Theme of the final qualifying work: The organization of the protection of confidential information during meetings (on the example of the share of investment - Commercial Industrial Construction Bank "Stavropolye", Public Corporation branch in the city of Pyatigorsk)

The author of the final qualifying work: Mariam Borisovna Khasanova

Supervisor: Ryndyuk Victoria Alexandrovna, Ph.D., Associate Professor, Department of "Information Technology, Mathematics and distance learning tools."

Background study: Due to the high role of confidential information in the banking systems, as well as the features of the existing mechanisms of protection, the development of Russian subsystems protection of confidential information occurs within the framework of existing legislation and the various aspects of information security. Plenty of options for development generates no single model of the subsystem to protect confidential information, the different approaches to its defense, using a variety of mechanisms and tools, and, accordingly, the coexistence of different options subsystems. The above mentioned problems can be solved within the framework of the design of particular models of subsystems. So it follows out that the conduct of this study on the protection of confidential information during meetings is relevant and constructive.

The purpose of the study - the development of subsystems to protect confidential information in the meetings of the bank.

Research objects:

1) analysis of special and methodological literature, regulatory and legislative acts of the Russian Faderation on the protection of information, the study of the theoretical aspects of the protection of confidential information in the bank;

2) the study and analysis of a set of measures for the protection of information in the organization;

3) identification of gaps in the protection of confidential information in the meetings of the bank;

4) development of subsystems to protect confidential information during meetings.

The theoretical significance of this work lies in the fact that the analysis of specific and methodical literature, regulatory and legislative documents of the Russian Federation for the Protection of Information has been done; the theoretical basis of the bank "Stavropol" of a branch in the city of Pyatigorsk as well as the main channels of leakage of confidential information during meetings have been studied; the particularities of the protection of confidential information in the office for meetings were revealed.

The practical importance is the development of subsystems to protect confidential information in the office for meetings.

Research results: The bank established various means of protecting information, but, in our opinion, they do not provide any confidential information during meetings. Moreover, a study in which the meetings are held, not even equipped with specialized tools for data protection. Therefore suggested to develop a sub-system protection of confidential information during meetings of the director's office of the bank.

It’s necessary to install:

1. Selective field indicator «RAKSA-120", which will search for radio transmitting devices used for eavesdropping audio - and video in the office;
2. Protection device wired - Scrambler «Panasonic»-SCR will protect speech information when speaking of acoustic monitoring and eavesdropping. It can be used either interlocutor similar product, or "Mobile scrambler";
3. Cell network «Anti-bug PS1 » will suppress the activity of cell phones in the room for meetings;
4. AC suppression filter OP-10 prevents leakage of information through supply chains, and office equipment to protect against interference, do not miss the informative signals about working office equipment;
5. Shielding copper grid space, as this embodiment, unlike transmits light shielding

sheet and the air easier sheets therefore it is much easier to transport and install;

6. Aluminum screen battery is welded at the input to the entire circumference of the sleeve overall screen to ensure complete screening of the room;

7. Metallized film on the glass will increase the thermal protective performance of windows, protect against leakage of information through various channels, will reduce the tension in the room of the electromagnetic field generated by external sources;

8. Windows with glazing "Triplex" sound insulation properties will enhance the room;

9. Door "Outpost M65" will provide reliable protection of acoustic information due to the contours of the 4 seals and additional heat and sound insulation;

10. The complex vibro-acoustic protection "Baron" speaker reliably protect the information circulating in the office of the means of acoustic speech intelligence.

11. The system of guaranteed data destruction "SGU-2" will provide reliable erasing confidential information stored in the machine as follows:

- the destruction of files containing sensitive information by writing on their physical addresses clobbered sequences due to the global destruction of the information on hard disks, flash-drives, hard drives and volumes of floppy disks to interact with an electronic key for added protection against unauthorized use of the system.

Also the following arrangements are provided:

1) prior to the meeting to conduct a visual inspection of premises to identify by the embedded device security officer and a person familiar with the usual office setting, for example, employee protection;

2) immediately prior to the meeting of protection adjacent to the office premises should be inspected for removal of these employees or third parties that may result directly through the interception of communications ventilation system or through the wall by means of special equipment, office must be closed on the time of the meeting and the entrance must be monitored;

3) the number of persons involved in confidential negotiations should be kept to a

minimum;

4) entry of unauthorized persons during the meeting should be prohibited;

5) the security of the cabinet should be developed during a meeting, as well as monitoring the situation on the floor. During the closed meeting strangers or employees of the organization must be avoided near the door of the cabinet;

6) Any work in the office, held outside the time of the confidential meetings should be mandatory in the presence of a security officer;

7) after a cabinet meeting should be carefully inspected, closed and sealed;

8) between the meetings the cabinet must be closed, and the keys are handed over to the cabinet guard duty shift on receipt and stored at the guard post, access should be established by management.

These measures of organizational information security are considered highly effective and have no serious material costs or problems with the staff and can be used both individually and collectively, that will increase the level of information of the object.

Leakage of confidential information carries a certain negative economic consequences for the bank. Consequently, investment in improving the protection of information in the bank, in particular subsystem protection of confidential information is completely justified.

Subsystem Privacy Policy was created to improve the information security system of the bank so that the forward projected economic profit from the introduction of a subsystem is missing.