International Journal of Research
ISSN: 2348-6848 Vol-5, Special Issue-18
2nd EduIndex® International Conference on Science Changes the World held on 28-29th June 2018 at **Edupedia Publications Pvt Ltd**, New Delhi in Association with www.tadqiqot.uz of the Republic of Uzbekistan

Turobova Gulnoza
Sultanova Rushana
Jurayeva Raykhon
(Tashkent, Uzbekistan)

CREATING METHODOLOGY OF CHOOSING DLP SYSTEM

Abstract

In this story is on theme "Creating methodology of choosing DLP system". The systems of DLP methodology was introduced in the final work and according to these, evolution method was created by Uzbekistan technology of security and preserving of society was produced.

Keywords: DLP systems, the arts, Falcon gaze, Search inform, Info watch, methodology

Over the last few years, companies in every industry sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. A wide range of high-profile data loss incidents have cost organizations millions of dollars in direct and indirect costs and have resulted in tremendous damage to brands and reputations. Many different types of incidents have occurred, including the sale of customer account details to external parties and the loss of many laptops, USB sticks, backup tapes and mobile devices, to name just a few. The vast majority of these incidents resulted from the actions of internal users and trusted third parties, and most have been unintentional[1,p.10-15].

This section discusses the existing DLP systems and their advantages and disadvantages. It also provides information on DLP transformation technology. The term "data loss prevention" describes technology that automates the identification and protection of sensitive data. A DLP system has components that implement three functions: Management, Identification and Protection. The Management component is where an administrator creates and manages policies that the DLP system implements and generates any reports that are needed. The Identification component finds the sensitive data that the system's policies define. The Protection component safeguards the sensitive data that the Identification component finds[2, p.5-9].

This story examines the status of DLP systems in Uzbekistan. Based on the information obtained from the Information Security Center, all parameters of DLP systems were analyzed. During the analysis, the following DLP systems were used in Uzbekistan. For instance, InfoWatch, SearchInform, and Falcongaze DLP systems use in Uzbekistan's information security systems. This story provides an overview of these systems and provides them with the analysis of the variables given.

The table below shows the basic DLP systems in Uzbekistan based on different and different parameters. The first column shows the DLP system settings (1.1.Table). Mainly DLP systems in Uzbekistan Falcongaze, Infowatch, SearchInform. Elements are important, and the arguments d.erived from them are multiplied by one. The value of the parameters is set to 1 to 10.

*Table 1..1.*Table based on estimation values

DLP system building module	Falcongaze Consists of two modules: Falcongaze SecureTower (5)	InfoWatch It consists of 4 modules: IW Traffic Monitor - module for monitoring network transmission channels; (10)	**SearchInform Modular, server and client (3)**
Methods of counteracting information leakage	Identification and blocking (9)	Identification and blocking(9)	Identification (7)
Controlled protocols (SMTP, POP3, IMAP, MAPI, NNTP, S / MIME, ESMTP)	Yes, via agent (9)	Yes, SMTP(1), POP3(1), IMAP(1), MAPI(1), NNTP(1), S / MIME(1), ESMTP(1) (7)	Supervises: SMTP(1), SMTPs(1) , POP3(1), POP3s(1), IMAP4(1), MAPI(1), NNTP(1), Webmail(0.5), S-MIME(0.5), ESMTP(0.5) (8.5)
Controlled protocols (FTP, P2P, FTPS, FTP over HTTP)	Yes (9)	Yes, only FTP (2)	Controls: SMTP(0.4), SMTPs(0.4), POP3(0.4), POP3s(0.4), IMAP4(0.4), MAPI(0.4), NNTP(0.4), Webmail(0.4), S-MIME(0.4), ESMTP(0.4) (4)
Protocols of individual applications: iTunes(1), Dropbox(1), Yandex.Disk(1), uTorrent(1), GoogleDrive(1), Mail.RU(1), Skype(1),	Yes(10)	Yes(10)	Only Microsoft SharePoint(5)

ICQ(1), UltraISO(1), Nero(1)			
Blocking of miners in corporate networks	Yes(10)	No(0)	No(0)
Controlling the removal or transfer of confidential data to quarantine	Yes(3)	No(0)	No(0)
Scanning methods: through agents, without agent, etc.	through agents (8)	through agents (8)	through agents, remote (10)
Search by digital labels	Yes(3)	Yes(3)	No(0)
Digital document prints (binary)	No(0)	Yes(3)	Yes(3)
Digital prints of documents (text)	Yes(3)	Yes(3)	*No(0)*
Analysis of documents	All formats of Microsoft Office documents(1), Apache OpenOffice(1), Adobe Acrobat(1), RTF(1), HTML(1), XML(1), mail message formats(1). (7)	All formats of Microsoft Office documents(1), Apache OpenOffice (1) Adobe Acrobat(1), RTF(1), CHM(1) (5)	All document formats (9)
Searching over hash functions	Yes(5)	No(0)	No(5)
Find similar	Yes(5)	No(0)	Yes(5)
Control the movement of scanned documents (without OCR, pattern recognition)	Yes(5)	Yes, passports, credit cards. The ability to teach the system to recognize other documents, regardless of the filling. (10)	Yes(5)

Handling Encrypted Files	Yes, Word, Excel and PDF, archives, letters with PGP encryption. Yes, the document is marked as encrypted. It is possible to configure the notification.(3)	No(0)	Yes(5)
Voice Recognition	Yes(0)	No(0)	Yes(4)
Video Recognition	No(0)	No(0)	Yes(4)
Screen (desktop images)	Yes, with a specified time interval or when changing the window of the active process. (5)	No(0)	Yes(3)
Monitoring of installed / remote applications	Yes, only installed applications. (3)	No(0)	Yes(5)
Monitoring of installed / remote services	Yes, only installed services (5)	No(0)	No(0)
Monitoring of visited sites (including encrypted protocols)	Yes(5)	No(0)	Yes(5)
Logging the time spent on a particular tab of the browser	Yes(3)	No(0)	Yes(3)
Black and white list of sites	Yes(5)	No(0)	Yes(5)
Blocking websites	No(0)	No(0)	Yes(5)
Monitoring of correspondence in ICQ (protocol OSCAR)(1), Skype(2), WhatsApp(1),	Yes(9)	Yes, only ICQ (text, file)(1), Skype (text, file, voice)(2), Mail	Yes(9)

Google Hangouts(1), Telegram(1), SIP(1), Viber(1), Microsoft Lync(1).		Agent (text messages)(1) (4)	
Employee cards (IP addresses, email, IM, Skype, etc.)	Yes(4)	Yes(4)	Yes, by the administrator(5)
Notification of system users by the security administrator	Yes(3)	No(0)	No(0)
Masking the agent in the system	Yes(5)	No(0)	Yes(5)
Summa	C = 179/36 = 5	C = 85/38 = 2.36	C = 134.4/38 = 3.733

This table calculates the value of each column. It will be in the number of rows. Based on the values generated, the program is created. The program uses the selection operator.

Today, the protection of information security is a major problem. Main safety of enterprise and organization information is maximized, therefor, in this work methodology of choosing DLP system using InfoSec data is created. At first, security threats are considered. So, Threat-based protection systems are analyzed. Among them, the DLP system is selected as an effective protection mechanism.

All DLP systems in world are analyzed. Basically, information about the best DLP systems in recent years is accumulated. Their advantages and disadvantages are examined. Moreover, the DLP system parameters are analyzed based on the findings of DLP systems used by Information and public security in Uzbekistan. The value of each parameter depends on the security level. The assessment process was

calculated with the ratio of overall high indicators to all the functions. Using the results of general calculations, a program was created for use on the territory of Uzbekistan.

References

1. Nelson P. DLP Technology for Spectroscopy //DLPA048 Texas Instruments. – 2014.

2. Caldwell T. Data loss prevention–not yet a cure //Computer Fraud & Security. – 2011. – Т. 2011. – №. 9. – С. 5-9.

Information about the author of the article

Turobova Gulnoza Orifovna is a 4 course student of the Faculty of Information Security. Tashkent University of Information Technologies (Tashkent, Uzbekistan); +998998078214; TurobovaGulnoza@mail.ru

Sultanova Rushana Rakhimovna is a 3 course student of the Faculty of Information Security. Tashkent University of Information Technologies (Tashkent, Uzbekistan); +998909791128;

Jurayeva Raykhon Sobirovna is a 1 course student of the faculty of telecommunications technology. Tashkent University of Information Technologies (Tashkent, Uzbekistan); +998998348082; scientific adviser - senior lecturer, director of the Center for New Information Technologies Sharipov Z.Z .; certificate: N E F G H; about the conference learned from the scientific adviser