ISSN NO : 2770-0003
Date of Publication : 15-12-2021

# DLP system overview

**Yulchiyev Ibrokhimjon Usmonali o'g'li**

**Abstract:** The DLP system is currently very relevant and is an important tool for the safe implementation of business processes and strategies. Data Leak Prevention systems contain a large number of modules. The modules of almost all systems of this type are the same, except that some modules and their operating principles or the tools they use may differ. In this article, we will take a closer look at this system. That is, we will consider what modules should be in the system and what functions they perform.

**Key words**: DLP system, business

The DLP system is currently very relevant and is an important tool for the safe implementation of business processes and strategies. Data Leak Prevention systems contain a large number of modules. The modules of almost all systems of this type are the same, except that some modules and their operating principles or the tools they use may differ. In this article, we will take a closer look at this system. That is, we will consider what modules should be in the system and what functions they perform.

The DLP system consists of three parts. These are the agent, the server, and the workstations of company employees.

Agent - The agent is installed on users' computers and sends every action of the user to the server. Of course, this is done based on the policy of the system. Organizations that use the system may disable modules they do not need, or re-filter or reconfigure modules as they see fit.

Server - All data received by the agent is stored on the server. Here, the information sent by the agent is processed and conveniently stored in the database. Before this information is sent to the UI (user interface), it is taken from the database, rendered and sent to a user-friendly view in the UI.

Workstations of company employees – it could be the computers or tablets of the organization's employees. These devices are equipped with an agent that acts as a spy. These "spies" monitor the actions of employees and send information to the server.

DLP system includes following modules:

Dashboard is the main panel. The basic data and statistics are presented mainly in the form of graphs. This module allows you to view data conveniently. The data collected and analyzed by employees over a period of time is provided to the security staff of the organization in a convenient way. It is also possible to view statistics about the server.

Employees is one of the most important modules, as current firewalls have a high level of security. Therefore, the biggest factor in the leakage of information is the employees of the organization. This module provides a list of employees and information about them. These can include employee names, computer names, mac addresses, employee statuses, departments, positions, and so on. You can also view separate weekly, monthly, or annual statistics for each employee.Computers are the basic tools needed to make a system work, because it is installed the agent and employees' computers which is the main part of the system. This module is further subdivided into various sub-modules:

active applications - This module displays information about applications used by the employee.

keylogger - this module displays the information entered by employees using the keyboard.

screenshots - This module stores screenshots of the employee's computer or tablet at regular intervals.

internet usage - this module displays information about the sites visited by the employee, the information searched in the browser, the information sent by mail.

clipboard - this module stores information about the copied data.

social networks - this module displays the employee's correspondence on social networks, sent and received files.

USB is a module that stores files copied to an employee's flash drive and information about that flash drive.

ISSN NO : 2770-0003
Date of Publication : 15-12-2021

printed documents - this module displays information printed using a printer.

Policy - Each organization sets its own system policy based on its own requirements, and there are settings that allow you to manage that policy. It is also possible to group employees, processes, usb, websites in this module.

Incidents - This module describes the actions of employees of the organization against the laws set out in the policy module.

File analyzer- this module stores files stored on employees' computers and analyzes them in the prescribed manner.

Reporting is one of the main modules, the system automatically prepares reports based on events recorded by employees. The report can be in the form of plain text, tables or diagrams.

Settings - this module stores various types of system settings, for example: database management - copying from it, changing the system database. Agent updates, notifications, network settings.

Keywords - Keywords are defined by each organization based on its security policy.

Global Search - This module serves to search the entire system, not just one part of the system.

Logs - this module can store the time of entry of employees into the system and the different actions of the employee and the system, depending on the system itself

## References

1. Bhaimia, S. (2018), The General Data Protection Regulation: The Next Generation of EU Data Protection, Legal Information Management, vol. 18, no. 2018, pp. 21-28.
2. Peneti, S. & Rani, B. P. (2016), Data Leakage Prevention System with Time Stamp, 2016 International Conference on Information Communication and Embedded Systems (ICICES), 25-26 Feb. 2016, Chennai, India, pp. 1-4.
3. Ram, K. (2015), Analysis of Data Leakage Prevention on cloud computing, International Journal of Scientific & Engineering Research, vol. 6, issue 1, pp. 457-461.