" (Dublin Core Metadata Initiative, 2012). Metadata is essential for data discovery, retrieval, and interoperability in various domains, such as digital libraries, archives, e-commerce, and social media.

Metadata is often placed in a document by the software or hardware from which the document was created. Since this process is automated, the user may remain unaware of the existence of such data, and not take measures to protect this information, which is often of particular importance.

Document types that contain metadata include MS Office documents, Adobe PDF, Corel Word Perfect, images created by Corel DRAW, Adobe Photoshop, created or processed by various GIF and JPEG bitmap editors, MP3 audio files, video files, web pages, electronic letters. These are the most common formats used on various office platforms in daily activities.

Metadata can include the name of the document's author, organization, software or hardware label, document modification history, and so on. In particularly complex cases (MS Word), it can even be text that was once included in the document, but later deleted, but is stored in the document file as metadata. Metadata can also be present in the source code of application programs in the form of developer comments, and in executable files.

It should be noted that most users believe that converting a document from MS Word to PDF format destroys all metadata in the document. This is not always the case, and a prudent document author must first remove the metadata from the source document (there are special programs for this), and then convert it to PDF format. Similar problems and methods of solving them also exist for other file formats.

Certain hidden vulnerabilities related to metadata in legal activities can be noted. For example, the risk for a lawyer is that, no matter how careful he is, a document he transmits electronically may contain metadata that is hostile to his client's interests or, in the worst case scenario, reveals the client's secrets or confidential information. Many practicing lawyers in small and medium-sized firms do not know what metadata is at all, or do not understand the possible potential risks. In the process of preparing the final document, a lawyer who uses all the text or data processing tools on his computer goes through several stages, all of which are supposedly hidden in the document and invisible to

everyone except the lawyer himself. The reality, however, is that the document's history is embedded in its files and is effectively available to anyone, including opposing counsel, who receives the document electronically.

Despite all its specificity, metadata is sometimes considered by courts as evidence, including when justifying a position in a case. For this, it is only necessary to have elementary technical skills. Metadata research also plays a significant role in investigations of copyright violations, detection of plagiarism or attempts to falsify documents. The fact of using the EXIF tag as evidence in a criminal case is known.

A typical example of a hardware (and not only hardware) tag can be the so-called EXIF tag (Exchangeable Image File Format tag). It is a hidden part of the document file. It is in this part that metadata is contained. The word tag is translated exactly as a "label" or even a "price tag, label" contained in a file taken by photographers in JPEG format (or in another format) with digital cameras. This metadata includes, among others, such data as the date, time, mode of shooting the frame, and others. The EXIF tag allows you to store a lot of useful information: from shooting parameters to information about which program and how the photo frame was edited for one or another purpose. Another interesting example of hardware placement of metadata is marking a paper printout with color laser printers.

The risks arising from the use of metadata can be divided into two main groups: 1) the use of code and 2) the disclosure of significant information. For example, e-mail metadata are characteristics of messages that, without providing the content of the message, determine the addressees of correspondence and some other circumstances of this process. More precisely, e-mail metadata includes: the sender's name, his postal address, his IP-address on the Internet, the name of the recipient, the unique identifier of the message and related messages; date, time and time zone of sending and receiving the message; message header formats; the subject of the letter; message status; request for confirmation of receipt and opening of the letter. As you can see, the collection of metadata of the mail service can give a detailed picture of the activity of some user, even if he encrypts his messages. At the same time, collecting data is quite simple.

Firstly, because the metadata of telecommunication services – mail, mobile communication, web services and others – are either not protected by the legislation of most countries at all, or are protected to a much lesser extent than the content of the service messages themselves. That is, while the disclosure of the content of correspondence on the Internet requires a court decision, the collection of metadata is not considered an attack on information security and can be carried out without hindrance.

Secondly, it is easier to tie the metadata of e-mail to a specific user. Email metadata is stored on the sender's and recipient's computers (as well as the messages themselves), but, dangerously for user privacy, also in the logs of the mail servers that transmitted those messages. Metadata of users of a mail service is much easier to find on the servers of providers than metadata of users of a web service. The provider of the hotel, train station or cafe where they are temporarily staying, or through a public mail server such as Gmail. The user receives mail also through a certain server on which he has an account. This situation is not similar to a web service, where a user can visit any server on

 ISSN 2786-491X (Print)

the Internet, so it is almost impossible to find traces of his visits by checking the servers, even if the user registered on some of them.

The value of metadata is well understood and used by special services and police in some countries. Such technologies realize mass collection and analysis of metadata of mobile users. At the same time, privacy laws prohibit wiretapping, but they do not prohibit the collection of mobile phone customer metadata.

It should be noted that, in general, threats and vulnerabilities in the processing of metadata have not yet been sufficiently investigated by cyber security specialists. With the general gigantic growth of information volumes, metadata is becoming more and more widespread as a means of data indexing (a way to speed up the search for information in information systems). As a result, new (or already existing) vulnerabilities appear, and new code implementation methodologies are developed.

Another group of risks includes disclosure of information contained in metadata. This can be confidential or trade secret information, e-mail addresses, file paths on the system on which the document was created or processed, other information about the author and his software and hardware.

The leakage of information through metadata in MS Office documents has given rise to some incidents that have gained international publicity. In one case, it was a document signed by the prime minister of one of the countries, which related to the international situation. Examination of the file revealed text removed from it, containing information not intended for open access. Another case added to the long history of the lawsuit of one of the companies against many other companies. An analysis of the lawsuit filed by a law firm representing the firm's interests showed that the name of one of the major banks was removed from the text – so the bank was one of the targets of the lawsuit, but for some reason the firm's lawyers refrained from making claims against the bank. For a knowledgeable and interested person, this is important information.

Metadata is usually ignored as a threat to digital security because we focus on the content of the file. But sometimes they can turn out to be more useful than the file itself and become a source of information about a potential victim at the first stage of a social engineer's work.

Based on the metadata of the photo games that you have published on social networks, you can calculate the main routes of movement around the city: where you live and work, your favorite cafes and shops. If you send photos via messengers as an attached file, additional information is also sent with them – technical characteristics and model of the device on which the photo was taken, date of shooting and geolocation. Thus, having a number of images of the same author, it is possible to judge the presence of certain gadgets, the daily routine, travel routes and other details of private life (Luther, 2022; Kosychenko & Rybalchenko, 2022; Rybalchenko et al., 2022).

The attacker can use the received information to prepare a scenario of actions and the necessary means of social engineering attacks (phishing resources, malicious attachments, etc.), as well as to win the user's trust.

Metadata can also be used in attacks on organizations. For example, an attacker can prepare an exploit (a program that uses vulnerabilities in software to attack a computer system) by knowing the version of the software. Moreover, in the metadata of MS Office documents, you can see the author of the file, usually this is the first name or the current login of the operating

system. Accordingly, carelessly published company documents can become a source for login dictionaries. Fraudsters willingly use them in the process of sifting through credentials on available company resources. From the attacker's point of view, the metadata is more useful than the file itself. They are especially likely to be used in social engineering attacks. Digital Security analysts advise to get rid of metadata, this can be done through the "Properties" section. To do this, click on the "Details" tab and edit or delete the metadata by clicking on the "Remove properties and personal information" link and selecting the desired items. In messengers and mail, users send countless documents and photos, and few remember that the files being sent contain automatically assigned data about them: the date and time of creation, the name of the author, the version and technical characteristics of the program or device and, of course, the location mark, which deserves special attention.

These digital footprints are capable of playing a wicked joke. Therefore, if you do not want to share personal information with third parties, delete the metadata. And to hide your location, you should disable geolocation in the camera settings. The presence of metadata in each file is just another reminder that users themselves can become the culprits of leaking their own personal information or their company's sensitive information.

Most social networks, messengers and platforms automatically remove the metadata of image files if you upload them using the Camera function and not as a document attachment. With this method of sending an object to Telegram, WhatsApp or Viber, the picture or video will not contain information about the user's device, software and other characteristics. However, text file metadata is preserved regardless of platform and download method. When placing graphics on photo stocks such as Unsplash, Pinterest, Pexels, the metadata completely disappears, and if you send files through mail services – they remain.

Here are options to reduce the amount of metadata:

– Use software instead of online services. Open source applications help generate less metadata than web tools;

– Remove metadata. Programs have been developed for various OSes that help get rid of this type of information. For the Windows operating system, this is MS Office Document Inspector (text documents), for Mac OS – ImageOptim (graphic files).

In general, there are many programs, websites, and software that allow you to remove metadata. Here are some of them.

Online tools. Websites and online tools are a great option if you're short on time. No need to download or install anything. You simply upload your file, click a button, and then download it without metadata.

MetaClean – a free online tool from Adarsus, a Spanish IT and cyber security company. MetaClean can be used to view and remove all metadata from files of various formats. It works with images, videos, PDF and Docx files, as well as mp3 tracks and many other files.

PDFYeah – a free online all-in-one PDF solution. PDFYeah has a special program for removing metadata from PDF files. Moreover, unlike MetaClean, this tool has a maximum of 50 MB. PDFYeah lets you work with large files without compromising your privacy. MetaCleaner – a comprehensive and professional online metadata removal tool. MetaCleaner allows you to remove

 ISSN 2786-491X (Print)

metadata from more than 40 different file formats directly on websites. MetaCleaner provides encrypted communication, guarantees confidentiality, as well as compliance with the European requirements for the protection of personal data GDPR.

Online tools are great for getting the problem resolved quickly. However, they are inconvenient if multiple uploads and downloads of files are required. For example, if you need to regularly clean large files from metadata.

Metadata Touch – a professional tool that supports more than 30 file formats, from MS Office and Open Document files to various image, audio and video formats, including scalable vectors and compressed audio files. Metadata Touch is great for bulk editing or deleting metadata. It allows you to customize different file formats and metadata fields to suit your needs. Metadata Touch only works on Windows.

Mobile applications. Online tools and software can be a great option when using a desktop device, but there are also mobile apps for removing and editing metadata. You can install them directly on your smartphone or tablet.

Scrambled EXIF – an open source Android smartphone and tablet application used to remove EXIF metadata from images. The program allows you to simultaneously remove metadata from several images. You can also access application settings and control data type and metadata. For example, you can force the program to automatically rename images because images often contain a date and time. EXIFTool – another open source Android application that removes metadata from various files. Compared to Scrambled EXIF, EXIFTool does not allow bulk metadata removal. But EXIFTool can be used with a wider range of file formats, from images, audio files and video files to text documents such as PDF and Docx. Instead of simply removing the metadata, EXIFTool allows you to edit it right on your smartphone or tablet. Although the process is manual, the result is more customized. You will only send approved files to other people or to the open Internet.

In general, removing metadata should become a habit in many activities. By using effective time-saving tools and programs, you can get into the habit of cleaning up metadata before emailing or posting to the web. It's just a matter of finding the right tools and being motivated to protect your privacy online.

Conclusions. The conclusion from the above is simple – the use and protection of metadata of documents, photos, audio and video should be given more attention in all activities where files containing important information are used. At the same time, it should be noted that there is no metadata protection at all. Encrypting the document file does nothing to hide them. There are methods to remove metadata from documents before they are used or sent. Unfortunately, both in legal and business practice, attention is not always paid to this, which leads to various problems.

Metadata analysis has already become a daily practice for lawyers and other professionals in developed countries. Unfortunately, security issues related to metadata in Ukraine still remain at best open, rather they have not yet been properly addressed both at the legislative and practical level. Perhaps in the future, legislation in the field of personal data protection will be stricter, and metadata as well as personal data will become more protected.

Conflict of Interest and other Ethics Statements

The authors declare no conflict of interest.

References

Are Your Documents Leaking Sensitive Information? Scrub Your Metadata! Authors: Michael Spiegel. URL : https://er.educause.edu/blogs/2017/1/are-your-documents-leaking-sensitive-information-scrub-your-metadat.

Broughton, V., Hiom, D. & Dovey, J. (2019). User-centered metadata: A study of use and utility in digital libraries. Journal of Documentation, 75 (5), pp. 997-1015. Doi : https://doi.org/10.1108/JD-07-2018-0120.

Dublin Core Metadata Initiative. (2012). Introduction to Dublin Core. URL : https://www.dublincore.org/specifications/dublin-core/dces/.

Facebook. URL : https://www.facebook.com/business/help/952192354843755.

Finn, B. (2022). How to Protect Yourself from Metadata. Global Investigative Journalism Network. By Reporters Without Borders. URL : https://gijn.org/2022/04/13/how-to-protect-yourself-from-metadata/.

Gutsalyuk, M., Havlovskyi, V. & Khakhanovskyi, V. et al. (2020). Vykorystannya elektronnykh (tsyfrovykh) dokaziv u kryminal'nomu provadzhenni : metod. [Use of electronic (digital) evidence in criminal proceedings: method.]. Ed. 2nd, add. Kyiv: Ed.-vo Nats. Acad. of Internal Affairs, 104 p. [in Ukr.].

Holmes, H. Digital Asset Management. A Metadata Guide. URL : https://www.acquia.com/blog/metadata.

Introduction to Metadata. Third Edition. Edited by Murtha Baca. URL : https://www.getty.edu/publications/intrometadata.

Is Metadata a Threat to Your Online Security? URL : https://fastestvpn.com/blog/is- metadata-a-threat-to-your-online-security.

Kosychenko O. & Rybalchenko, L. (2022) Peculiarities of using visual means of information and analytical acticiti in legal and law enforcement sphere. *Philosophy, Economics and Law Review*, 2 (1), pp. 162-169.

Luther, D. (2022). What Is Metadata & Why Is It Important? Oracle netsuite, May, 19. URL : https://www.netsuite.com/portal/resource/articles/data-warehouse/metadata.shtml.

Mateeva-Stoyanova, Z. (2020). Principles of personal data protection. *Xüsusi buraxılış. Special Issue. Audit,* 2 (28), pp. 95-104.

Metadata in Digital Media. URL : https://sector035.nl/articles/metadata.

Smirnov, S. Metadata: digital footprints that we (almost) don't notice. URL : https://te-st.org/2020/02/12/metadata/.

Riley, J. (2017). Understanding metadata. Washington DC, United States: National Information Standards Organization, 23, pp. 7-10. URL : http://www.niso.org/publications/ press/UnderstandingMetadata.Pdf.

Rybalchenko, L., Kosychenko, O. & Klinitskyi, I. (2022). Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review,* 2 (1), pp. 96-102.

Shaliyar, M. & Mustafa, K. (2022). Metadata Analysis of Web Images for Source Authentication in Online Social Media. In: Rushi Kumar, B., Ponnusamy, S., Giri, D., Thuraisingham, B., Clifton, C.W., Carminati, B. (eds) Mathematics and Computing. ICMC 2022. Springer Proceedings in Mathematics & Statistics, vol 415. Springer, Singapore. Doi : https://doi.org/10.1007/978-981-19-9307-7_7.

Tallerås, K. H., Oltedal, S., Aalberg, T. & Liestøl, G. (2018). Metadata practices in museums and archives: The case of Norway. *Journal of Documentation*, 74 (4), pp. 812-827. URL : https://doi.org/10.1108/JD-07-2017-0091.

Олександр КОСИЧЕНКО, Ілля КЛИНИЦЬКИЙ

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ДОКУМЕНТІВ З МЕТАДАНИМИ

Анотація. В останні роки стало актуальним розглядати так звані метадані файлу (документу). Це додаткова інформація, яка створюється програмою та пристроєм, на якому відбулося створення цього файлу. Аналіз метаданих уже став щоденною практикою для юристів та інших професіоналів у розвинених країнах. На жаль, питання безпеки, пов'язані з метаданими, в Україні досі залишаються в кращому випадку відкритими, точніше, ще не вирішені належним чином як на законодавчому, так і на практичному рівні.

У статті розглядаються проблеми різного характеру, які виникають у будь-якому виді діяльності з недостатньою увагою до видалення або приховування інформації, що міститься в метаданих різних документів. Розглядаються різні типи документів, які можуть містити метадані, від офісних до медіафайлів. Аналізується вміст метаданих, доступ до яких може викликати проблеми ділового, правового характеру, яки можуть бути використані зловмисниками для вчинення фінансових та інших злочинів. Крім того, аналізуються проблеми, пов'язані з використанням телекомунікаційних сервісів, таких як електронна пошта та різноманітні месенджери.

Описано деякі способи видалення метаданих за допомогою різних типів прикладних засобів, як онлайн-сервісів, так і спеціальних програм для різних операційних систем. Зроблено висновок, що аналіз метаданих уже став повсякденною практикою для фахівців розвинених країн. На жаль, питання використання та безпеки метаданих в Україні все ще перебуває в недостатньому стані.

Ключові слова: *інформація, метадані, персональні дані, інформаційна безпека, шахрайство.*

Submitted: 09.01.2023
Revised: 20.01.2023
Accepted: 07.02.2023

UDC 336.221.26
DOI 10.31733/2786-491X-2023-1-161-170

Tetyana ZAHORELSKA©
Ph.D. (Economics), Associate Professor *(Prydneprovs'ka State Academy of Civil Engineering and Architecture)*, Ukraine

Biswajit DAS©
Ph.D. (Management), Professor *(Institute of Industrial technologies (KSOM))*, Odisha, India

EFFECTIVE TOOLS OF CONTROL AS A COMPONENT OF TAX MANAGEMENT

Abstract. The article deals with the actual issues of tax management with focuse on VAT. Tax analysis is an important tool for assessing the tax burden on an enterprise. It allows you to identify the most significant factors influencing the dynamics and structure of taxes and fees, as well as to find opportunities to minimize tax payments. To achieve these goals, it is necessary to conduct an analysis of the dynamics and structure of tax deductions, calculate the relative tax burden, and conduct analytical reasoning regarding the lost benefit of minimizing tax payments.

A tax analysis was conducted based on the amount and structure of taxes paid by a domestic enterprise that provides services, the tax burden for value added tax was calculated, the results of tax planning for VAT were determined, and the system of internal control over its calculation was improved. Special attention was paid to the development of the stages of tax analysis and the development of a working document for internal control – a table in which

© Zahorelska T., 2023
ORCID ID: https://orcid.org/0000-0002-9465-7411
zahorelska.tetiana@pdaba.edu.ua

© Das B., 2023
ORCID ID: https://orcid.org/0000-0002-0817-2929
biswajit@ksom.ac.in