ISSN 1815-4840
Himičeskaâ tehnologiâ. Kontrol′ i upravlenie
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2019, №1 (85) pp.72-77
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

UDC 681.324: 519.21

T.F.BEKMURATOV, F.B.BOTIROV (TUIT)

MULTI-AGENT SYSTEM OF PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS

Локал тармоқдан маълумотларнинг блоклашини очиш усуллари ва воситалари таҳлил этилган. Локал тармоқдан маълумотларни руҳсатсиз фойдаланишдан ҳимоялашнинг замонавий усуллари ва дастурий воситалари таҳлил этилган. Маълумотлардан руҳсатсиз фойдаланишдан ҳимояни тақдим этган DLP(Data Loss/Leakage Prevention) тизимининг афзалликлари ва камчиликлари келтирилган. DLP тизимининг самарадорлигини ошириш мезонлари ҳамда мультиагентли интеллектуал DLP тизим таклиф этилган.

Калит сўзлар: *агент, интеллектуал тизим, сертификат.*

Проанализированы методы и инструменты разблокировки данных из локальной сети. Проанализированы современные методы и программные средства защиты данных от несанкционированного доступа из локальной сети. Преимущества и недостатки системы DLP (предотвращение потери / утечки данных) демонстрируют защиту данных от несанкционированного доступа. Предложены критерии повышения эффективности системы DLP и системы DLP с многоагентным интеллектом.

Ключевые слова: *агент, интеллектуальная система, сертификат.*

Methods and tools of unlocking data from the local network are analyzed. Modern methods and software for data protection from unauthorized access from the local network are analyzed. The advantages and disadvantages of DLP (data loss / leakage prevention) demonstrate data protection against unauthorized access. Criteria for improving the efficiency of DLP system and DLP system with multi-agent intelligence are proposed.

Keywords: *agent, intellectual system, certificate.*

Introduction

Today, information technology is developing very fast. Receiving, storing, processing, and transmitting almost all data is being processed electronically because electronic information is easier and more convenient to use. However, in order to use confidential information electronically, such information must first be sufficiently secured.

Confidential information is only accessible for registered users. The most reliable way to protect electronic information from unauthorized access or unauthorized exit from system is to use DLP systems to ensure the information security of this system.

DLP (Data Loss / Leakage Prevention) is a software, hardware and software tool used to protect the confidential or sensitive electronic data from unauthorized access or unauthorized use of information.[1]

Framing the issue. Usage of multi-agent intellectual methods to increase the effectiveness and reliability of the DLP system to protect data from unauthorized spread.

The main part

Using the DLP system, it is possible not only to protect data from unauthorized access, but also to filtrate data flow through the network's entire transmission channel and track the flow of data.

The DLP system employs the software agent executing the same kind of tasks and the same type of software agents.

Software agents are the information structure that exists in the software environment. They are executed asynchronously according to the purpose of the predetermined aims, which implies the individual model of the environment created on the basis of the available information and can adapt to the change in the environment by learning [1].

A multi-agent system is created using DLP software agents. The main reason for being a multi-agent system with software agents is that all agents should be able to connect to a single database at the same time, and that is not possible in a hierarchical structure. Because the hierarchical structure is generated by a known type of slash, and the software agents are linked to the datasheet only by the socket node. The request sent to the system center by the software agents will have to be queued at the right time. The system cannot operate in real-time mode. Therefore, when merging software agents into a single system, a multi-agent system is developed and the system is divided into several blocks. Each block is a subsystem of the DLP system because each block is assigned a separate task and a separate subsystem is developed to perform this task. The blocks do not include a set of software agents, only software analysis and query response from software agents have been developed there.[2]

The DLP system is adapted to the organization so that the organization can work with other security devices and interfere with them, and have the ability to control electronic information through this system. To understand how the DLP system works, it is necessary to analyze its structural scheme (Figure 1) [4].

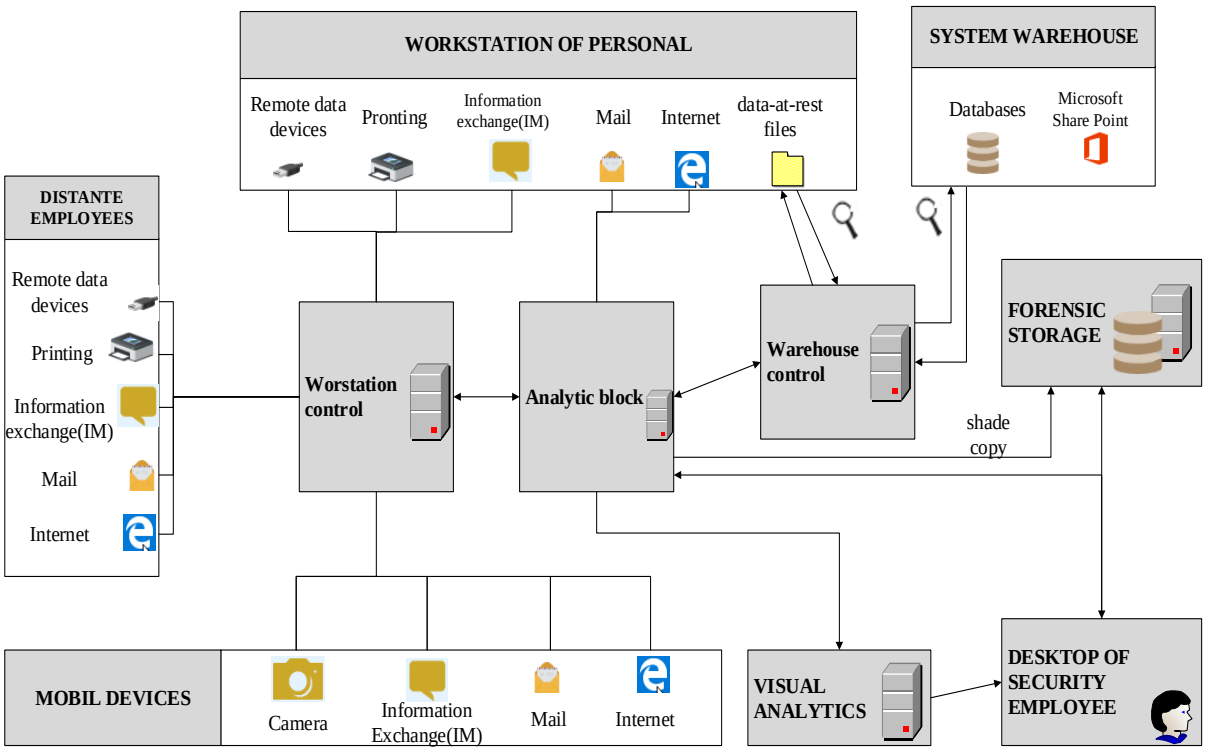

Figure 1. ***Structural scheme of DLP system.***

The DLP system is capable of controlling the electronic document sharing system if the mobile device is connected to the Internet through the workstation's access point in the "Workstations Control" block, "employee workstations", "remote personnel" and even "mobile devices". Therefore, the DLP system combines several hundreds of agents into a single system and controls the workstation through this unified system.

The workstation control unit, in turn, works with the analytical block, the warehouse control unit and the warehouse blocks. At the same time, these blocks form a linear linkage (Figure 2).

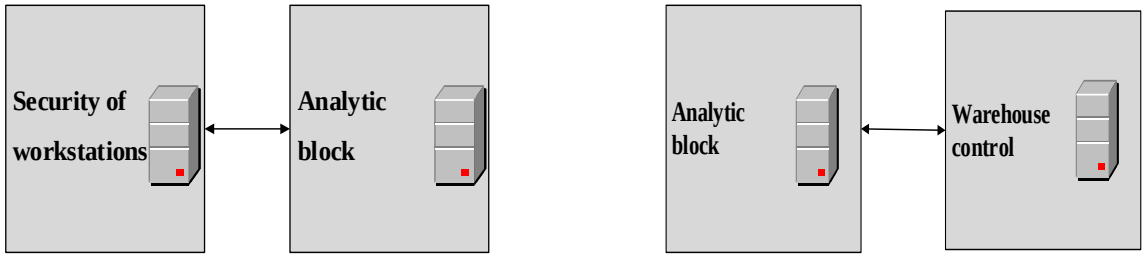

Figure 2. ***The linear linkage of blocks of DLP system***

The reason for this is that they are linearly linked to the confidential data brands (keywords, gifs, ...) and stored in the data warehouse, which is then connected in a warehouse block. Therefore, the software agents located on the computers of the network users prior to the blocking of the electronic data are transferred to the control unit of the workstation and analyze this information block (Figure 3).

In the warehouse block, Microsoft will contact SharePoint to determine if this type of electronic document is allowed to be used on the network, if it's authorized to use it on the network or otherwise restrict access to the network. In this case, the user will only be able to use such data only on his or her personal computer.

Microsoft SharePoint is a browser-based document management platform. So before using this platform the user opens a browser window and goes through the user authentication process. This allows groups to set up a central, password-protected place for document sharing. Documents can be used, saved, downloaded, and edited, and then downloaded in order to continue later. [7]

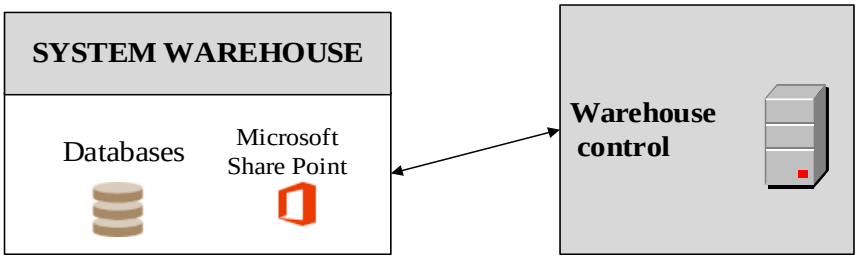

Figure 3. ***Communication between warehouse system and warehouse control***

An inspection block performs a fast search through a warehouse control unit to identify the most common types of confidential information in the system that can be disposed of through unauthorized access. This block increases the speed of the system. If the result of the analysis does not go out of the warehouse, it then addresses to the data warehouse.

The DLP system is multidimensional and multifunctional, and is based on intelligent architecture. But some experts do not agree with it. The reason for that is because the first DLP system was that it was possible to control electronic document management systems only by shutting down the data transmission channel. It is impossible to determine whether this information is confidential, and this type of DLP architecture is not based on intelligent architecture. However, the DLP is being currently developed and is able to make a decision as a result of in-depth analysis (i.e., whether the information is confidential, closed or opened). In order to make it possible for the system to make decisions, its architecture must be developed in the form of an architectural system of the intellectual system. Therefore, DLP systems, which are currently being developed, incorporate the intelligent system architecture.

At the same time, when the number of users in the network exceeds a few thousand, the DLP system's data warehouse and query will increase. As a result, the response time for the programming agent that sent the request is prolonged. This, in turn, leads to a slowdown in the system.[3]

To address this type of problem, the development of the DLP system, which combines the functional components of multidimensional intelligence systems, is essential. The multi-agent system is the family of intellectual systems.

One of the most important stages of introducing the DLP system is the ability to respond adequately to customer needs. Therefore, the wise choice of the DLP system used to provide information security of an enterprise based on artificial neural networks is of great importance. Usually, the organization works hard to prevent the spread of its confidential information, but continuously changing information infrastructure makes it difficult to achieve this goal. The spread of mobile devices, data communication and cloud computing always allows the use of the Internet and e-mail, allowing the data flow easily across the corporate network, making it harder to secure information. The number of such cases is rising year after year, according to Info Watch and Kaspersky Lab's Division of Protection against Unauthorized E-Information.

Info Watch has been operating in the field of information security for more than 14 years and has become a group of companies that protect companies against various threats of information security. Info Watch is a group of companies that develop software products to deal with external and internal security threats as well as providing information security to organizations [8].

When installing hardware and software used to secure information security, clients require software that is easily accessible to the existing infrastructure without altering the architecture of the network or interrupting business processes. The convenience of using and installing the DLP system is that it can be controlled from a single console [5-6].

The solutions used to prevent the spread of information should be adequate and correspond to the net asset value of the protected asset. Users typically set the following requirements for the DLP system:

- Support various operating modes;
- introduction of different information technologies;
- Complete management channels;
- Ease of management, ease of installation and adjustment;
- capabilities of record logging and reporting;
- availability of a certificate;
- low price.

To fulfill these requirements, the independent DLP system must, of course, incorporate the functional components of the multi-intellection system as described above.

Depending on the degree of fulfillment of these six consecutive requirements, the requirements , the price of the DLP system i.e. the seventh requirement appears. That is why DLP developers are generally trying to keep the aforesaid six requirements at a high level.

DLP systems with functional components of multitasking intellectual systems have the advantage of the six main DLP systems. These six criteria allow the fulfillment of these six requirements and the effectiveness of the DLP system.

Criterion 1. Mode of operation. DLP systems have two main modes: active and passive.

Enabling 'blocking' behavior will block the violation of security policies, such as forwarding confidential information to an external mailbox.

Passive mode is often used to verify and configure situations where incorrect positions are too high during system setup. In this case, a rule violation is detected, but restrictions on the movement of information are not imposed.

Criterion 2. Familiar information technology. Identification technologies allow classifying confidential data transmitted over an electronic channel. Today there are several basic technologies and their types. They are essentially similar but differ in implementation. Every technology has its advantages and disadvantages. Additionally, different class agents are needed to analyze information in different classes. Therefore, DLP manufacturers are trying to add maximum technology to their products. This, in turn, leads to an increase in the number of DLP agents.

Criteria 3. Fullness of supervised channels. An optional channel is a way to spread information. Even one open channel can undermine all information security risk management services. It is therefore important to keep control of channels that are not used by employees for the purpose of blocking channels and preventing others from spreading. Although the best modern DLP systems can handle many network channels, it is recommended to block unwanted channels. This type of protection applies to local channels. However, blocking separate channels in this case is difficult because ports are often used to connect external devices, tools, and so on.

Criteria 4. Ease of Control. Performance and management features may be less than technical capabilities of the software. Indeed, it is difficult to apply complex software protection. Therefore, programming tool management should be understandable and user-friendly. Regular checks and errors in configuration without proper use can lead to a sharp reduction in the quality of confidential information over time.

Criterion 5. Capability of record logging and report. DLP archive is a database that is maintained by system sensors stored and operated on the data (files, emails, http queries, etc.). The information collected from the database can serve as a basis for different purposes, including the analysis of user behavior, the basis for verifying information security breaches to keep copies of important information.

Criteria 6. Availability of certificate. Certification does not have serious advantages in the competition. At the same time, it is mandatory for a number of customers, primarily, to have a certificate for public institutions. However, the reliability of the certificate used in this DLP system is high because the certificate for the application is not prepared separately, but is developed in conjunction with the program.

Each of these criteria improves the system's performance by solving a specific problem of protecting data against unauthorized dropping. But nowadays, the main problems of protecting data from unauthorized dropping are:

- If the user agents on the PC check their databases for analysis prior to switching to the data transfer channel, they will consider this information as unusual and will not block it if there is no information on its data in its database. Therefore, it is necessary to keep permanently entering into the database of any confidential or confidential information. In order to avoid this shortage, it is crucial to add a database to the system database. Through the Knowledge Base, in any case, it can find information that is close to it through its knowledge for explicit or informal information. If the database does not find the information that the agent sends, it then contacts the knowledge base and will be informed of this type of information (confidential or secret).

Conclusion

In sum, the creation of DLP systems with multi-intellectual systems increases the reliability of the system. Six criteria were proposed to improve the efficiency of the system. Use of the information against unauthorized deliveries through the proposed criteria allows to:

- Supports various operating modes;
- introduce different information technologies;
- Ensure the availability of controlled channels;
- Ease management, installation and adjustment;

- enable record logging and reporting;

The functional components of the intelligent system used to enhance the effectiveness of the multidimensional intellectual DLP system provide the following possibilities:

- Manipulation of objects,
- unifying the organizational units, which are distinguished in many agencies;
- Sorting tasks;
- Creating an environment in which agents and things are available;
- Promoting the diversity of relationships between agents;

Through the multidimensional intellectual DLP system, all users in the organization's network can control data traffic and detect and analyze data unauthorized, in other words, to prevent unauthorized transmission of logical protocols, ports, and devices.

References:

1. Bekmuratov T.F., Botirov F.B., Multiagentli tizimlarni axborot xavfsizligi tizimlarida qo‘llanilishi // Problemi informatiki i energetiki. 2018. № 5. S. 78-83.
2. Bekmuratov T.F., Kontseptsiya i zadachi postroeniya intellektualnix sistem informatsionnoy bezopasnosti // Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari: Respublika miqyosidagi ilmiy-texnik konferentsiya. Toshkent - 2018., S. 4-8.
3. Bekmuratov T.F., Botirov F.B., Kiberhimoya boshqaruvining intellektual mexanizmlari // Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari: Respublika miqyosidagi ilmiy-texnik konferentsiya. Toshkent - 2018., S. 108-112.
4. Andriyanova T. A., Salomatin S. B, DLP: Snijenie riska utechki konfidentsialnoy informatsii banka., Cistemnыy analiz i prikladnaya informatika 2017-3 ,C. 76-82.
5. InfoWatch: ot DLP k zasch’ite ot vnutrennix ugroz. http://www.crn.ru/news/detail.php?ID=79072.
6. Eksperti rinka o vnedrenii DLP-sistem. – http://itsec.ru/articles2/focus/eksperti-rinka-o-vnedrenii-dlpsistem/.
7. DanilovA.D, BorovtsovA.N., Pprotsessniy podxod MOF i MICROSOFT SHAREPOINT kak put k povisheniyu kachestva it-uslug. https://cyberleninka.ru/article/n/protsessnyy-podhod-mof-i-microsoft-sharepoint-kak-put-k-povysheniyu-kachestva-it-uslug.
8. Elektron resurs. https://infowatch.com/company.

Bekmurodov Tulqin Fayziyevich – academic, professor, professor of technics, Scientific innovation centre on information technologies under TUIT named after Mukhammad al-Khorazmy ,
Phone:(+998) 71 234-07-92 (m.), E-mail: bek.tulkun@yandex.com;
Botirov F.B. – post graduate of TUIT named after Mukhammad al-Khorazmy,
Phone: (+998) 97 751-16-97(m.), E-mail: botirov_fz@mail.ru.