Bikas S. Aghayev, Shakir A. Mehdiyev, Tarlan S. Aliyev DOI: 10.25045/jpis.v07.i1.05
Institute of Information Technology of ANAS, Baku, Azerbaijan
depart6@iit.ab.az, depart11@iit.ab.az

ELECTRONIC INFORMATION CARRIER AS AN OBJECT OF INFORMATION SECURITY

The article addresses the problem of information security and protection methods of some information carriers. The methods and devices for protection, recycling, recovery, backup information stored in electronic media and paper waste, which store confidential communications and state secrets are analyzed. Establishment of management system of information carriers is highlighted.

Keywords: *electronic waste, electronic waste recycling, electronic information carriers, information security, information protection, magnetic/optical carriers, strimmers.*

Introduction

People working in any field generate wastes along with material goods and services. These wastes create health threat for human and pollute environment. At the same time, they are important for heat power resources and raw material resources for industry. Harmless or very harmful (dangerous) wastes are distinguished due to the threat and damage it poses on human health and environment.

Electronic waste is a (dangerous) waste type and three groups of e-wastes are distinguished by the hazards it poses. According to the classification of the International Union for Standardization, e-waste embraces electronic devices, installations and equipment, including computer equipment, along with the electrical (power) devices, and they are marked briefly as *WEEE (Waste Electrical and Electronic Equipment)*.

EU 2012/19/EU Directive on electronic waste includes electronic waste comprising 600 electrical and electronic equipment items in 10 groups [1]. Telecommunications and networking equipment is the third classification group.

Nonetheless, historically, information has been one of the most important factors providing high-quality performance of man and society. On one hand, significance of information as a mean of enhancing the quality of life of people increases, on the other hand, the quantity and quality indicators of possible danger and damage are also increasing in the modern information society. This damage can be, more or less, dependent on the degree of privacy and secrecy and due to data loss and seizure for malicious purposes. The development of information security and its security methods are accompanied by advanced techniques and technology used for the expansion and theft (seizure) of leakage channels. Studies have shown that, over time, importance of information security issues is increasing. Therefore, any serious organization should handle data security and protection issues as multi-factor and multi-purpose problems and pay particular attention to the implementation of a) institutional and legal; b) software and hardware; and c) technical aspects of effective security system.

The paper mainly focuses on information security software and hardware issues of information carriers of electronic waste.

Electronic information carriers

Formation of information society in recent years is characterized with computerization and networking processes. This primarily indicates the rapid increase in the number of computer and network equipment. Only in a small country as Azerbaijan, according to the statistics of the year 2014, about 1 million computers and more than 10 million mobile phones had been used []. Ensuring information security of technical devices of each user is very important. Vast majority of technical devices and equipment nowadays has electronic memory, elements and nodes -

electronic information carriers. Therefore, from a technical point of view, information security, first of all, is the security of its carriers.

Information security of data carriers is provided by the optional protection methods and rules depending on the type of carriers, and their physical, mechanical, chemical and ergonomic features. The major amount of information is stored in the following material carriers:

- hard and soft magnetic drives (disks, floppy disks);
- magneto-optical drives (discs);
- streamers;
- *ZIP*-memory drives;
- Flash-based flash-disks - flash-drives, flash-card;
- Paper;

The content of texts, audio and video materials, photos, projects, calculations and so on the content of stored in these material drives may comprise confidential information (personal, business, commercial, trial and investigation, professional, production etc.) or state secret (especially important, very confidential and secret). These drives can be displaced, thrown out, stored, transported, transferred to other locations, in which the data is written (home, work places, public places etc.). Obviously, uncontrolled movements of these drives, unauthorized use, loss or theft, deletion with malicious purposes, modification and other cases may harm public interest, organizations or ordinary citizens. US non-governmental organization *Identity Theft Resource Center* reports that, as the result of the disposal of e-waste with unreliable methods, 50 data loss cases, including the loss of state secret occurred in the government and military sector in 2014 (2.5 million text files) [2]. Therefore, ensuring information security stored in these drives is important and urgent for state, organizations, and each individual. Unauthorized dissemination of information (leakage) from drives is mainly carried out through the following channels.

- insider and outsourcing activities;
- research and development (R & D);
- manufacturing activity;
- paper and electronic data waste carriers.

Violation of information security by the outsourced employees during the insider activity (information security violations by current or former employees, partners, etc.), as well as outsourcing activities (transferring agency workers, job places, job function, and other resources to another organization) occurs through illegal data acquisition and transmission. Paper documents (sketches, projects, notes, calculations, reports, etc.), models, nodes, elements, product samples and their waste, defective products, production wastewater emitted to the environment, air mass, radioactive element ray generated by R & D, as well as manufacturing process may be confidential and secret data carriers. Information security of these sources must be provided by existing legislature,, organizational and legal documents, manuals, organizational rules, and so on.

In modern times, the foremost data drives are electronic. The vast majority of information security violations stored in electronic carriers occur when the stored data is not deleted or destroyed, if necessary. Here “if necessary” means possible interventions are expected to occur. These operations primarily include the followings:

- deletion of expired electronic and electrical equipment (including discharge of households) – becoming electronic waste;
- transferring to primary and secondary waste processing in accordance with the requirements of e-waste management system;
- disposal of domestic and industrial wastes;
- transferring to other institutions for repair;
- transferring electronic waste (e.g. computers) to other institutions as a gift or donation;

- transportation of carriers from one place to another (from departments to offices, from workplace to house, repair places, etc.).

Disposal of e-waste drives

According to the legislation of the Republic of Azerbaijan, regardless of working conditions, moral or physical deterioration, after the lifecycle of 9 years (by 10.1% in nominal depreciation) computers can be discarded. Discarded computers may be stored in the warehouse. According to the law of the Republic of Azerbaijan on "Production and Domestic Waste" the law [3] and the law on "Precious metals and stones" [4] computer is considered to be precious metal waste from the moment of discard since it includes precious metals (gold, silver and platinum group elements). To reproduce the precious metals in the composition of the waste, it must be processed in a specific way or be transferred to private institutions for this purpose. However, due to the lack of "e-waste" and "e-waste management" concepts in the legislation of Azerbaijan, there is no infrastructure for primary and secondary processing of this group of waste [5]. To avoid controversy with the provisions of the law, organizations usually delay discard of computers, as well as other electrical and electronic equipment (especially, if warehousing capabilities are limited), they store them in the warehouses or transfer them to kindergartens or schools as a donation, gift and so on [6]. In most cases, computers are discarded as household and industrial wastes. The same is true for households. Computers brought to disposal sites are eliminated by burying or simply throwing away.

Observations show that, in many cases, the entities dealing with households do not safely delete or destroy the information stored in discarded computers or information drives. "Safe disposal" means deletion of information that is not supposed to be recovered in any way. Otherwise, the data obtained by malicious parties in certain ways, may possibly be used. The practice proves that one of the "favorite" sources of information obtained by the professional intelligence officials is the waste sites (landfills). Deletion of the information in the drives is carried out by two technologies depending on the confidentiality and secrecy of data:

1. deletion technologies based on writing principles of the information on the carrier. The technology often uses two methods: a) deleting by the functional capabilities of the computer's operating system; b) termination by specific deletion devices.
2. deletion (destruction) methods based on other mechanisms.

It is not possible to delete drive's information reliably with the capabilities of computer's operating system software. Principally, operating system is configured so that the information does not disappear as a result of random error of the user, that is, being able to be restored if necessary. Hardware also takes it into account. We can review the technique of deletion of information through the operating system avoiding the principles of writing (reading) solid and soft magnetic, magneto-optical disks and diskettes, as well as magnetic tapes (streammers). Deletion is carried out in three ways:

- through standard "*Delete*" command of the operation system;
- writing new non-informative information instead of the information to be deleted (on the occupied sector in the carrier);
- re-formatting the drive.

None of these methods provide 100% deletion of the information. In fact, magnetic (magneto-optical writing (deletion) heads of the drives are provided so that there will not be sufficient magnetic (optical field) intensity to fully erase information. On the other hand, expansion of power (intensity) of writing and deleting facilities (Winchester, CD/DVD-ROM, etc.), magneto-optical heads of computer to delete information without any possible recovery would be resulted in about 2-3 times increase of their size, which is in contrasts to the principles of miniature computers (especially mobile computers). In other words, according to the residual

magnetism (optical stream) of carriers initial information is possible to be recovered through special technical devices. Therefore, this simple method, as a rule, is used for the deletion of non-confidential data without a state secret. It should be noted that each subsequent application method of the three deletes the information more reliable than the previous one. According to some reports, based on the track advances devices specially designed for counter intelligence and other bodies recover the original data deleted through the most perfect deletion tools [7]. Therefore, the only way to safely delete the carriers storing high-level state secrets is to melt them at high temperatures. The second technology uses facilities generating powerful magnet (optical field), which are applied in the following terms:

- to be used in the stand-by mode (Figure 1).

The carriers designed for deletion are removed from the computer and placed on external device and the device is enabled. The devices have different structures depending on the type of the drives. It is used to delete the carriers in the workplace.

- to delete in emergency situations.

The device is installed inside the computer. It is used for emergent deletion in the cases of sudden occupation or theft of law enforcement, tax authorities, government and other bodies. Switch button is usually installed in a hidden place.

a) b) c)

Figure 1. Deletion facilities for solid disks (a), floppy disks (b) and ZIP-drives (c)

In case of confiscation or theft, usually electricity supply of the room where computer is located is stopped so that the owner could not delete the drives. Therefore, the device is equipped with the source of stand-by power supply, and the ability to enable deleting facility via radio channels (radio controller, mobile phone etc.). In case of unauthorized acquisition of the carrier (theft, robbery) the options automatically activating the device are available.

- to ensure the safety of transportation (Figure 2).

Figure 2. Security case for drive transportation

It is used to delete information remotely in the case of loss, theft and etc. when moving to another place for certain purposes. Deletion device is installed in the case, attaché-case and other

similar bags. The disc is placed inside the device. It has numerous functions as self-power supply, remote control, breach alarm, and so on.

- Carriers for backup copies storage (Figure 3).

Archive carriers may also be exposed to the unauthorized intervention. It is used to delete the data in case of theft, replacement by other copies and so on. However, some emergency situations (fire, earthquake, flood, etc.) can cause loss of data backup. Therefore, careful organizations have several copies, which are stored in various areas (organizational units, private institutions etc.).

Other technical enforcement tools (the cables, locks, alarm devices, etc.) are used against unauthorized transportation of computer, de-rigging of computer for the carrier theft, changing the content and etc.

Figure 3. Security wardrobe storage for storing carrier backups

As the large-scale ZIP-storage, which replaced previous floppy disks, is based on the principle of magnetic recording devices, it is deleted through the devices with same working principles and different structures. Basically, utilization devices for various purposes are used for safe deletion of strimmers - magnetic recording tape drives, which are used for audio-video recording, their archiving and backup.

Reliable deletion of the information stored on flash memory devices is realized through the use of external devices. The memory element of these devices comprises integrated circuit transistors (EPROM), which are programmable and re-writable (readable) with an electric current. And therefore, it cannot be deleted through the magneto-optical field, but through electric current with the special-shaped high-voltage impulse signals. As a result of deletion the device becomes useless for rewriting and reading. When deleting the flash memory device with non-secret data through computer operating systems (through two of the above-mentioned three methods) it can be used again. These devices are produced in various versions with addition security features (deleting via remote radio channels, safe transportation, etc.).

Several non-electrical-magnetic-based methods are used to delete the information of magneto-optical disc reliably. For example, the essence of one of these methods is that the surface of the disc is covered with a thin layer of pyrotechnic composition and fired up with electrical impulse. In this case, the disk surface temperature heats up to 2000 °C and destroys the information in a short period of time, however disk itself is not spoilt [8].

R & D wastes (model, nodes etc.), defected production of electrical and electronic equipment are processed as electronic waste, i.e., an element of the applied ETIE system.

Information Safety of Paper Carriers

Paper carriers may include confidential information and state secrets. Practice shows that the information in the hand-torn paper components of any size may be recovered. Therefore, in order to destroy data paper, special paper destruction devices (PDD) such as shredder, grinder, and disintegrators are used (Figure 4).



Figure 4. Shredder, grinder and disintegrator

According to purposes, PDDs are usually divided into the following groups:

- individual PDD - used in small offices and houses; small and inexpensive;
- office PDD - used in medium and large organizations;
- archives PDD - used for the destruction of large amounts of paper carriers;
- universal PDD - used for the destruction of folders, books, magazines and so on.

Depending on the degree of secrecy and confidentiality the papers are cut into strips of certain width and length. 4th and 5th grade confidential information cut into vertical and horizontal sheets. For example, standard 08x4mm size is adopted for the US government documents. Destroying 5th grade information is done by chemical solutions or special high temperature ovens. The last destruction method is considered to be more reliable for paper carriers with state secret. Secret data is destructed by grinders and disintegrators cutting it into pieces of width and length smaller than a millimeter in diameter. The size of cut sheets by above-mentioned devices varies depending on data confidentiality. Following table provides these sizes (R - radius of round cut-sheets).

Table 1.
Destruction and confidentiality dependence

Data confidentiality degree	Shredder	Grinder	Disintegrator
	Sheet dimensions (mm)		
I II II IV V	12 x unlimited 6 x unlimited 4 x 80 0,8 x 20 0,1 x 13	R = 1,0	0,8 x 0,8

Obviously, investigation, classification and backup of the large-scale carrier content, establishing and operating their storage facilities require complex work and considerable costs, even though, the loss of important information or recovery is much more expensive.

The US Larry Ponemon Institute studies the character of information security incidents and assesses the damage caused by them and provides annual report. The results of the study conducted on 31 large commercial organizations are shown in Figure 5 and Figure 6 [9].

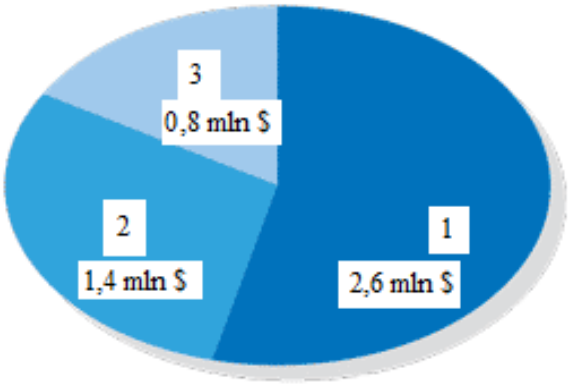

Figure 5. Average annual financial loss by an organization (by the US)

Annual average financial loss of an organization includes: 1) average cost of lost earnings: the losses resulting from decrease of authority, loss of customers, expenses for attracting new customers 2) direct losses: compensation paid to customers, drop of product and service costs, etc. 3) indirect losses: the costs incurred in litigation, informing customers about the information leak, payments mail and phones bills and so on.

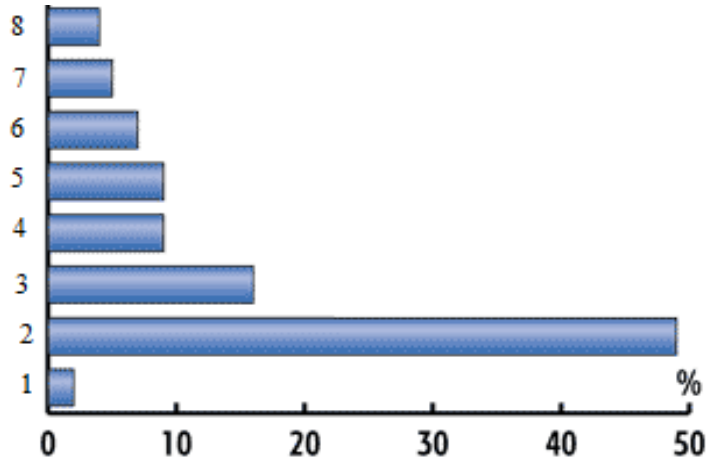

Figure 6. Nature of information leakage

Information leakage reasons include: 1) malicious programs; 2) data access prevention; 3) loss of backups; 4) insider activity; 5) loss of paper carriers; 6) outsourcing activities; 7) loss of mobile computers; 8) unknown reasons.

To show the seriousness of the consequences of the breach of information security, the following facts are mentioned:

1. important data recovery on a sheet averagely costs $ 1000,00 for specialized US companies [9].
2. A few years ago, the US Army distributed tens of thousands of personal computers as part of the improvement of computers provisioning to schools. Without any defined purpose, students, for the sake of the interest, restored the data on these computers, which contained state secret and confidential information, through regular programs downloaded from the Internet, and passed across the press. The implementation of the program was stopped after the scandal. Studies show that the carriers of personal computers were deleted through software capabilities of operating systems, which is unreliable method [9].
3. In 1979, the rebels, who captured the US embassy in Iran during the revolution, restored the information in the paper, which was deleted using shredder, and spread the information in a book form. It caused an international political scandal [10].

Each field of activity and each organization must establish its information security management system for data drives (ISMSDD) taking into account own capabilities and the nature of business features. To this end, the experience of a number of leading organizations and governments can be used. The management system should comprise the design and implementation of sustainable development concept in this area and management policies, current and future programs, and specific action plans (Figure 7).

Practices show that the cost of establishing and operating the management system is much less than the costs spent on the acquisition of stolen confidential and secret data, commercial secrets, including recovery of the lost data.

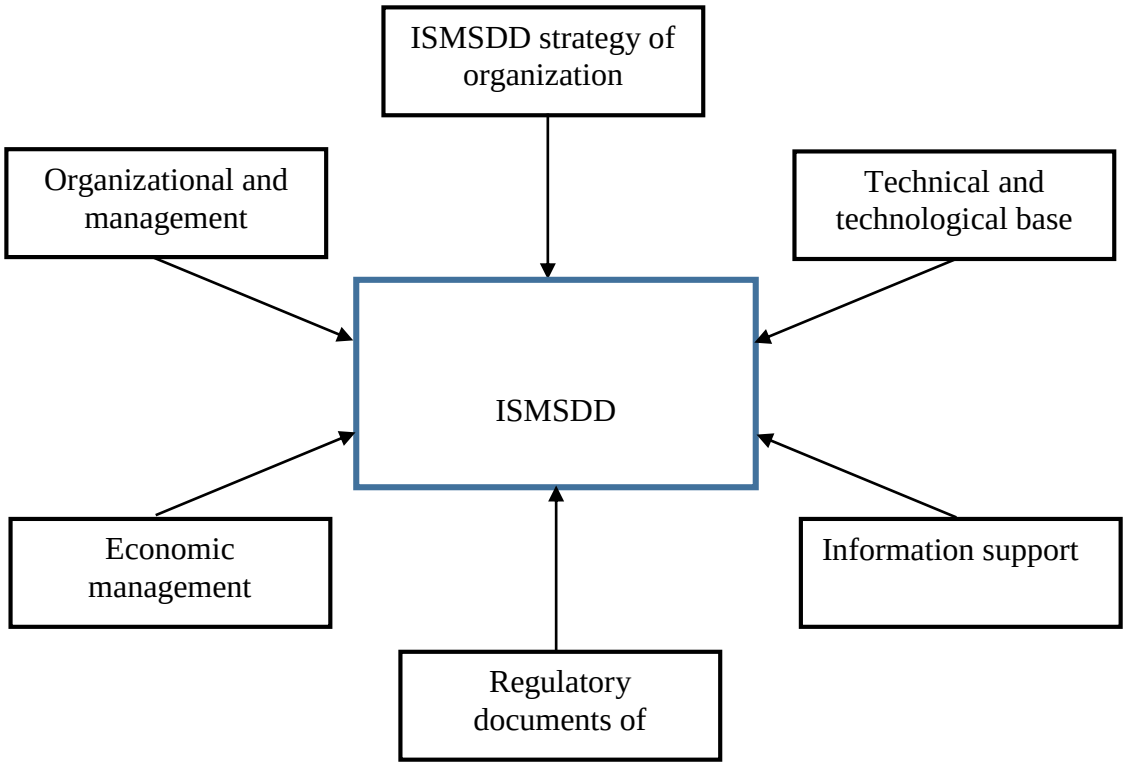

Figure 7. Architectural scheme of ISMSDD

Conclusion

The article studies scientific and practical aspects of information security and protection problems. Optimal methods are proposed for selection of facilities for storage, transmission and reliable deletion (destruction) of information stored in magnetic (magneto-optical) drives, strimmers, zip-drives, and flash drives depending on the degree of data secrecy and confidentiality. Similarly, reliable data destruction methods and devices for paper carriers comprising state secrets and confidential data are described. Studies show that leading organizations of some countries have created an effective management system to ensure information safety of information sources of electronic wastes. It is shown that management system covers disposal of electrical and electronic equipment, its storage, handling (transportation), backup, archiving, processing as waste, organization of regulatory documentations, economic incentive mechanisms, development and implementation of action plans. Finally, the feasibility of establishing appropriate management system is justified.

References

1. Directive 2012/19 / EU of the European Parliament and the Council of 4 July 2012 on waste electrical and electronic equipment, http://www.ec.europa.eu
2. Breach 2011 20120207pdf http://www.idtheftcenter.org/artman2/uploads/1/ITRC
3. Law of AR on "Production and Domestic Waste", http://www.qanun.az
4. Law of AR on "Precious metals and stones", http://www.qanun.az
5. Aghayev B.S., Aliyev T.S. Comparative analysis of electronic waste management systems in Azerbaijan and the European Union / Proceedings of Republic Scientific and Practical Conference of "E-government building problems" works. Baku: Information Technology, 2014, pp. 196-199.
6. Alguliyev R.M., Alakbarov R.G. Social and environmental problems of disposal of used computers. // Problems of Information Society. Baku, 2010, No 2, p. 38.
7. Prokofiev N. // Heavy artillery information security, Computer press, 2002, No 3, pp.115-118.
8. Aghayev B.S., Aliyev T.S. The problem of electronic waste and information security / republican scientific-practical conference on the problems of information security dedicated to the 90th anniversary of national leader Heydar Aliyev. Conference Proceedings. Baku: Information Technology, 2013, pp.145-148.
9. http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime
10. http://ru.wikipedia.org/wiki/ Shreder_(ustrojstvo)