Expert System for Modeling Threats and Protecting Premises from Information Leaks

Marina Rudenko [1], Evgenia Zhivago [1] and Andrei Rudenko [1]

[1] *V.I. Vernadsky Crimean Federal University, Prospekt Vernadskogo 4, Simferopol, 295007, Crimea*

Abstract

This paper considers the evolutionary path of developing physical ways of information leakage and methods of their minimization or possible elimination in the premises allocated for negotiations. The work aims to development of an expert system that interacts with the knowledge base, focused on modeling threats and means of protecting meeting rooms based on user-specified data and parameters. The features of the application, the principles of operation and the architecture of expert systems, a knowledge base developed for the intellectualization of the developed expert system are considered. The result of the work done is an expert system that implements the ability to simulate threats and protect premises from information leaks. The developed expert system can have practical application in organizations, the importance of information secrecy for which is one of the main tasks.

Keywords

Expert System, Information Leakage Channels, Knowledge Base, Knowledge Representation Model, Meeting Room, Information Security, Technical Leakage Channels

1. Introduction

In the realities of the modern world, information and its possession play a key role both in the ability to be competitive and in the process of economic development in general.

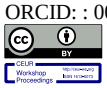
Information can be a product, service, raw material, and its correct application leads to various kinds of material benefits for its owner. As a result, each owner of information strives to protect it from dissemination and intruders. Often, such attackers are individuals or organizations interested in the possibility of unauthorized gaining access to confidential information and intending or attempting to organize such access [1, 3].

Also, do not forget that some companies work with confidential information, including personal data, the protection of which required by law [4][5]. The interests of the state in the information sphere are to create conditions for the harmonious development of the Russian information infrastructure, for the implementation of constitutional rights and freedoms of man and citizen in the field of obtaining information and using it in order to ensure the inviolability of the constitutional system, sovereignty and territorial integrity of Russia, political, economic and social stability, in the unconditional provision of law and order, the development of equal and mutually beneficial international cooperation [2]. Therefore, behind the successful development and maintenance of the functioning of enterprises, there is concern about ensuring information security in the field of business, entrepreneurship and production.

The topic of protecting premises and meeting rooms in particular is relevant, and in this area, developments are underway that will help to move from manual calculation of indicators to an automated process [6]. A large base of theoretical knowledge accumulated with recommendations for choosing and arranging a meeting room. However, in reality, it is not always possible to choose a room that meets the criteria for the selection of premises, due to various reasons - constructive, requiring large

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia

EMAIL: rudenko.ma@cfuv.ru (Marina Rudenko); zhivago.evg@cfuv.ru (Evgenia Zhivago); rudenkoandre@gmail.com (Andrei Rudenko)
ORCID: : 0000-0002-8334-8453 (Marina Rudenko)



changes that may entail delays in the work of the company or the subjective capabilities of a manager or a responsible person [7][9].

2. Physical paths of information leakage

Physical paths of information leakage according to state standard specification GOST R 50922-96, information security threat is a set of conditions and factors that create a threat of information security breach. All technical channels of information leakage can be divided into 4 groups are shown in the Table 1.

Table 1

Technical channels of information leakage

№	Channel	Example
1	Visual-optical channel	Windows of the meeting room from the side of the courtyard Ajar door Door
2	Acoustic channel	Floor of the controlled room Room walls Heating batteries Controlled room windows
3	Electromagnetic channel	Telephone PC Overhead power line
4	Material channel	Enterprise personnel Paper documents Meeting participant Industrial waste

The visual-optical channel is a TKU, arising due to the exit of the controlled zone of light energy carrying this or that information.

The visual-optical channel is understood as remote or direct observation, including television. Light emitted by a source of classified information or reflected from it in one of the ranges - infrared, visible or ultraviolet acts as a conductor of information.

One of the most common channels of leakage is acoustic, since hearing is the second most informative for a person. In the acoustic leakage channel, the carrier of information from a source to an unauthorized recipient is an acoustic wave in the atmosphere, will, or solid medium. Sources of an acoustic signal can be people, sounding mechanical, electrical or electronic devices, devices and means that reproduce previously recorded sounds [8][9].

In the electromagnetic channels of information leakage, the information carrier is electromagnetic radiation (EMP), arising from information processing by technical means:

- side electromagnetic radiation arising from the flow of informative signals through the elements of technical means of information processing;
- modulation by an informative signal of side electromagnetic radiation of high-frequency generators of technical means of information processing (at the frequencies of high-frequency generators);
- modulation by an informative signal of parasitic electromagnetic radiation of technical means of information processing (for example, arising from self-excitation of low-frequency amplifiers).

A material-material leakage channel can be understood as a variety of objects in various states of aggregation. These can be production waste, rough materials or defective products.

Depending on the nature and extent of the damage, it can be divided into:

- financial damage associated with the costs of restoring the company's information system, as well as due to downtime caused by changes in the information security system;
- material and moral damage caused to information owners, whose information was stolen and, as a result, damage to business reputation and business relationships was caused.

3. Expert system design

The most difficult and common are semi-structured or unstructured tasks associated with decision-making, control and management tasks. Expert systems are aimed at solving such problems [10][11].

Expert system - a computer system capable of partially replacing a specialist-expert in resolving a problem situation.

The use of expert systems can help achieve a number of positive aspects:

- exclude possible subjectivity;
- the ability to simplify the process by dividing the problem to be solved into smaller subtasks;
- there is no need to involve expensive experts and specialists;
- development of ES allows to accumulate human knowledge and experience;
- there is no need to study a large number of materials in order to make a decision or check the correctness of the decision of the involved expert;
- the ability to minimize contacts with strangers, keep confidential data that is undesirable for publicity;
- the solution can be obtained in a human-readable form.

Also, the ES has mandatory components that form it:

- user interface;
- ES user - it can be both an end user who wants to get a solution, and an expert who introduces new knowledge into the database, as well as a knowledge engineer who debugs the work of the expert system;
- knowledge base editor - implements the ability to edit, delete, change and add data;
- expert - a specialist in the required field, able to find reasonable, correct and effective solutions to the task;
- knowledge engineer - a person who has knowledge and skills in the field of computer science, artificial intelligence and the construction of expert systems, who can systematize, properly present knowledge and help the programmer in writing a software product;
- memory;
- inference mechanism - an inferred solution obtained during the operation of the expert system;
- system of explanations - a system of justifications, based on which this or that decision was made.

The basis of ES is the so-called knowledge base in a specific subject area. The data is constantly entered and accumulated in the process of building and operating an expert system.

4. Modeling threats and protecting premises from information leaks

In the modern world, market relations are moving away from industrial ones, and are increasingly becoming informational. Thus, information plays a key role in the development and functioning of market participants [12].

The reality is that a manager cannot always fully assess the existing threats of information leakage, of which there are many [13].

For example, consider a typical office is also used as a meeting room.

Sometimes, the leader does not even realize that his office is essentially a sieve from which valuable information flows without any special obstacles.

Physical methods of protection against information leaks are understood as a complex of technical, organizational and organizational-technical measures aimed at weakening or excluding the uncontrolled exit of classified information outside the control zone.

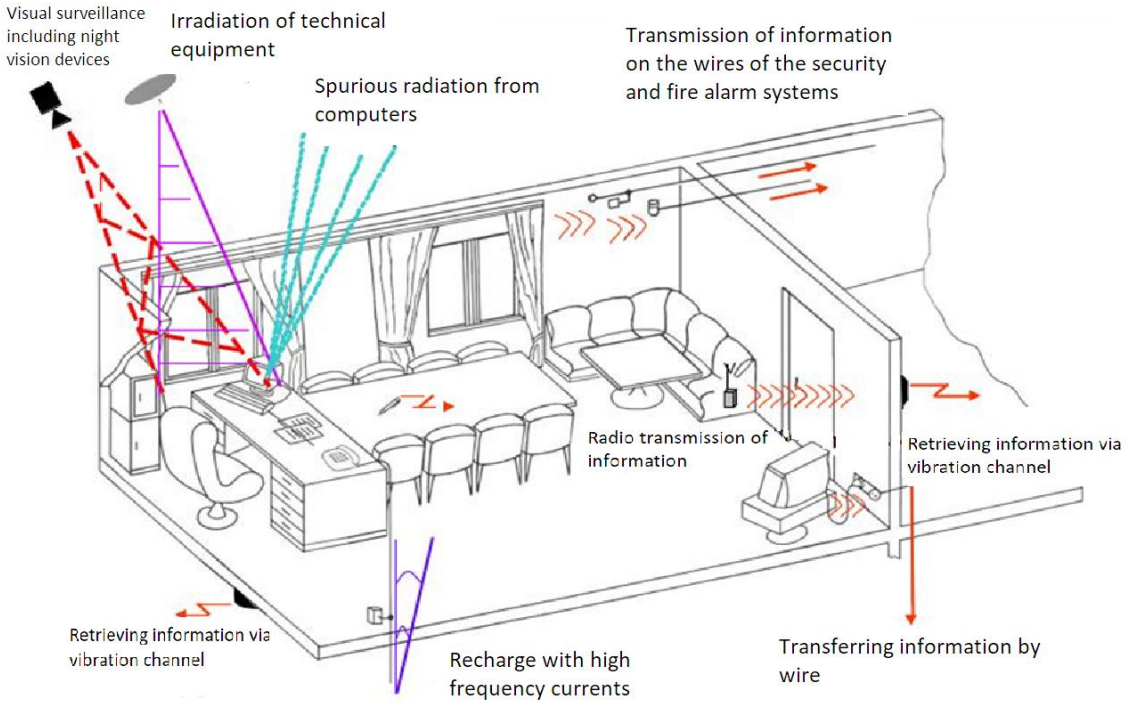


Figure 1: Peculiar properties of information leakage channels for premises

The following restrictions are imposed on protection methods:

- for protection, only funds certified and approved for circulation in the Russian Federation can be used;
- methods and means untested, prohibited or related to the spyware category are unacceptable;
- protection against leaks must be based on legal methods of dealing with them;
- for the successful functioning of the protective complex of measures, it is also necessary that it constitutes a single system.

The complexes of protective measures are divided according to the principle of grouping of leakage channels - methods of protection of visual, acoustic and vibration, electromagnetic and material-material channels of information leakage.

5. Knowledge base of the expert system

The basis of the expert system is the so-called knowledge base in a specific subject area. The data is constantly entered and accumulated in the process of building and operating the expert system. The organization of knowledge and its accumulation are important properties of any expert systems[13][15].

To solve the tasks assigned to the expert system, three databases needed to store information and indicators, which will form the knowledge base [14].

The representation of knowledge in expert systems is a fundamental concept that is a decisive aspect in development. To represent knowledge, a production model and a formal-logical model of knowledge representation chosen.

The production refineries are based on the rule (products):

IF <condition> THEN <action>. This rule consists of two parts: conditions - antecedent and actions - consequent. In the form of a production model of knowledge representation, the knowledge necessary for the system to display security recommendations is presented.

Formally, the logical model of knowledge representation is similar to the production model. This is partially true, but they make a huge difference. The difference is that the production model of knowledge representation does not define any connections between the stored objects of the domain.

6. Expert system for modeling threats and protecting premises from information leaks

The initial data will be all the necessary information about the room that the user wants to allocate for the meeting room, check and secure. The user enters information about the floor, the material of the walls, about the rooms nearby, about the ceiling, decoration, about windows and doors, about the ventilation, about the presence of radiation elements. The user also edits the scheme of his meeting room in the program designer.

As a result, the user will receive a scheme with color identification of the threat, recommendations in text form on the necessary measures to improve security.

The subtasks for solving the general problem are as follows:

- Processing of input data;
- Determination of the level of security and highlighting the element, depending on the level of security;
- Offer security for low-security elements;

Justification of decisions bases on the knowledge and experience of experts. The more experts involved in the development of the knowledge base. The more unbiased decision can be issued by the ES.

It can be difficult for the user to collect data on the materials of the room, on the presence or absence of certain elements that affect the security. Therefore, ES can give some error.

The expert system for modeling threats and protecting premises from information leaks "Avarazh" consists of a main form for entering data and describing the room considered by the user; forms for editing the scheme of the room in question; forms for training the expert system, which is necessary for experts to interact with the system; reference books of objects and materials and information about the expert system itself.

The program menu contains reference books for some objects, allowing you to more accurately classify objects when entering data into the system. The "Training" menu item opens the form that experts use to train the "Avarazh" expert system. The menu item "About the program" contains the documentation on the basis of which the expert system works - Federal laws, GOSTs, SNiP and a set of rules. It also contains an area where the results of processing the entered data are displayed. This area consists of a visual sub-area, which shows a diagram with color identification of the security levels of the elements of the tested room, detected leakage channels and recommendations for improving the level of protection of the room. When you select the "Training" menu item, a window appears in front of the expert, containing facts and fields for filling in the coefficients.

To create a room scheme, you need to press the "Edit scheme" button of the main form, by clicking the user enters the scheme editing mode on the new form.

Using shape buttons, you can add elements to the room that affect the safety of the room as a whole. Symbols have been introduced for some elements that may be intuitively incomprehensible. All added items can be removed using the Clear All button. If the created scheme satisfies the user, then by clicking the "Add to main window" button the resulting scheme is added to the main form for further analysis. All elements of the room layout can be resized, moved, deleted or added again. Also, if one element is varied, a tooltip appears.

7. Conclusions

On average, an expert needs about 6 hours to conduct a special survey of a room to measure indicators when choosing 15 control points, and about 2 hours for calculations. Thanks to the use of the "Avaraj" expert system, within 30 minutes, you cannot only receive recommendations that are understandable to a nonprofessional, but also clearly see the hazard levels of the existing leakage channels.

In the course of the work, all the tasks were completed and the goal of the final qualification work was achieved - the development of an expert system interacting with the knowledge base, focused on modeling threats and means of protecting meeting rooms based on user-specified data and parameters.

The novelty of this work lies in the development of an expert system in the field of threat modeling and protection of meeting rooms, which not only generates recommendations for protection, but also analyzes the existing leakage channels and has a graphical identification of the security level of room objects and their ability to cause these leakage channels.

This expert system has directions for further development and improvement, but already at this stage, it has an extensive and sufficient toolkit to complete the task confirmed by its commissioning at UNIG LLC.

8. References

[1] SEI Cyber Minute: Insider Threats. Available online: http://resources.sei.cum.edu/library/asset-view.cfm? assetid=496626 (accessed on 30 September 2021).

[2] Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. Int. J. Inf. Manag. 2016, 36, 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[3] Al-Dhahri, S.; Al-Sarti, M.; Ahmed, J. Information security management system. Int. J. Comp. Appl. 2017, 158, 29–33. DOI:10.5120/ijca2017912851

[4] Dupuis, M.; Khadeer, S. Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In Proceedings of the 5th Annual Conference on Research in Information Technology, Boston, MA, USA, 28 September–1 October 2016. DOI:10.1145/2978178.2978185

[5] Insider Threat Report. Insider threat report. Insider threat related data breach detection time. In Insider Threat Report: Executive Summary; Verizon business ready: New York, USA, 2019. https://www.verizon.com/business/resources/reports/insider-threat-report/

[6] Alzhrani, K.; Rudd, E.M.; Boult, T.E.; Chow, C.E. Automated big text security classification. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28-30 September 2016. Sustainability 2020, 12, 6217 14 of 14 https://www.researchgate.net/publication/309388110_Automated_Big_Text_Security_Classification

[7] Kim, K.; Kim, J. A Study on analyzing risk scenarios about vulnerabilities of security monitoring system: Focused on information leakage by insider. In Proceedings of the International Workshop on Information Security Applications, Jeju Island, Korea, 23–25 August 2018; Springer: Cham, Switzerland, 2018. DOI:10.1007/978-3-030-17982-3_13

[8] Shin, H.J.; Kim, M.H. A detection method of data leakage by cooperation of insiders. Int. J. Appl. Eng. Res. 2017, 12, 13321–13327. Corpus ID: 51808393

[9] Bromiley, M. Defend Your Business against Insider Threats; SANS Institute Information Security Reading Room, Sans Institute: Boston, MA, USA, 2019. Corpus ID: 173171997

[10] Mandelli, D.; Yilmaz, A.; Aldemir, T.; Metzroth, K.; Denning, R. Scenario clustering and dynamic probabilistic risk assessment. Reliab. Eng. Syst. Saf. 2013, 115, 146–160. https://dblp.org/rec/journals/ress/MandelliYAMD13.html

[11] Ha, D.; Kang, K.; Ryu, Y. Detecting Insider Threat based on Machine Learning: Anomaly Detection Using RNN Autoencoder. J. Korea Inst. Inf. Secur. Cryptogr. 2017, 27, 763–773. DOI:10.13089/JKIISC.2017.27.4.763, Corpus ID: 208108705

[12] Lee, J.; Kim, I. Detecting Abnormalities in Fraud Detection System through the Analysis of Insider Security Threats. J. Soc. E Bus. Stud. 2019, 23, 153–169. DOI:10.7838/JSEBS.2018.23.4.153, Corpus ID: 199710981

[13] Bokova O.I., Drovnikova I.G., Etepnev A.S., Rogozin E.A., Khvostov V.A. Methods of Estimating Reliability of Information Security Systems which Protect from Unauthorized Access in Automated Systems. DOI:10.15622/sp.2019.18.6.1301-1332

[14] Kim, A.; Oh, J.; Ryu, J.; Lee, J.; Kwon, K.; Lee, K. SoK: Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization. Sustainability 2020, 12(15), 6217; https://doi.org/10.3390/su12156217

[15] Oh, J.; Kim, T.; Lee, K. Advanced insider threat detection model to apply periodic work atmosphere. TIIS 2019, 13, 1722–1737. DOI:10.3837/tiis.2019.03.035