

Lykova O.I.

Donetsk National University of Economics and  
Trade named after Mykhayilo Tugan-  
Baranovsky, Donetsk, Ukraine,  
e-mail: admin@study.dn.ua

## ANALYSIS OF OUTSOURCING OF ENTERPRISE INFORMATION SECURITY

**Objective.** *The aim of the article is the outsourcing analysis of information technologies related to a commercial enterprise information security.*

**Methods.** *In the course of study the following is used: methods of theoretical generalizing and comparison as well as analysis and synthesis (for the content elaboration in the notion of information security outsourcing).*

**Results.** *Based on the study conducted the notion is established on the outsourcing of information security of a commercial enterprise, head components are formulated in functioning of information protection systems, in particular, DLP (Data Loss Prevention) system. Besides, the basic advantages and problems of outsourcing are determined, and selection criteria are established on an outsourcer company that would be responsible for complex measures taking in order to provide information security.*

**Academic novelty.** *The conceptual system of the outsourcing of a commercial enterprise information security is specified, the scientific methodical approach to selection criteria on an outsourcer company related to protection of commercial information is improved together with prevention of problems arising due to unauthorized data leakage in order to contribute in strengthening of information security of a commercial enterprise.*

**Practical importance.** *The findings obtained shall be utilized for optimization of commercial information protection system as well as improvement of a commercial enterprise's information security. The infrastructure of distribution networks information systems has its specific features like large scale and great territorial separation that may lead to the loss of important data. Thus, for information security provision the necessity is substantiated in attracting outside experts of an outsourcing company.*

**Key words:** *information security, outsourcing, systems of information protection, DLP systems.*

In the environment of development of modern information society together with competition strengthening and dramatic reduction of companies' expenditures the growth of effectiveness of contributions in the means of information security provision becomes one of the tasks of paramount importance. A number of commercial enterprises are far from being ready to complement their staffs with the service of experts in information security able to solve the branch problems and

issues on high professional level. One of the most prospective versions in the situation is transfer of such function to an outside institution specialized in the given services rendering. In other words, the outsourcing of an enterprise information security is spoken about.

It often occurs in the modern business that information is even of higher value than material assets as risks of confidential data getting into strange hands are too high. Realization of such risks can result in reduction of the business value or its complete loss. The main weapons of competitive activity become utilization of information. In Ukraine there exist regulations in general legal fundamentals of obtainment, use, distribution, and storage of information as well as system of information and its sources. The status of a party of informational relations is established together with access to information, and its protection [1, 2].

In accordance with findings by Zecurion Analytics Analytic Center the calculated loss due to public incidents of information security in 2011 was in excess of USD 20 billion i.e. USD 25.13 M per an incident. Then personal data of more than 350 million persons were compromised. The highest number of incidents (45.2%) happens due to personnel's mistakes or negligence and low awareness of companies workers of information security issues. The greatest amount of information leaks from medical institutions (20.4%), governmental bodies (16.7%), schools (15.2%), and retail companies (13.8%). The mostly encountered way of information loss is through notebooks and mobile information tanks (together 19.4%), web-services (18.2%), computers (16.1%), and non-electron carriers (13.8%).

In the modern national and foreign economic literature a great number of works deals with the issue of outsourcing among which the researches of such authors as Mikhailov D., Gottschalk P., Anikin B., Sparrow E [3-6]. Information security of enterprises was considered by such scientists as Godin V., Korneyev I., Kurilo A., and Shiversky [7-9]. However, the problems related to outsourcing processes as for an enterprise information security require further deeper study and analysis.

The outsourcing of information technologies means full or partial transfer to a strange institution of functions related to information technologies of an enterprise, and namely: management of information systems, net infrastructure servicing, placement of corporative databases in servers of specialized companies, etc. [5,6]

The outsourcing of information security of an enterprise is the contract-based transfer of some business processes or functions connected with the security of information resources for servicing by a strange company specialized in the given industry. So, the strange company adapts own inner resources and knowledge depending on business needs to use them for the benefit of a given client. As opposed to rendering service and support in non-recurrent manner the outsourcing is based on long-term contracts [4].

The aim of the article is the analysis of outsourcing of information technologies in the connection with information security of a commercial enterprise.

As far as information security is concerned the term itself has several definitions. They mainly relate to technical specifics of activity and coverage of general number of directions where the protection is executed. But all definitions

characterize security as the activity that is immediately directed to termination of information leakage out of the borders of information systems of a commercial enterprise or prevention of unauthorized data transformation.

In accordance with the Law of Ukraine “Information” any information which possession can give its real or potential owner the opportunity to get moral, material or political advantage is subject to protection [1].

According to [7] information security means immunity of information contained in any carriers against incidental and intentional impacts of natural or artificial character designed for destruction and modification of these or those data as well as change of accessibility degree of important information.

Other experts [8] define in the following way: information security is one of kinds of security expressed through the state of immunity, especially confidence and trust in security. Such confidence is oriented to society including an individual or a group of individuals waiting for or being eager of some aims achievement and making some steps in this connection. There is a special comment related to the security of nets and information systems emphasizing as follows: “The whole business is the issue of trust. The trust can only develop in the case when parties of an agreement feel reliable and secure”.

To provide information security of commercial enterprises they utilize special systems for information security. Each separate system for information security includes the integral complex of organizational, technical, technological, software, and other means, methods and measures for reduction of information vulnerability and prevention of unauthorized or illegal access to information, its leakage or loss [9].

A lot of experts believe that the leak of information of commercial value may be considered to be one of key problems in this direction. The DLP (abbreviation from the English language “Data Loss Prevention”) system is used for struggle against information leakages.

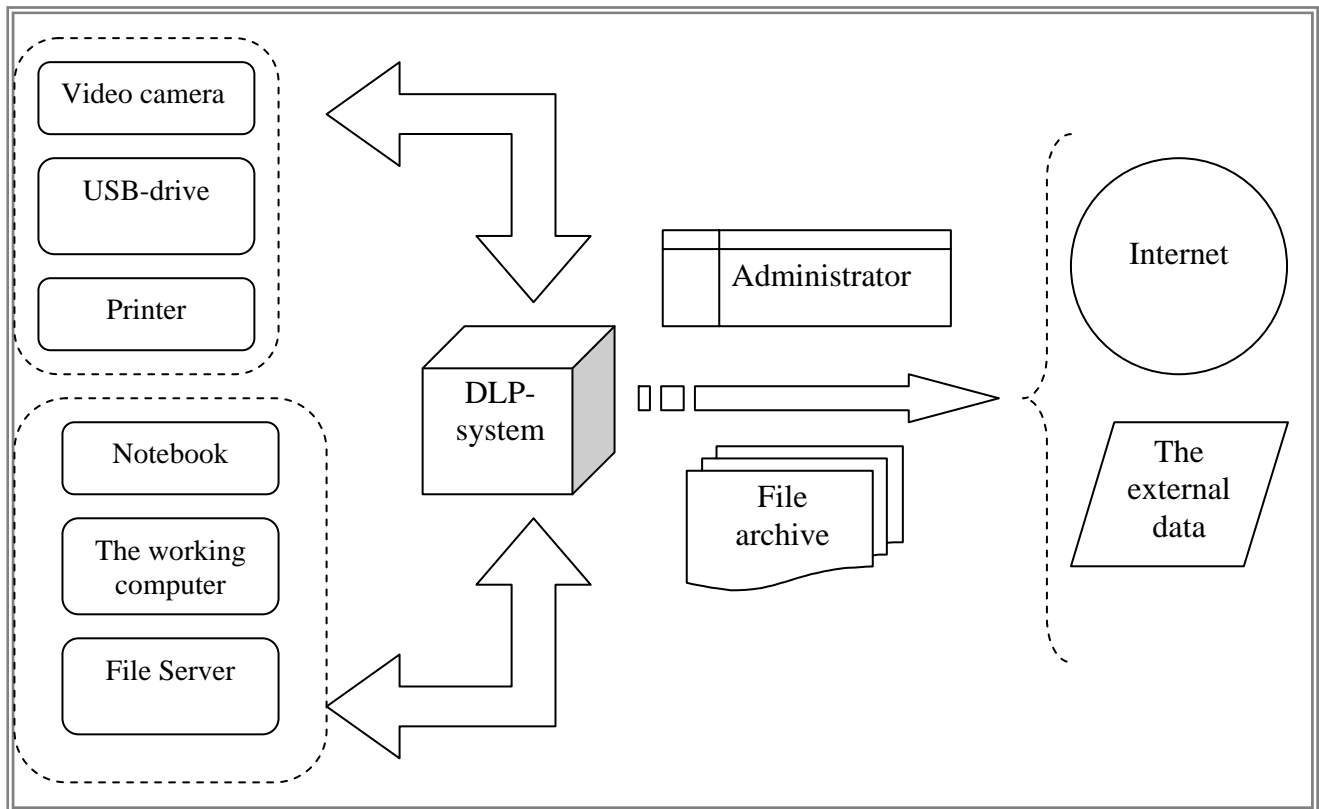
As opposed to computer anti-virus programs the task of the DLP system is to protect corporative information against any attempts of its transfer to competitors’ hands. Rivals can organize both theft and further transfer or sale of commercially important data using the personnel of an enterprise for the purpose. Another reason of the leakage can become a human factor including banal carelessness, ignoring of common security norms as well as their non-recognition.

In the majority of cases experts distinguish the following decisions related to the DLP system (Figure 1).

1. Maximal full control over all known channels of information leakage including control of internet channels – sites together with social nets, chats, electron mail as well as other information carriers and tanks not immediately connected with nets like disks, flash tanks, etc.

The same group can also include mobile phones based upon the cellular principle of radio communication. However in case of telephones some special methods are utilized, for example systems for radio signals suppression, and it is beyond the range of DLP systems.

Another group may include such local devices as printers, scanners, etc.



**Figure 1 – The DLP system functioning scheme**

2. Organization of monitoring and analysis of information. Here we speak of control organization on traffic (internet) and transfer of information itself (movement of documents in office, work with files, making copies of information, etc.).

Recognition of potential threat of leakages is followed by their maximal quick blocking and detection of persons who are involved in illegal actions of such sort. When an extraordinary situation arises the system automatically makes steps within the frames of set regulations, and specifies the working place from which the attempt of violation is done.

3. Information storage. The DLP system loads all necessary data into a special database until all the causes are clarified on the situation of potential treat qualified by the system.

Certainly, for maintenance of all decisions' life support in enterprise information security highly professional special experts are required. Besides, these experts are to be provided by specialized program complexes and information systems that would be actual just in the given ad-hoc segment. Thus, for administration of an enterprise the most acceptable decision is attraction of outside specialists from an outsourcing company.

As a rule, an outsourcer company possesses much greater experience in the sphere of equipment assembling and operating response on arising incidents. Besides, and which is highly important, being a strange institution an outsourcer can be more objective and not inclined to suppression of problems due to personality partialities. As far as finances are concerned the availability of prepared decisions in information

technologies allows to economize on expensive development of the own software followed by its testing, adjustment, tuning and maintenance.

The problem of criteria establishment for outsourcer company selection that is to be responsible for the whole complex of measures in organization of information security is of paramount importance [10].

Here one shall pay attention at the following items:

- Algorithms of actions in introduction and further maintenance of information security of the commercial enterprise accurately fixed and recorded in due manner
- The own material and technical resources and availability of necessary equipment
- Sufficient possession of own resources and opportunities like possibility of permanent being on duty for technical personnel
- Availability of own program developments in the core sphere
- Employment of qualified (certified) specialists for technologic and technical sphere in the company
- Presence of regular high level clients as well as positive references from these clients
- Agreement on the level of services rendering SLA – Service Level Agreement
- The costs of introduction and maintenance
- Potential risks associated with strange people's access to secrets of the company

The reduction of costs for the corresponding infrastructure can be understood as a serious advantage to be taken into account with initiation of the process for information security transition to outsourcing. Optimization of the enterprise financial flows allows some funds accumulation for development of basic business directions. It assists in more accurate and transparent financing and extra expenditures reduction. Besides, the load of home specialists of information and security departments gets lower.

However it may be difficult to make a positive decision. The need of giving access to confidential information is followed by difficulty of making decision on the outsourcing itself, and then the issue of clearance limits continues to be important. Here appears the problem of outsourcers' actions control. The next threat may become a spontaneous involvement of the enterprise in the eternal confrontation between information security specialists and their antipodes i.e. computer hackers.

As for practical implementation of information security systems the worldwide experience shows that it makes sense for large commercial enterprises. One should emphasize that the infrastructure of information systems of trade nets has its special peculiarities like large scale and great territorial division. The information technologies infrastructure of retailers includes serious computing facilities, office information systems as well as great nets for data transfer with various apparatus devices for logistics, shop equipment, and shop floor provision. Thus, in this case to provide information security the professionally adjusted system is required for protection of commercial information, and improved information security. This, in its turn, requires attraction of strange outsourcer experts.

## Conclusions

1. The notion of outsourcing of information security of a commercial enterprise is established as the contract-based transfer of corresponding business processes or functions connected with the security of information resources for service by a strange company specialized in the corresponding sphere.

2. Main components are specified on information security systems functioning, in particular, DLP systems

3. Main criteria of selection of the outsourcer company that is to be responsible for the whole complex of organization measures in information security are fixed.

## References:

1. Law of Ukraine, "About information", available at: <http://zakon1.rada.gov.ua/laws/show/2657-12>.

2. Law of Ukraine (1997), "About defence of information in the automated systems", *Zakon Ukraine*, Vol. 7.

3. Mihailov, D.M. (2009), *Autosorsing. Novaya sistema organizatsii biznesa* [Autorsoring. New system of organization of business], KNORUS, Moscow, Russia.

4. Gottshalk, P. and Solli-Seter, H. (2007), *IT-autosorsing: postroenie vzaimovыgodnogo sotrudnichestva* [IT-AUTSORSING: construction of mutually beneficial collaboration], Translated by Petrov, A. and Satunin, A., Alpina Biznes Buks, Moscow, Russia.

5. Anikin, B.A. and Rudaya, I.L. (2006), *Autosoring i autstaffing: vysokie tehnologii menedjmenta* [Autorsoring and autstaffing: high technologies of management], Infra-M, Moscow, Russia.

6. Sparroy, E. (2004), *Uspeshnyi IT-autsorsing* [Successful IT-autsorsing], Translated by Alabina, Yu., KUDIC-OBRAZ, Moscow, Russia.

7. Godin, V. and Korneiev, I. (2000), *Upravlenie informacionnymi resursami* [Management informative resources], INFRA-M, Moscow, Russia.

8. Kurilo, A.P. (2006), *Audit informacionnoi bezopasnosti* [Audit of informative safety], BDC-press, Moscow, Russia.

9. Shiverskii, A.A. (1996), *Zashita informacii: problemy teorii i praktiki* [Defence of information: problems of theory and practice], Yurist, Moscow, Russia.

10. Lavruhin, A. (2012), "Autorsoring of informative safety – «pro and con»", *CONNECT*, No. 11, pp. 62-63.