Chemical Technology, Control and Management

Manuscript 1461

INVESTIGATION OF INFORMATION SECURITY INCIDENTS IN THE ENTERPRISE

Fayzullajon Botirov

ISSN 1815-4840, E-ISSN 2181-1105
Himičeskaâ tehnologiâ. Kontrol′ i upravlenie
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2023, №3 (111) pp.64-69.
International scientific and technical journal
journal homepage: https://ijctcm.researchcommons.org/journal/

Article history: Received 11 April 2023; Received in revised form 13 June 2023; Accepted 28 June 2023; Available online 11 July 2023

Since 2005

INVESTIGATION OF INFORMATION SECURITY INCIDENTS IN THE ENTERPRISE

Botirov Fayzullajon

TUIT named after Muhammad al-Khwarazmi,
Address: 108, Amir Temur st., Tashkent city, Republic of Uzbekistan,
E-mail: botirov_fz@mail.ru, Phone:+998-97-751-16-97.

Abstract. *This article analyzes the concept of investigating information security incidents and the processes of responsibility for their commission, checking the place where the incident occurred, collecting and storing their data, as well as organizing the investigation of information security incidents at the enterprise.*
Keywords: *information security, incident, investigation, crime, criminal, punishment, evidence.*

Аннотация: *Ушбу мақолада ахборот хавфсизлиги инцидентларини тергов қилиш концепцияси ва содир этганлик учун жавобгарликлар, инцидент содир бўлган жойни кўздан кечириш ва далилларни тўплаш ҳамда сақлаш, шунингдек корхонада ахборот хавфсизлиги инцидентларини тергов қилишни ташкил этиш жараёнлари таҳлил қилинган.*
Таянч сўзлар: *ахборот хавфсизлиги, инцидент, тергов, жиноят, жиноятчи, жазо, далил.*

Аннотация: *В данной статье анализируется концепция расследования инцидентов информационной безопасности и процессы ответственности за их совершение, проверки места, где произошел инцидент, сбора и хранения данных, а также организации расследования инцидентов информационной безопасности на предприятии.*
Ключевые слова: *информационная безопасность, инцидент, расследование, преступление, преступник, наказание, доказательства.*

Introduction

Today, the spread of computer technologies has become commonplace, and today it is difficult to imagine the activities of any enterprise or organization without computer tools. They are introduced to new and new spheres of activity; more important and more serious issues are assigned to them

Information security incident investigation concept and responsibilities

But along with the ever-expanding scientific and technical development processes on a global scale, types, forms and manifestations of crimes that did not exist before are emerging, that is, crimes related to the field of information technologies are emerging, both their number and type is also increasing. This situation, in turn, required the legislator to take measures that could not be delayed. Consequently, a lot of work has been done in this regard in our country, and a number of normative legal documents have been adopted that regulate the activity of preventing and combating crime in the field of information systems.

The Laws of the Republic of Uzbekistan "On Guarantees and Freedom of Information", "On Principles and Guarantees of Freedom of Information", "On Informatization", Cabinet of Ministers' Law "Using Electronic Digital Signatures" 5 and others include the decision on improvement of the legal framework in the field of law [1-3].

Thus, relations in the field of information technologies have criminal-legal protection, as a result of which closed (confidential) information was formed as a new object of crime. Development of methods of investigation of these crimes, taking into account their uniqueness, is one of the urgent problems today.

In the criminal process, inspection is one of the most important investigative actions and allows to collect the most information about the crime.

In addition, when it is not possible to involve an expert in the field of information technologies in the investigation, the circumstances that the investigator should pay special attention to at the scene of the incident and the tasks that he should perform as the head of the investigative team are highlighted.

Investigate the scene of the incident and collect and preserve evidence. An IT crime scene investigation is one of the most important and most information-gathering investigative activities in a crime. This investigative action includes a number of important conditions, including:

- the main feature of the incident being studied, the presence of a criminal element in it;
- the place and time of the crime; what were the actions of those involved in the crime;
- goals and motives; what objects or things were left at the scene of the incident;
- how the perpetrators entered the place of the incident, how long they were there;
- what technical means and documents were used to reach the subject of aggression and commit illegal actions with him;
- what actions were taken to hide the real events;
- where to look for negative consequences and their traces;
- allows you to determine what caused the occurrence of negative results and others.

It should be noted that the "incident scene" and "crime scene" may not be the same. A criminal act may be committed remotely over computer networks in one location, and its consequences occur elsewhere.

Depending on the specific investigation situation, the investigation team includes the following personnel:

- an investigator specializing in the investigation of crimes in the field of information (the head of the investigation team);
- employee of the department for combating crimes in the field of information technologies;
- an operative assigned to the area where the crime occurred;
- a criminologist-expert with certain knowledge in the field of finding, researching, recording and obtaining traces of this type of crime;
- an expert on computer equipment that should be examined during the investigative process;
- a specialist who has sufficient knowledge of the technological process carried out when crime traces are found;
- a person materially responsible for the digital information (its digital information carrier or computing device) affected by the crime;
- applicant or victim [4,5].

The members of the above-mentioned investigation-quick group to the investigator to study and record the environment; finding, recording, obtaining and preserving evidence; preliminary investigation of necessary evidence at the scene of the incident; to identify objects that will be needed for future research; determine the circumstances that allowed the crime to occur; to highlight specific traces in the report; use of technical means in the process of investigation; drawing up plans, drawings and schemes; provides assistance in choosing an effective direction in the search for criminals, witnesses and the victim, etc.

This investigative action should be prepared in advance and planned in detail. Initially, it is advisable to do the following [6,7]:

- identification of the persons participating in the investigation based on the investigation situation that has arisen;
- clearly and fluently define the goals and sequence of actions to each member of the investigation team;
- attract relevant specialists and arrange for them to bring the necessary technical means (except for the technical means at the disposal of the investigator and forensic expert);

- to explain to the participants their rights and obligations, the set goal, as well as precautions when moving in the place of the incident and working with special substances before starting the investigation;

- selection of neutrals, instruction and explanation of their rights and obligations. It is desirable to attract persons who have sufficient (not inferior to the knowledge of an average personal computer user) knowledge in the field of computer information in the selection of biases.

After the investigation-ambulance team arrives at the place of the incident, the investigator should perform the following actions [8,9]:

1. To ensure the access of persons unrelated to the work to the place of the incident and the protection of the object. Conditionally, the following should be protected:

- the area where the incident occurred;
- the place where the computer equipment used to detect crime traces is installed;
- a local network server that manages the technological process and stores information about the last operations;
- points of disconnection of the source of electric current (if the equipment is turned on).

In this situation, the following should be taken into account: working at the computer keyboard, turning it off (or turning it on) from the power source, disconnecting (or connecting) communication with the local network server and peripheral devices - computer information, digital media and paper. may result in the modification or deletion of minor documents. Therefore, if the computing device or other electronic device is turned on (off) at the beginning of the investigation, it should remain in its position until the examination by the relevant expert is completed.

2. Ask the victim (applicant), materially responsible person and witnesses in order to clarify the true content of the incident, the change of the equipment available at the place of the incident, the actions of each person before the arrival of the investigative team. elimination (questions identified during a detailed inspection of the incident site will be clarified);

3. When the investigation-emergency team arrives at the place of the incident, record the situation in the report, make a photo or video recording with orientation or view;

4. Assigning tasks to the members of the investigation team that went to the scene of the incident. In particular:

- to the regional operative representative - to make a drawing of the place where the incident happened, to explain that all the traces found during the inspection of the place of the incident should be reflected in this drawing. It is intended to attach an expert involved in the investigation to provide practical assistance in determining the state of connection of computer equipment to each other and peripheral devices, security systems limiting access to computer information, elements of various video surveillance security systems and other situations when creating a drawing. according to In addition, instructing the regional operational representative to conduct a number of tactical operations (opening a hot trail of a crime, personal search of an arrested person, interviewing the applicant and witnesses, etc.);

- assigning tasks to an expert-criminologist to identify traces of crime;

- to the expert on the computer equipment that should be examined during the investigative action, to determine the type of the computer equipment, the purpose of use, the possibilities of communication, as well as the electronic documents and other computer information relevant to the work in the memory of this equipment tasks such as providing practical assistance to the investigator in obtaining and recording in the report.

It is advisable to use an "eccentric" tactical method when conducting an investigation of the scene of an information crime incident.

In this process, depending on the type of location where the incident occurred, the "hub" may be the place where the computer equipment used to commit the crime is installed, or the workplace where the tool prepared for the commission of the crime is manufactured.

In the report of inspection of the place where the incident took place, drawn up as a result of investigative action, attention should be paid to the following [10]:

- the name and tasks of the inspected object;
- territorial location of the inspected object, access roads to it, buildings around it and the distance to them;
- the presence of the object's security system, its location and appearance, if any, as well as special protective signaling devices aimed at preventing the leakage of computer information;
- the location of the computer equipment that can be used to commit a crime in relation to the door, window, other computer equipment, video surveillance equipment (if available) and others in the building;
- to other computer equipment and electrical equipment available in the room, except for the computer equipment of interest in the investigation;
- the presence of communication channels or technical means of connecting with other computing devices of the computing device where the crime was committed;
- the availability of technical means of computer equipment that can be used to commit a crime to connect with computer equipment in other rooms (if available, the limits of inspection of the place where the incident took place can be significantly expanded);
- traces left by the criminal in the facility, on the access roads to it;
- to the availability of documents of the computer equipment under review.

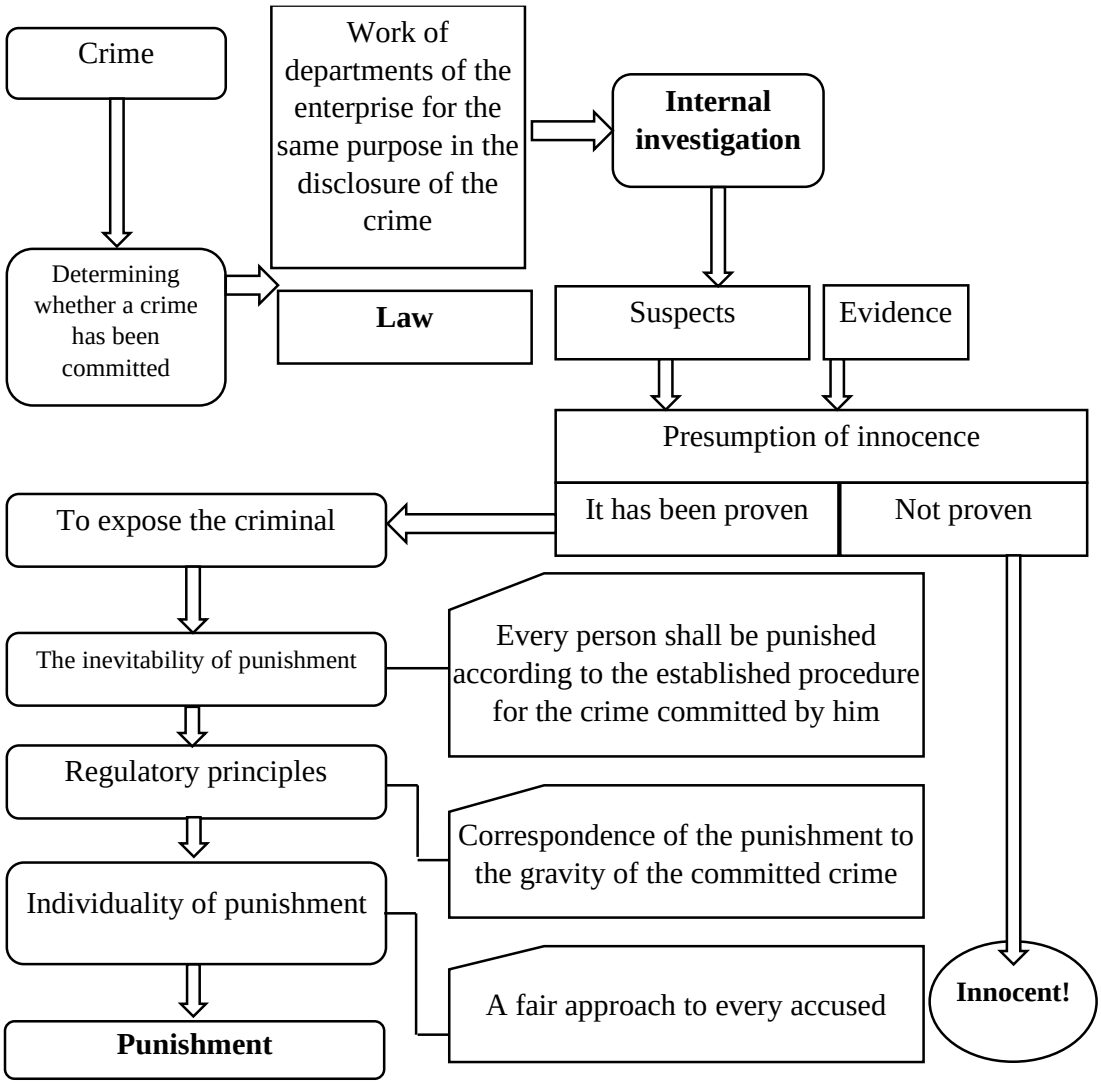

Fig. 1. ***Organization of investigation of information security incidents in the enterprise.***

From the above, it can be concluded that in addition to the inspection of the scene of the incident in the field of information technology, complex rapid search and inspection activities are carried out, which leads to the implementation of other investigative activities that cannot be delayed. may occur, including: search, seizure, inspection of documents and objects, detention, interrogation, presentation for identification, etc.

The purpose of the internal investigation- to find the person responsible for the incident, to determine the cause of the incident, to develop requirements and proposals to avoid such incidents in the future.

The main tasks of the internal investigation are: to find out why the worker committed the crime, under what circumstances and circumstances; determining the degree of guilt of a specific person or persons involved in the crime; development of recommendations on the organization and conduct of warning-preventive activities to eliminate the types, causes and circumstances of crime (Fig. 1) [11].

Investigate, identify, analyze and evaluate information security incidents. Ensuring the successful operation of these steps in taking measures against incidents in a timely manner and correctness.

Implementation of the principle of inevitability of punishment is one of the important conditions for the effectiveness of legal responsibility and the performance of its tasks.

The principle of inevitability of responsibility means that a person will be punished according to the established procedure for the offense committed by him, regardless of his official or material status.

The principle of inevitability of punishment should not contradict the principle of inevitability of responsibility - the presumption of innocence. Every person accused of committing a crime is presumed innocent until proven guilty in accordance with the law and until proven guilty by a legally binding verdict [12-14].

Conclusion

Organization of internal investigation in the enterprise is entrusted to the department of internal security. A commission will be established by the head of the enterprise to conduct an internal investigation. In some cases, the investigation may be conducted by a specialist of the information security control center. Depending on the nature of the crime, employees of the personnel department of the enterprise and employees from other departmental departments are included in the ranks of the commission members. The duration, completeness and impartiality of the commission's work are organized by the chairman and carried out by the employees. The duration of the investigation is usually indicated by the head of the enterprise. The results of the internal investigation will be formalized through service documents after the investigation is completed. Investigative materials are stored in the Department of Homeland Security for several years, after which they are archived.

References:

1. Botirov, F.B., Gafurov, Sh.R. (2021). Automation of information protection processes in the enterprise information system. *Ict in education: Challenges and solutions, International conference*, Tashkent, 62-66.
2. Botirov, F.B., Gafurov, A.A. (2021). Information security incident management processes. *Ict in education: Challenges and solutions, International conference*, Tashkent, 66-68.
3. Botirov, F.B., Gafurov, Sh.R., Gafurov, A.A. (2021). Identification of key persons in the information security incident management process and distribution of roles between them. *Chemical technology. control and management*, 3(99), 72-77.
4. Botirov, F., Gafurov, Sh. (2021). Structure and characteristics of the information security monitoring system. *The use of information and communication technologies in the training of specialists in the air defense system International online scientific and practical conference*, Tashkent, 375-380.
5. Botirov, F., Yusupov, B., Gafurov, Sh. (2021). Assessment of reliability of information protection means in information security monitoring systems. *The use of information and communication technologies in the training of specialists in the air defense system International online scientific and practical conference*, Tashkent, 381-387.
6. Botirov, F., Yusupov, B., Gafurov, A. (2021). A structural approach to incident management and security improvement. *The use of information and communication technologies in the training of specialists in the air defense system International online scientific and practical conference*, Tashkent, 388-394.

7. Fayzullajon, B., Azam, G., Sherzod, S. (2023). Handling Information Security Events and Incidents. *In: Ranganathan, G., Fernando, X., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 383. Springer, Singapore. https://doi.org/10.1007/978-981-19-4960-9_40.
8. Fayzullajon, B., Sharifjon, G., Sherzod, S. (2023). Methods for Assessing Information Security Incidents in the Enterprise and Making Decisions. *In: Ranganathan, G., Fernando, X., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 383. Springer, Singapore. https://doi.org/10.1007/978-981-19-4960-9_12.
9. Fayzullajon, B., Azam, G. (2021). Stages of Processing an Information Security Incident. *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, 1-3. doi: 10.1109/ICISCT52966.2021.9670063.
10. Botirov, F.B. (2020). Reliable risk assessment method for effective organization of information security at enterprise. *Chemical Technology, Control and Management*, 2020(4), 64-70.
11. Botirov, F.B., Gafurov, S.R., Gafurov, A.A. (2021). Identification of key persons in the information security incident management process and distribution of roles between them. *Chemical Technology, Control and Management*, 2021(3), 72-77.
12. Abdukhalil, G., Sherzod, S. (2020). Principles of Adaptation in Protecting Corporate Systems. *2020 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, 1-4, doi: 10.1109/ICISCT50599.2020.9351461.
13. Sayfullaev, S. (2020). Analysis of information security methods in biosystems and application of intelligent tools in information security systems. *Chemical Technology, Control and Management*, 2020(3), 72-77.