ISSN: 2181-3337 SCIENCE AND INNOVATION
INTERNATIONAL SCIENTIFIC JOURNAL
2022
№ 3

PROTECTION OF INFORMATION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS FROM THE POINT OF VIEW OF DATA LEAKAGE

Muminova Sunbula Shaxzodovna
Seniour Lecturer, TUIT named after Mohammad al-Khwarizmi
Sidiqov Saidxon Murodjon o'g'li,
Sidiqov Bositxon Murodjon o'g'li
Students of TUIT named after Mohammad al-Khwarizmi

https://doi.org/10.5281/zenodo.6803326

Abstract. *Modern office work is impossible without the use of electronic document management programs. EDMS has been implemented in most large public sector organizations, and small businesses are gradually moving to it. Somewhere solutions are implemented on simple platforms, for example, based on 1C, somewhere more technologically advanced software options are used, integrated into the overall volume of enterprise automation. This article reviews several types of electronic document management systems, their capabilities and, of course, their shortcomings. The issues of information security in electronic document management systems, in particular, protection against leaks, are also analyzed.*

Keywords: *EDMS, data leakage, data protection, unauthorized copy, EDMS software.*

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ТОЧКИ ЗРЕНИЯ УТЕЧКИ ДАННЫХ

Аннотация. *Современная офисная работа невозможна без использования программ электронного документооборота. СЭД внедрена в большинстве крупных организаций государственного сектора, и малые предприятия постепенно переходят на нее. Где-то решения реализуются на простых платформах, например, на базе 1С, где-то используются более технологичные программные варианты, интегрированные в общий объем автоматизации предприятия. В этой статье рассматриваются несколько типов систем электронного документооборота, их возможности и, конечно же, их недостатки. Также анализируются вопросы информационной безопасности в системах электронного документооборота, в частности, защиты от утечек.*

Ключевые слова: *СЭД, утечка данных, защита данных, несанкционированное копирование, программное обеспечение СЭД.*

INTRODUCTION

Modern office work is impossible without the use of electronic document management programs. EDMS has been implemented in most large public sector organizations, and small enterprises are gradually moving to it. Somewhere solutions are implemented on simple platforms, for example, based on 1C, somewhere more technologically advanced software options are used, integrated into the general scope of enterprise automation. EDMS allows you to simplify and optimize the process of creating, coordinating, storing documents of any level of importance. But users are often concerned not only with the issue of convenience of working with the program, the task of preserving important information when working with contracts or correspondence becomes urgent.

The essence of the EDMS system is simple. Each document of a general administrative and legal nature that arises in the company - an order, a contract, an internal regulation - becomes

the basic unit to be processed in the EDMS. Accounting and production documents (waybills, invoices, waybills) are usually not processed in this way. But this rule only works for standard programs that provide office work.

Multifunctional modern software products offer additional financial blocks and CRM modules that store and process information related to customer interaction. If counterparties under any agreement have decided to sign all related applications with an electronic signature (ES), invoices and invoices will be included in the document management system, which will be exchanged between the supplier and the buyer or the customer and the contractor, while information from them will be promptly downloaded in accounting and production modules.

The presence of electronic signatures generated by different certification authorities will not become a problem if the software developer has provided the user with the opportunity to work with different certificates. This is provided for in most software products that work with ES as a necessary option, that is, for everything except simple ones designed for office workflow.

During processing, the document receives its unique number and a card in which all stages of its life are marked. The card contains the following information:

- initiator - person and subdivision;
- target character;
- price (if it is provided, for example, for contracts);
- classification - general business contracts, orders, assignments, protocols;
- approval route, it can be different for the head office and branches, for documents of different purpose, different cost - the matching departments change;
- remarks made during sighting and their fate;
- date of final sighting;
- appointed executors;
- performance results;
- expiration date.

Throughout its life, a document in one form or another - a picture or a text file - travels through networks within a company and is displayed on monitor screens. On this way, it can be repeatedly copied, intercepted, photographed from the screen. Therefore, when choosing an EDMS system, security services raise the question of how reliable the proposed solution is in terms of storing and ensuring the security of confidential information.

MATERIALS AND METHODS

OVERVIEW OF EDMS PROGRAMS

The choice of EDMS is a task consisting of several subtasks - determining the price, the degree of information protection, functionality.

Depending on the functionality of the EDMS systems are divided into several groups:

- programs that work mainly as an electronic archive. When choosing such programs, the emphasis is on the convenience of storing documents and searching through the database, it can be more or less clear or fuzzy, by name, purpose, phrases from the text, and other attributes;
- products that focus on the convenience of workflow (routing). It clearly spells out the process of creating and processing the basic unit of information, which changes at each stage of his journey. Routing is usually set rigid, prescribed by programmers for each type initially;

- hybrid type systems that combine the advantages of the two previous ones. They are characterized along with hard soft routing, when the path of a particular file is set independently by the head of the corresponding department;
- EDMS, involving joint work with files (collaboration). They are not initially set up for a rigid hierarchy and create convenience for design work, when each member of the group contributes to the processing of a common solution. Since they often use the forum type of discussion and the placement of files on publicly accessible sites, security issues are the most poorly resolved in them;
- multitasking products with additional services. So, CRM can be built into the workflow, and not vice versa.

The issue of data security is relevant for all programs, but its solution depends on another level of classification - the type of EDI itself. Systems can be:

- independent modules;
- cloud solutions;
- CRM modules or other enterprise management software.

The choice will also be based on who the software developer is. Recently, government policy has been aimed at supporting domestic software products.

Now the following solutions are on the market that enjoy the attention of users, but, unfortunately, in the description of the functionality of most of them by the developer, the security issue is poorly covered:

- ***Softline Go Remote***. Its advantage is the ability to control the process of general work based on the Gantt chart. There is no CRM functionality. The system for transporting and storing documents is implemented in Windows Exchange, which gives an idea of the overall degree of security.
- ***"1C Document Management"***. The task of protecting information in EDMS is solved in a standard way for a family of programs and depends on where exactly the files are stored - in the cloud or otherwise, on the server. User rights are ranked.
- ***"E-XAT"***. Router software is designed for streamlined office work. The safety of documents is entirely in the hands of the IT service of the enterprise, since it determines the security mode and access rights on its own.
- ***MyGov***. It has advanced functionality, helps in working with projects, financial tasks, citizens' appeals (for public services). Archiving is based on the principles of Russian legislation. The security of information is ensured by the fact that for third-party visitors the files are presented in the format of a reading room. The access control model has been implemented. Encryption and EP are used. Multifunctional system with good security version. The login model is implemented only from trusted devices, login by token and certificate.

RESULTS

DATA LEAKS: OPPORTUNITIES AND PRACTICES

Security officers often test electronic document management programs for the possibility of data leaks. In practice, high-level EDM systems provide greater protection against information loss than in a situation where files are simply stored in a database, on a server or users' computers, are not archived, are not encrypted, copied uncontrollably and transferred between counterparties

via unprotected communication channels of telecommunication networks. However, there are risks associated with their use:

– unauthorized access of third parties to the archive of documents when it is stored both on the server and in the "cloud";
– leakage of documents or information during transmission over insecure communication channels or in unencrypted form;
– copying or modifying files by users.

Most EDMS products include technical solutions that eliminate all or most of the risks, except for the risk of copying. These are such solutions for the protection of confidential information as differentiation of user rights, access control, encryption of documents during storage and transmission, the ability to work only with page photos, and an electronic signature. The choice should also be based on which of these means are implemented in a particular proposal. In the case of a full-fledged technical solution, the degree of safety of information and their text versions is significantly increased compared to the usual type of processing.

An integrated approach to data leakage protection is implemented in DLP systems.

WAYS TO PROTECT INFORMATION FROM LEAKS

The process of protecting information in electronic document management systems includes three tasks:

1. Protecting the archive of files and information from destruction and other threats in the event of hardware failures or as a result of intentional user actions. Thus, the accumulated archive may well be lost. And if undigitized paper originals may remain for previously created ones, then files already created in electronic form may perish forever.
2. Protection of information from leaks when it is in the EDMS or when transferred to the cloud storage or counterparties.
3. Protection of information from copying in any way.
4. Protection of data from destruction.

Risks such as deliberate distortion of data, substitution of routes, hacker attacks are also often mentioned. But in practice, they have already been solved by the developer, and the first and second risks are easily identified by each next appointed performer or during his registration, and protection against hacker attacks will be common to the entire organization.

All these tasks are solved in different ways, both at the level of software product developers and at the level of security services and IT departments of the enterprise. Independent construction of a threat model and its reflection in the architecture of an EDMS bucket program will not be appropriate solutions; each developer is already ready to offer a holistic data protection concept that provides for all current threats. This rule does not work only for very simple versions of programs that will have to be backed up with independent protection methods, additional modules and cryptographic tools.

Organizational security measures remain important, consisting in increasing the responsibility of employees when working with confidential data. Legal methods are traditionally used here, namely:

– development of regulations on trade secrets;
– inclusion in the list of confidential information of all copies and final versions of files contained in the EDMS;

– Inclusion in employment contracts of employees of a clause on liability for disclosure of trade secrets.

In addition, standard control over the actions of employees is necessary. According to company that learns data leakage SearchInform's research, the human factor causes 74% of valuable data leaks. Controlling the admission of external visitors to employees' offices and eliminating the possibility of third parties taking pictures of documents using a mobile device is also one of the tasks of the security service. The problem is solved in various ways - from holding negotiations only in special rooms to the mandatory requirement to turn off computers when organizing meetings.

The task of protecting information from leakage or destruction in electronic document management systems is solved at several levels:

– differentiation of user rights;
– the use of an electronic digital signature (EDS), only if it is available, full-fledged work with files is possible;
– cryptographic means of protection that encrypt data during transmission;
– transfer of information only via secure HTTPS protocols;
– logging user actions;
– control of entering the program. Modern solutions include models of trusted devices, tokens (special tools with electronic keys and PIN codes) and certificates that allow access only from specific devices. The problem is that keys and certificates are stored with users, and there is a risk of transferring them or trusted devices to third parties.

How to protect a document from copying. In practice, there are practically no electronic document management systems that could protect information from paper copying, and such solutions are quite expensive. There are options when systems with such functionality are already built into the general enterprise automation environment. If neither the first nor the second way to solve the problem is available, technical devices are offered on the market that help to cope with the problem autonomously.

Leak control programs for confidential paper documents can be connected to the EDF. The essence of the solution is that each user receives an individual copy of the electronic document, which is visually indistinguishable from the original. The software product does not increase the number of file copies and does not make it possible to archive them in the document management system, but allows you to save several important parameters in the database, namely:

– algorithm for converting a letter or contract;
– date and time of creation of an individual copy;
– information about the employee to whom the copy was provided.

This means that if during an internal investigation a leak of files in paper form or in the form of a photograph from the screen was revealed, the program, when comparing this copy, will instantly determine which employee is guilty of a particular leak. Informing about the implementation of this mechanism in the enterprise will play a preventive role in preventing leaks. Each employee will now know for sure that his actions to work with confidential data will be quickly identified.

DISCUSSION

*Protection from destruction. A*lso an important organizational task is to ensure the physical security of electronic documents and the servers on which they are stored. The

advantage of the electronic version of the contract or letter is that for it there is no concept of an original and a copy. All documents generated and signed with the electronic signature of an authorized person are originals, so timely backup of the archive with the condition of storing copies separately from the common database solves the problem.

From the physical destruction of information, electronic document management systems located in the "cloud" are better protected. Protecting information in this way has its drawbacks. The human factor can work here too: the IT specialist who carries out the backup may make a third copy for an unnamed competitor customer. Such issues are resolved on a case-by-case basis at the level of security services, and the solution will be to commission backups to third parties and copy only encrypted versions of the archive.

The integrity of information allows you to maintain access control to the archive and a particular file. Usually, users have the opportunity to work only with photographs of text, entering their comments in a special form and not having manual access to the archive, editing and deleting rights.

The risks of losing data in the cloud storage are eliminated by the level of service offered by the program developer. Most developers are ready to guarantee the absolute security of their own cloud archive at the level of technologies approved for storing personal data, since they are often contained in program files. This means that documents are encrypted, crypto-operations (coordination, signing with an electronic signature) are carried out with them via secure communication channels. These services also use two-factor authentication when logging in from a mobile device.

CONCLUSION

The acquisition of a functional and efficient EDI program helps to optimize the key processes of the enterprise, reduce costs and time required for processing files, and increase the responsibility of performers. An additional positive factor is the increased level of data security, protection against leakage and copying. When choosing an EDI program, you should pay attention to its functionality and level of security.

List of used literature

1. Sh.R.Gulomov., S.Sh.Muminova. Opportunities and problems of implementation of electronic document management systems. Journal “Technical science and innovation (ISSN: 2181-0400)” of Tashkent State Technical University named after Islam Karimov. No. 3/2021. Tashkent 2021.
2. S.Sh,Muminova., M.A.Asatov. Issues of information security in EDMS. Issues of information security in EDI. International scientific-online conference on "Innovation in the modern education system". Part-3. Collections of scientific works. Washington. USA – 2021. P.204-207.
3. S.Sh.Muminova., Prospects for usin artificial intelligence technologies in document automation systems. Academicia Globe: Inderscience Research. ISSN: 2776-1010. Volume 2, Issue 6. Open Access, peer reviewed journal. Indonesia. Jakarta. June.2021 P-293-302
4. S.Sh.Muminova., Q.Q.Sadritdinov. Analysis of methods for protecting EDMS elements from unauthorized use. Collection of materials of the Republican scientific and technical conference "Innovative ideas in the creation of information and communication technologies and software". Samarkand-2021. p. 385-388.