Development of a software tool for identification of information security information threats arising due to low–frequency acoustoelectric transformations

D Korochentsev[1], *L* Cherckesova[1], *P* Razumov[1,*]

[1]Don State Technical University, 1 Gagarina sq., Rostov-on-Don, 344003, Russia Rostov–on–Don, Russia

Abstract. The article considers the physical basis for the formation of a technical channel of information leakage that occurs due to low-frequency acoustoelectric transformations. The method of instrumental and computational control of the security of speech information in the considered channel of information leakage, which is currently used in special research, is presented with a representation in the form of a simulation model. Based on the developed simulation model, using the MVR design pattern, a software tool was developed. The main classes of software that implements the model are presented. The functionality of the developed software tool is demonstrated and recommendations are given for the possible use of a simulation model for identifying threats to information security that occur due to low – frequency acoustoelectric transformations.

1 Introduction

Currently, the technical protection of information is becoming increasingly important. This is primarily due to the active development of methods and means of obtaining information, allowing unauthorized receipt of an increasing amount of information at a safe distance, equipping office and residential premises, and recently cars and other vehicles, a variety of electrical and radio electronic equipment, which is a source of random dangerous signals.

The construction of an effective information protection system is possible only under the condition of a complete and comprehensive examination of the object of informatization (OI) for the presence of possible technical channels of information leakage (TCIL) [4, 8, 12].

Practically on any object of informatization there are certain technical means (TM) related to auxiliary technical means and systems (ATMS): telephones, fire and burglar alarm sensors, dispatch (loud-speaking) communication systems, office equipment, communication systems, etc. [1, 5, 6, 17–19]. In normal operation, these vehicles can form technical channels of information leakage.

The methods of unauthorized obtaining of protected information by connecting technical means of reconnaissance (TMR) to the functional lines of the indicated ATMS are well

* Corresponding author: center-bit@yandex.ru

known. As TMR, for example, low-noise amplifiers of low frequency with a high gain and special sets of connection elements can act [5, 11, 13, 14, 16, 17]. Such channels of leakage are created due to the phenomenon of acoustoelectric conversions (AEC) in the elements of technical means.

The manifestation of the AEC of the considered TCIL in most cases is not associated with the quality of performance of one or another vehicle, but is a concomitant of its activities.

In general, the information leakage channel formed by the AEC can be divided into low-frequency (LF) and high-frequency (HF) information leakage channels [1, 5, 14].

The aim of the research is to develop, in the form of a simulation model, a software tool for identifying threats to information security breaches arising from low-frequency acoustoelectric transformations.

2 Materials and methods

To identify the technical channels of information leakage, formed due to LF acoustoelectric transformations, special studies are carried out at the informatization object to assess the values of the "informative signal-to-noise" ratio Δ_i and verbal speech intelligibility W at the output contacts of the TM. Special studies are carried out in accordance with the methodology for instrumental and computational control of the security of speech information in the LF AEC channel (hereinafter referred to as the Methodology) [1, 14]. The technique is intended to assess the protection of acoustic speech information from leakage resulting from low-frequency acoustoelectric transformations, when informative signals containing acoustic speech information can be recorded as electrical signals in communication lines of technical equipment, in the ground bus, in the wires of the power supply network, and also when the TM is exposed to sound vibrations arising during pronunciation or speech reproduction. The essence of the considered Method [2, 3, 5, 7, 16] lies in the fact that the vehicle is acoustically affected by a tone signal at the geometric mean frequency of an octave $F_i, where\ \ i-octave\ \ number$.

At the output contacts of the TM, the signal and noise level $U_{ши}$ is measured. At the same time, the sound pressure of the tone signal is measured at the location of the TM L_i.

Then the acoustic source is turned off and the noise level $U_{ши}$ is measured.

Based on the results of processing the measurement results, the signal-to-noise ratio in the i-th octave Δ_i at the output of the auxiliary technical means and / or system is evaluated and compared with the standard value $\Delta_н$. When executing the inequality

$$\Delta_i \le \Delta_н \tag{1}$$

it is considered that the tested ATMS is not subject to the phenomenon of low-frequency acoustoelectric transformations.

Otherwise, the value for verbal speech intelligibility W_c is calculated. The calculated value W_c is compared with the normalized value $W_н$ [16, 5]. When executing the inequality

$$W_c \le W_н \tag{2}$$

it is established that the inspected ATMS is not subject to LF AEC.

Otherwise, it is necessary to assess the possibilities of intercepting speech information from the protected premises through the channel of low-frequency acoustoelectric conversion, for which it is necessary to determine the attenuation coefficient $K_{л,i}$ of dangerous signals of the line under study at the geometric mean frequencies of the octave bands [16]. Taking into account $K_{л,i}$ the investigated line at the geometric mean frequencies of the octave bands, the signal-to-noise ratio is calculated at the border of the controlled zone (CZ) in the i -th octave Δ_i^* .

When the inequality

$$\Delta_i^* \le \Delta_н \tag{3}$$

it is considered that the tested ATMS is subject to LF AEC, however, the characteristics of the investigated line do not allow an accidental dangerous signal to go beyond the boundaries of the controlled zone. If inequality (3) is not met, then the value of the verbal speech intelligibility W_c^* is calculated, which is further compared with the normalized value.

When the inequality

$$W_c^* \le W_н \tag{4}$$

it is established that the inspected ATMS is considered protected from information leakage due to the phenomenon of low-frequency acoustoelectric transformations, otherwise a decision is made on the need to use active or passive information protection methods. Conceptually considered the Methodology can be represented in the form of a simulation model, graphically shown in Fig. 1.

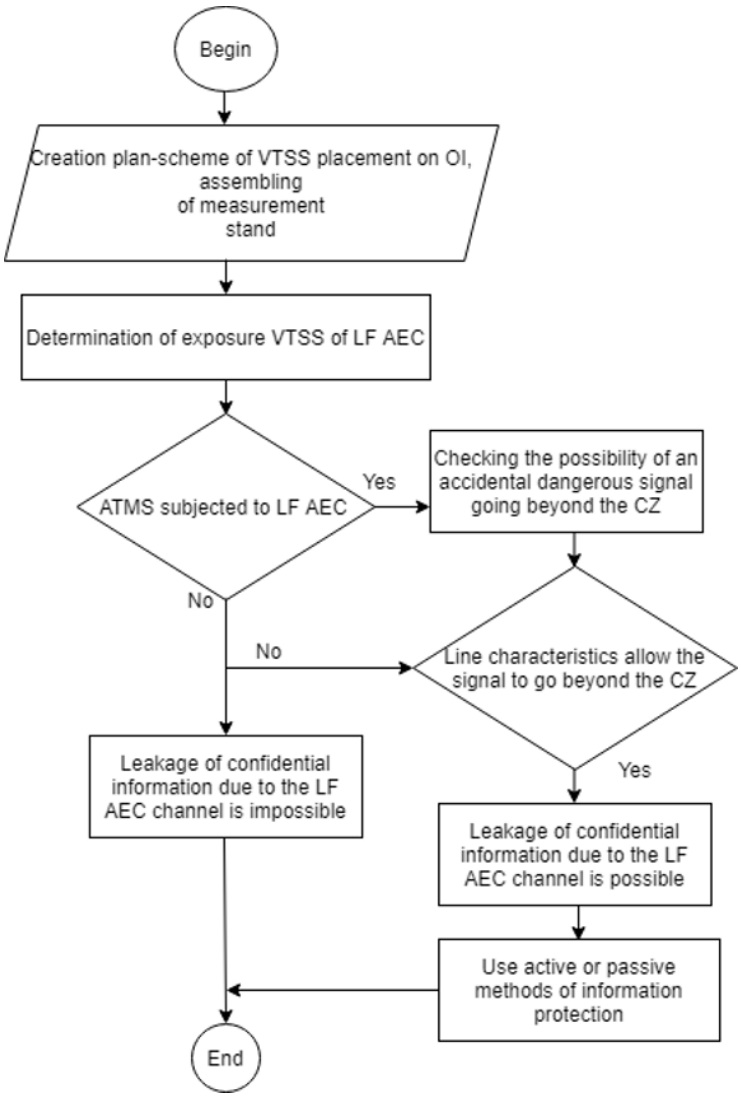


Fig. 1. Simulation model for determining technical channels of information leakage due to low–frequency acoustoelectric transformations.

To determine the susceptibility of auxiliary technical means and systems to the phenomenon of low-frequency acoustoelectric transformations, a special measuring stand is assembled, the general structure is described in [2, 3, 5, 7, 16].

After assembling the measuring stand, the low-frequency generator is tuned to the geometric mean frequency of the 1st octave and the levels of sound pressure L_1 and electrical signal and noise U_{cu1} are measured at the output contacts of the vehicle at the 1st octave frequency. Further, the low-frequency generator is turned off, and the level of electrical noise at the output contacts of the TM U_{u1} is measured in the bandwidth of the analyzer filter (the noise level is taken to be the minimum value U_{u} recorded during 30 s of continuous measurement). For geometric mean frequencies of 2–5 octaves, measurements

are carried out in the same way. In the event that passive or active protection means are used, the measurements are carried out in the same way, with the difference that the noise level is additionally measured with the protection means disabled.

If inequality (3) is not fulfilled and the determination $K_{л,i}$ is necessary, the circuit considered in [16,17] is assembled, and at the point of disconnection of the ATMS at the i -th frequency, a signal from the signal generator is supplied to the line under investigation and the voltage of this signal is measured with a probe at two points: near the supply signal to the line at point T1 ($U_{1,i}$) and at the boundary of the CZ at point T2 ($U_{2,i}$). The measurement results are recorded in the protocol of special studies.

Special studies for susceptibility to the phenomenon of low-frequency acousto-electrical conversions are carried out for all possible modes of operation of the ATMS and for all possible options for connecting the technical means of reconnaissance to the ATMS. The procedure for processing the results of measurements and calculations of $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$ is given in [2, 3, 5, 16].

3 Results and its discussion

A simulation model for identifying threats to information security breaches arising from LF AEC is implemented by means of a software tool, the components of which were developed in the C # language, using the .NET Framework 2.0 - 4.5.2. in the development environment Unity3D 2018.4 and JetBrains Rider.

As a design pattern for the software under consideration, the Model-View-Representative (MVR) pattern was used [9, 10, 20].

The main classes of software that implement the used design pattern "Model-View-Representative" are the following:

- Task - a exercise class that contains the interface of the ITaskCompleteChecker condition and returns the condition of the condition (completed / not completed) to the system. On the basis of this class, a system of stages is built, which checks the fulfillment of all tasks belonging to this stage (for example, conditions of the form "installation of a low frequency generator", "distance between a shielded acoustic speaker and ATMS", "distance between an auxiliary technical device and / or a system and spectrum analyzer ", etc.);
- IDataProvider is an interface that defines the type of data required by the class being requested (for example: the CalculationTableLabLFAT class is a table in the protocol with the results of special studies, and CalculationTableLabLFATProvider is a class that implements the IDataProvider interface with the CalculationTableLabLFAT parameter and provides the considered table of the special study protocol);
- TestBenchForLFAT - a class that implements the logic of the test bench. This class checks the assembly conditions of the measuring stand and simulates the values of the parameters of the used technical means in accordance with the selected option (for example: the sound pressure level of the acoustic signal at the geometric mean frequency of the 1st octave; the level of the electrical signal and noise at the output contacts of the ATMS at the frequency of the 1st octave etc.);
- TableView is a class that implements processing of measurement results. The class in question takes a data model, in accordance with which it builds a display. A data model not only contains information about what structure the data has, but also what logical connections there are with other data models, as well as how they are calculated.

When the software is launched, the user interface appears, which consists of four main components: the Menu panel (1), the device panel (2), the workspace (3), the task list (4) (see Fig. 2).

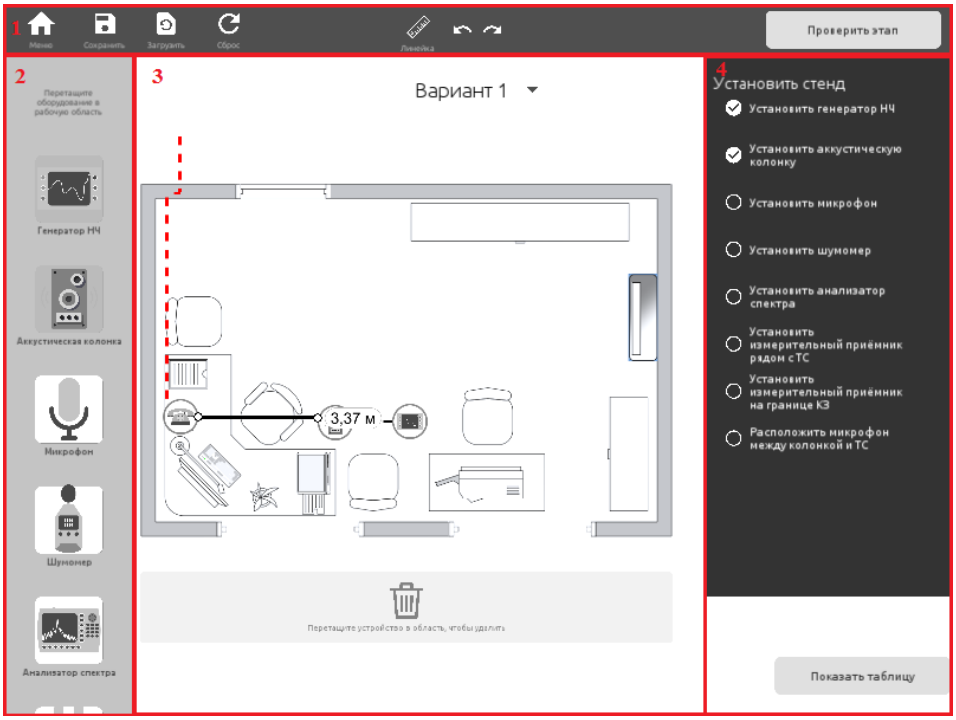


Fig. 2. User interface of the software tool.

The "Menu" panel contains the main controls. Among them there is a button for returning to the descriptive part of the simulation model (Menu button), a button for resetting the course of the stage of special studies of OI, a button for calling the tool "Ruler" and a button for checking the correctness of the stages of special studies of OI in accordance with the Methodology. The ruler button is a toggle button.

The "ruler" tool itself works only within the working area and allows you to measure the distance between two points (for example, between the ATMS and the shielded speaker (see Fig. 2)). The stage execution button is contextual and, depending on the state, either checks the stage of special studies of the informatization object, or calls the table from the protocol.

The toolbar contains the necessary control and measuring equipment (CRO) used in special studies of OI and is a pictogram and a signature with a name.

The work area contains the plan-diagram of the object of informatization, the area for deleting the CRO and the menu for selecting options, in the form of a drop-down list (as options, various basic technical means and systems (BTMS) are used, often located on the object of the OI, for example, in Fig. 2, option 1 is presented – ATMS - telephone set). When you change the option, the entire process is reset. The working area, within which the measuring stand is assembled, is an informatization object with schematically depicted enclosing structures, technical means, interior items, and furniture. At the bottom of the work area there is a delete area, when dragged into which the test equipment is removed from the work area and appears on the device panel.

The list of tasks contains the stages of the Methodology, divided into subtasks, which must be performed to complete the stage. Each subtask has a corresponding marker that displays its status ((completed or not completed), see Fig. 2).

The first step of the Technique is the assembly of a special measuring stand, for this you need to select the CRO on the device panel and drag it to the workspace. After clicking on the button for checking the completion of the stage, the program will check the conditions and mark those that were successfully completed.

After a special measuring stand has been assembled in accordance with the rules for carrying out instrumental control, it is necessary to make measurements and obtain the initial data for the calculation of $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$.

To do this, click on the icon of the corresponding CRO (for example, a spectrum analyzer or sound level meter) in the working area, thereby calling a dialog box in which the measurement results will be displayed. In the dialog boxes of some KIO there are controls (for example, in the dialog box of the speaker there is a switch for its state (on / off), and in the LF generator window, you can tune the geometric mean frequency of the generated signal from the 1st to the 5th octaves). In fig. 3 graphically depicts measurements of sound pressure levels L_1 and electrical signal and noise $U_{cш1}$ at the output contacts of the TM at a frequency of the 1st octave (275 Hz).

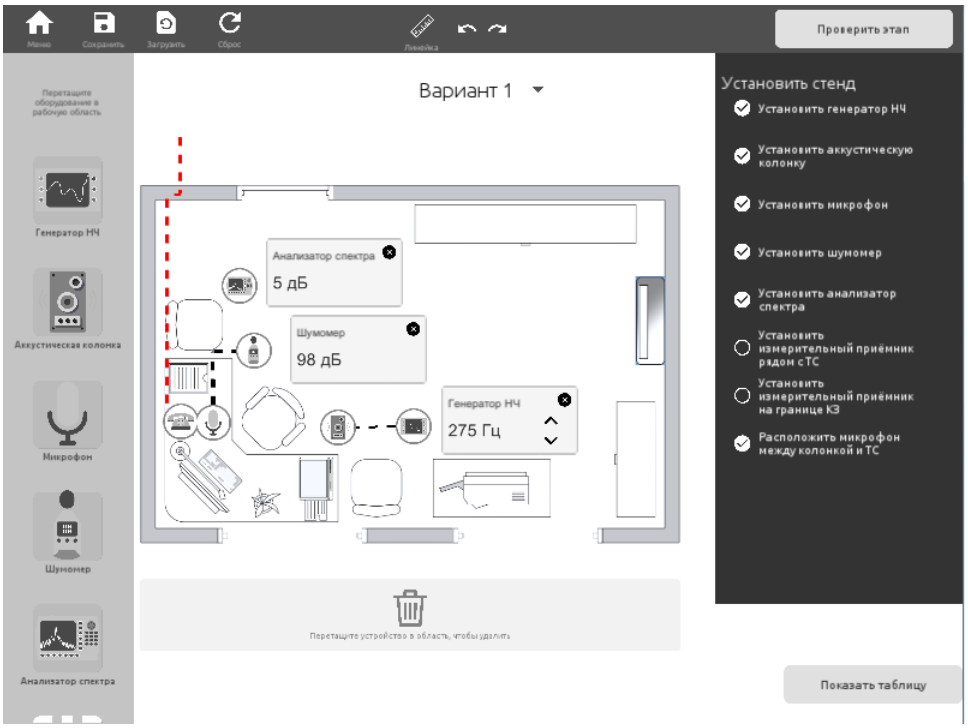
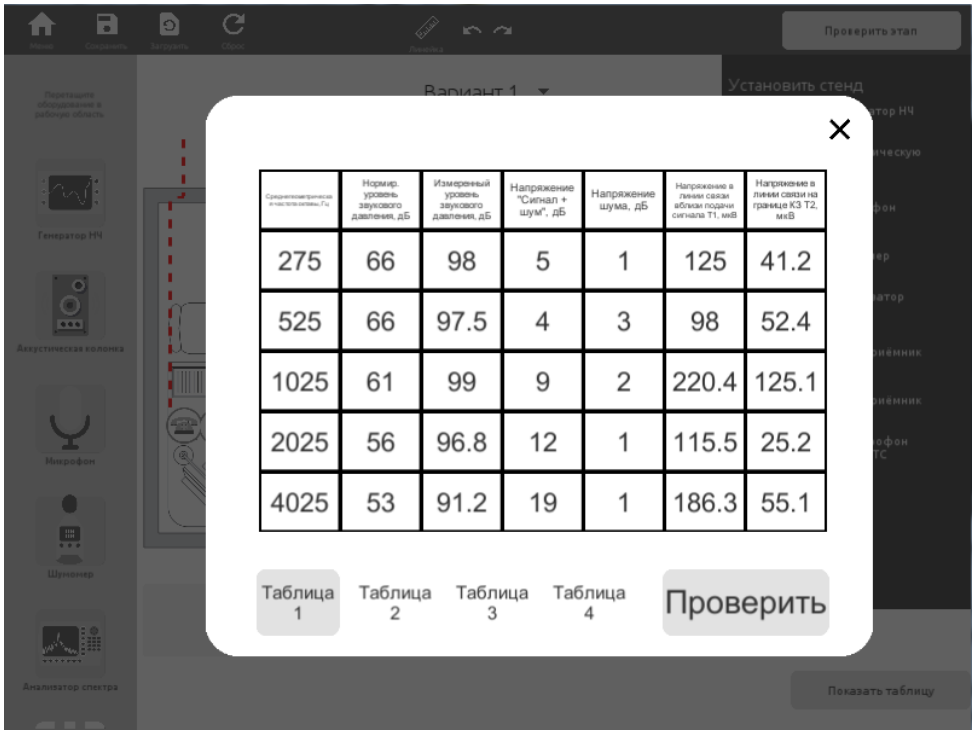


Fig. 3. Measurement of sound pressure levels and electrical signal and noise at the output contacts of auxiliary equipment and systems at a frequency of 275 Hz.

After measurements of the values of the sound pressure levels L_i, electrical signal and noise U_{cuii} at the output contacts of the TM, electrical noise at the output contacts of the TM U_{uii} ,, and in the case of non-fulfillment of inequalities 1 and 2, the signal voltage at points T1 ($U_{1,i}$) and T2 ($U_{2,i}$), on the geometric mean frequencies of all octaves, they are entered into the protocol of special investigations of the OI (Table 1, which appears after pressing the contextual button in the "Task List" panel, see Fig. 4).



	Нормир. уровень звукового давления, дБ	Измеренный уровень звукового давления, дБ	Напряжение "Сигнал + шум", дБ	Напряжение шума, дБ	Напряжение в линии связи вблизи подачи сигнала Т1, мкВ	Напряжение в линии связи на границе КЗ Т2, мкВ
275	66	98	5	1	125	41.2
525	66	97.5	4	3	98	52.4
1025	61	99	9	2	220.4	125.1
2025	56	96.8	12	1	115.5	25.2
4025	53	91.2	19	1	186.3	55.1

Fig. 4. Table of values measured using control and measuring equipment).

Further, the measurement results are processed and calculated with $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$ [2, 3, 5, 16]. The calculation results are manually entered into the table of the protocol of special studies, which is visually divided into tables 1 – 4.

Additional functionality of the table. 2-4 is the verification of the calculation results obtained in accordance with the procedure for processing the measurement results. If the correct value was entered into the table cell, after clicking the "Check" button, the cell fill color will change to green, otherwise the cell will turn red.

4 Conclusion

A simulation model for identifying threats to information security breaches arising from the phenomenon of low-frequency acoustoelectric transformations, executed in the form of a software tool, allows, by varying the set of initial data (the choice of options for the auxiliary technical means and / or systems used), to simulate situations in which the considered technical channel of information leakage may be relevant (calculation) and verification of the fulfillment of inequalities 1–4).

Such a simulation model can be used by security specialists of both large and small enterprises that implement information protection measures. In addition, this model creates conditions for its active implementation in the educational process of training specialists in the field of information security, using both traditional (in the form of contact work) and distance learning.

The developed simulation model can be used in the study of such disciplines as: "Technical information security", "Technical means of information security", "Attestation of objects of informatization", etc.

References

1. Buzov G A 2005 *Protection against information leakage through technical channels: the manual* (Moscow: Hotline-Telecom) p 416
2. Volkov D S 2014 *Scientific search* **25** 4-6
3. 2002 *Collection of temporary methods for assessing the security of confidential information from leakage through technical channels* (Moscow: State Technical Commission Of Russia)
4. *Russian Federation Standard GOST R 51275-2006*
5. Durakovsky A P 2015 *Control of speech information security in premises Certification tests of auxiliary technical means and systems for information security requirements: Tutorial* (Moscow: National Research Nuclear University MEPhI) p 152
6. Emelyanov S L 2010 *Information processing Systems* **3** 20-23
7. Zheleznyak, V K 2000 *Special technique* **4** 39-45
8. Zaitsev A P 2009 *Technical means and methods of information protection* (Moscow: Mashinostroenie) p 507
9. Pavlovsky Yu N 2000 *Simulation models and systems* (M: fazis: VC RAS) p 134
10. *Development patterns: MVC vs MVP vs MVVM vs MVI* https://habrcom/ru/post/344184/
11. Skripnik D A *General issues of technical protection of information* http: / / www intuit ru /goods_store/ebooks/8563
12. 2001 *Special requirements and recommendations for the protection of confidential information, the state Commission of Russia* (Moscow)
13. Titov A A 2010 *Engineering and technical protection of information: A textbook for students of the specialties Organization and technology of information protection* (Tomsk: Tomsk state University of control systems and Radioelectronics) p 197
14. Torokin A A 2005 *Engineering and technical protection of information* (Moscow: Helios ARV)
15. Chaliapin D B 2009 *The world of security* **5** 47-53
16. Horev A A 2009 *Information Protection Insider trading* **1** 42-52
17. Horev A A 2009 *Special technique* **5** 12-26
18. Horev A A 1998 *Protection of information from leakage through technical channels Part 1 Technical channels for information leakage* (Moscow: state technical Commission of the Russian Federation) p 320
19. Horev A A 2000 *Methods and means of information protection Textbook* (Moscow: MO RF) p 316
20. Vijini Mallawaarachchi *Towards Data Science* https://towardsdatasciencecom/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013