Lecture-15. Law enforcement activities in the investigation of crimes in the field of information security

Purpose of the Lecture

The purpose of this lecture is to provide students with a comprehensive understanding of law enforcement procedures, methods, and principles in investigating crimes related to information security. The lecture aims to develop knowledge about the legal framework, roles of investigative bodies, and stages of criminal investigation in the digital sphere, as well as the technical and procedural aspects of collecting and analyzing digital evidence.

As noted earlier, despite the fact that not every incident entails prosecution, in order to bring the perpetrator to the appropriate type of responsibility, it is necessary not only to have an offense/crime/misdemeanor in his actions, but also to prove these circumstances. These requirements are most fully implemented when bringing to administrative, and even more so - criminal liability. It should be noted that, as a rule, crimes/offenses in the sphere of information security are quite latent in nature - i.e. as a rule, in the absence of statements by the injured party due to possible image risks for it (banks and financial organizations - especially), distrust in the work of law enforcement agencies, the presence of their own shortcomings and offenses in the field of information security and the threat of their detection during the investigation, etc. . - it is these reasons that make even the self-identified fact of a crime unknown to law enforcement agencies, during which no investigation takes place, nor the perpetrators are held accountable - which means that the possibility of repeating such or more serious actions on the part of the perpetrators as in relation to the already injured party , and in relation to other potential victims - to become extremely high. That is why the very fact of detecting a crime in the field of information security without investigating it and bringing it to justice in itself only partially affects the prevention of such crimes and preventing their recurrence - i.e. the principle of the inevitability of punishment for what has been done is not fully implemented.

The state legislatively establishes a special procedure for investigating such crimes, which is based on a set of actions of law enforcement agencies to collect, seize, investigate and evaluate evidence. At the same time, the process itself is divided into pre-trial investigation and trial. Failure to comply with the established procedure and requirements for such investigations may result in the impossibility of bringing the guilty person to justice in accordance with the procedure established by law - due to lack of evidence, due to violations of the investigation, etc.

Evidence in a criminal case is legally obtained factual data, on the basis of which, in the manner prescribed by law, law enforcement agencies and / or the court establish the presence or absence of an act provided for by the Criminal Code of the Republic of Kazakhstan, the commission or non-commission of this act by a suspect, accused or defendant, his guilt or innocence , as well as other circumstances that are important for the correct resolution of the case. Such factual data, which are important for the correct resolution of a criminal case, are established: by the testimony of the suspect, the accused, the victim, the witness, the witness entitled to defense, the expert, the specialist; conclusion of an expert, specialist; material evidence; protocols of procedural actions and other documents.

As already noted, the process of proving itself consists in collecting, examining, evaluating and using evidence in order to establish circumstances that are important for the legal, reasonable and fair resolution of the case. The duty to prove the existence of grounds for criminal liability and the guilt of the suspect lies with the law enforcement agencies.

The collection of evidence is carried out both in the process of pre-trial investigation and trial through the production of procedural actions (including the so-called investigative actions). The collection of evidence, in turn, includes a sequence in their discovery, consolidation and withdrawal. The collection of evidence is carried out subject to a number of conditions, procedural and forensic.

When collecting evidence, unconditional compliance with the requirements of legality is necessary:

- collection of evidence only in the ways prescribed by law;
- the use of legal methods of collecting evidence only within the framework of their procedural procedure, which is established by law;
- collection of evidence only by a person authorized by law;
- objectivity, impartiality in collecting evidence;

As already mentioned, the methods of collecting evidence are those procedural actions by which evidence is discovered, recorded, seized and stored. But the methods of collecting evidence provided for by law must be applied in strict accordance with the norms of criminal procedure law that regulate them.

Of course, the law provides only general rules for using one or another method of collecting evidence and cannot regulate numerous technical means and tactics for conducting investigative actions aimed at increasing their efficiency and ensuring the completeness of collecting evidence. An indispensable requirement is made to these technical means and tactics: they must not contradict the law, comply with the principles of legislation.

The collection of evidence involves ensuring the completeness of the evidence collected in the case. All procedural actions to collect evidence must be carried out with high quality, carefully, none of the evidence essential to the case should be out of sight of the subjects of proof.

It is important to note the timeliness of actions to collect evidence, the correct choice of the moment for conducting one or another investigative action to collect evidence. If this investigative action is urgent in nature, then it should be carried out immediately, as soon as it becomes necessary, if the moment of such an action is determined by some tactical considerations, then this should also be taken into account by the investigator or the court.

According to Davtyan G.E., the necessary guarantees of the reliability of information about the received factual data must be observed. This condition is provided:

- firstly, the choice of reliable sources of evidence,
- secondly, compliance with those tactical conditions and methods of conducting investigative actions that create the prerequisites for obtaining reliable results
- thirdly, the use of such technical means that allow you to fully identify, accurately record and securely store evidence.

In the analysis of this condition, the important role of forensics is especially noticeable. The subject of this science includes the development of such technical means and tactics for collecting evidence, which are designed to ensure the reliability of the data obtained. The totality of such means, techniques and approaches within the framework of homogeneous types of crimes forms the so-called. forensic methodology for investigating these types of crimes, which is based on the forensic characteristics of this type of crime. In its most general form, the forensic characterization of a crime is a systematized information about the forensically significant signs of crimes of a certain type, reflecting their relationship and contributing to the investigation and proof of crimes of this type. Ta

As Davtyan G.E. - discovery of evidence - this is their search, identification, paying attention to certain factual data that can acquire evidentiary value, this is the initial and necessary stage of their collection, because you can collect only what is found, discovered, became known to the

subject of proof . Indeed, at the stage of collecting evidence, law enforcement agencies actually deal not with evidence, but with factual data, which (according to their assumption) can only become evidence, i.e. with traces of the event that do not yet have the procedural status of evidence. Moreover, in the process of discovery, the search for such data/information can involve almost anyone - information both in oral and written form or in the form of an electronic document, as well as objects and documents for attaching them practically any participants and not only participants in the process - the suspect, the accused, the defender, the victim, etc., as well as any citizens and organizations, have the right to provide evidence in a criminal case. In relation to the field of information security, the detected evidence can be logs of actions in the IS, individual components and EIR software, their material carriers and means of processing and transmission, etc.

Evidence discovered and collected needs to be consolidated for further use – i.e. fix.

In the scientific literature, the following forms of fixing evidentiary information are distinguished:

- verbal (verbal);
- graphic;
- subject;
- visual-figurative.
- combined.

In this case, the main methods of fixation are measurement, description and modeling. The technical methods for implementing these methods are:

- in the verbal form of fixation - logging, audio recording;
- with a graphic form of fixation - a graphic display (schematic and scale plans, drawings, drawings);
- in the subject form of fixation - the removal of the object, its preservation, the production of derivative evidence - copying, etc.;
- with a visually figurative form - photo-video shooting.

It is allowed to combine methods of fixation techniques, their complex application. The use of any form of fixation, the application of its methods and techniques, since we are talking about the process of proof, are subject to certain legislative and procedural requirements.

In criminal procedure science, there are three forms of fixing evidence: drawing up protocols, attaching material (material) evidence to the case, attaching other documents (including electronic ones) to the case.

Factual data can be used as evidence only after they are recorded in the protocols of procedural actions. The participants in investigative and judicial actions, as well as the parties to the proceedings, should be provided with the right to get acquainted with the protocols, which record the course and results of these actions, to make additions and corrections to the protocols, to express comments and objections regarding the procedure and conditions for carrying out this action, to propose his version of the entry in the protocol, draw the attention of the investigator, investigator, prosecutor or court to circumstances that may be relevant to the case. To consolidate evidence, along with the preparation of protocols, sound, video recording, filming, photography, making casts, impressions, plans, diagrams and other ways of capturing information can be used.

Discovered and recorded evidence for the purpose of their further use, research, evaluation and inclusion in the case file, as well as their safety, as a rule, are subject to seizure. In those cases when it comes to material evidence, the seizure of which in kind for some reason is inappropriate or impossible, some special forms and methods of fixing evidence act as means of seizure. Those. in this case, the evidence is not withdrawn, but its evidentiary properties are withdrawn, transferred, transferred to the new object, and the new object itself, as the carrier of these

properties, is a derivative material evidence. For example, in the field of information security, this is usually copying information to other media. If it is impossible to seize objects of probative value for various reasons (significant weight, large size, suspension of the KVOIKI, etc.), special measures are taken at the place of their discovery to preserve them (detailed description, photographing, etc.), or there is a detailing of the stage of fixation - examination of evidence with the involvement of a specialist, forensic examination of these objects on the spot, etc. - we will dwell on this a little lower.

The evidence collected in the case is subject to a comprehensive and objective examination. The study includes the analysis of the received evidence, its comparison with other evidence, the collection of additional evidence for their verification, verification of the sources of evidence.

Each evidence is subject to assessment in terms of relevance, admissibility, reliability, and all collected evidence in the aggregate - sufficiency for resolving a criminal case.

A judge, a prosecutor, an investigator, an inquirer evaluate the evidence according to their inner conviction, based on a comprehensive, complete and objective consideration of the evidence in their totality, guided by law and conscience.

Evidence is recognized as relevant if it is factual evidence that confirms, refutes or casts doubt on the conclusions about the existence of circumstances relevant to the case. Evidence is considered admissible if it is obtained in the manner prescribed by law. Evidence is recognized as reliable if, as a result of verification, it turns out that it corresponds to reality. The totality of evidence is recognized as sufficient to resolve a criminal case if admissible and reliable evidence related to the case is collected, without any doubt and undeniably establishing the truth about each and every one of the circumstances to be proved.

Obviously, due to the specifics in the field of information security crimes, one cannot do without special knowledge and the use of scientific and technical means in the process of proving. Scientific and technical means in the process of proving in a criminal case can be used by the body conducting the criminal process, as well as by an expert and a specialist in the performance of their procedural duties provided for by law.

The use of scientific and technical means is recognized as admissible if they:

1) are directly provided for by law or do not contradict its norms and principles;
2) scientifically sound;
3) ensure the efficiency of criminal proceedings;
4) safe.

The use of scientific and technical means by the body conducting the criminal process is recorded in the minutes of the relevant procedural actions and the minutes of the court session, indicating the data of scientific and technical means, the conditions and procedure for their use, the objects to which these means were applied, and the results of their use.

To assist in the use of scientific and technical means, the body conducting the criminal procedure may involve a specialist. Cases of mandatory participation of a specialist in investigative and judicial actions are directly provided for by the Code of Criminal Procedure. As part of an investigative or judicial action, a specialist has the right to conduct a study that does not lead to the complete or partial destruction of objects or a change in their appearance or basic properties, with the exception of comparative, case materials with a reflection of its progress and results in the protocol of the ongoing investigative or judicial action or in an official document attached to the protocol of the investigative action. In contrast to the examination of a specialist carried out as part of a specific investigative action, an examination as an independent action is assigned in cases where evidence relevant to a criminal case can only be obtained as a result of an expert examination of the materials of a criminal case based on special scientific knowledge. In addition, after the necessary research has been carried out, the expert, on his own behalf, draws up a written opinion,

in which he reflects the evidence obtained in the course of the expert study. The expert opinion is an independent source of evidence in a criminal case.

In the most general form, in a criminal case, the following must be proved:

1) an event and the elements of a criminal offense provided for by the criminal law (time, place, method and other circumstances of its commission);
2) who has committed an act prohibited by criminal law;
3) the guilt of a person in committing an act prohibited by criminal law, the form of his guilt, the motives for the committed act, legal and factual errors;
4) circumstances affecting the degree and nature of responsibility, the suspect, the accused;
5) circumstances characterizing the identity of the suspect, the accused;
6) the consequences of the committed criminal offense;
7) the nature and extent of the damage caused by the criminal offence;
8) circumstances excluding the criminal wrongfulness of the act;
9) circumstances entailing release from criminal liability and punishment.

With regard to crimes in the field of information security, the following circumstances are subject to establishment in accordance with the forensic methodology for investigating these types of crimes:

- facts of illegal access to IS, EIR, etc.;
- individuals or legal entities (owners of IP, EIR, etc.) who have suffered from a crime;
- the place of the crime (on the territory of the location of the APK IS, EIR, etc.);
- the time of the commission of the crime, as well as the time of occurrence of harmful consequences;
- instruments of crime, i.e. devices and tools, as well as software that were used by the criminal;
- establishing the fact of EIR IS security, etc. and information in them.
- the method of committing the crime (UAS, distribution of malware, etc.);
- the harmful consequences of the crime, their assessment by the owner/owner of IP, EIR, the nature and extent of the harm, the onset of grave consequences;
- the subject of the crime, whether he has access to IS, EIR, communication networks, the presence of a criminal group, the distribution of roles between its participants;
- the guilt of each subject of the crime, the form of guilt, the motive of criminal activity;
- circumstances characterizing the personality of each subject;
- circumstances excluding criminality and punishability of the act (extreme necessity, coercion, etc.);
- circumstances mitigating and aggravating punishment;
- circumstances that may entail exemption from criminal liability and punishment (reconciliation, active repentance, etc.);
- the causes and conditions that contributed to the commission of the crime.

Accordingly, since the above facts are subject to proof, then the search for the discovery of evidence is focused on proving precisely these circumstances. However, they are interconnected and often follow from each other. For example, in case of UA to prove the crime scene, the search for evidence depends on the method - physical UA at the level of connection to the router, software via a server with access to the network, etc. – i.e. depending on the method, the entry point will also differ geographically - NSD into the network - i.e. and the scene of the crime will differ, respectively, the proof will be reduced to the discovery of traces (magazines, additional cables, etc.) in this very place, which, after investigation, in turn, will prove both the place of the UA and the method of UA.

Speaking of traces, it should be noted that the ways of committing crimes in the field of information security are directly related to certain operations and commands aimed at processing information in IS, EIR, etc. However, many crime-related operations can be carried out regardless of the actual location of the perpetrator - i.e. remotely, be single or recur periodically. At the same time, rather traditional traces (fingerprints, etc.), although they may be present, usually have only a secondary significance. The most important traces of cybersecurity crimes are usually information or part of it on electronic media. This can be special software (not always malicious) or part of it, a set of interrelated non-standard commands for IP, saved logins and passwords, action logs, etc.

As we have already noted, cybersecurity crimes, especially if they have not caused major damage, can go unnoticed for quite a long time.

An important element of the forensic characteristics of computer crimes is the identity of the offender. In the scientific literature there is a statement that the majority of persons who have committed crimes in this area are:

- -computer users with certain training and access to a computer network;
- -operators, system programmers, persons performing maintenance and repair of computer networks or systems;
- administrative and managerial personnel (including top and middle managers, accountants, economists, etc.).

At the same time, in the field of crimes in information security, the predominant role as subjects of crimes is played by people with specialized or not education and work experience, and the more difficult the method, the higher the qualifications of such people, which means the narrower the circle of suspects, whose age is usually lies in the interval - 16-40 years.

The following factors contribute to the commission of crimes in the field of information security:

- the presence of a large number of geographically separated points for receiving and transmitting information, and the exchange between them is usually carried out automatically;
- the presence in the IS of application software with inadequate quality in relation to information security;
- the possibility of unauthorized access or modification of information;
- high concentration of information of various nature in common databases in one system, lack of redundancy and reconciliation mechanisms;
- lack of proper control over access to information and IP;
- negligence or negligence of users and administrators, non-observance of precautionary measures;
- constant increase in the volume of information in IS and databases;
- a wide range of users who have access to information and IP in general.
- - and etc.

The most common motives for committing such crimes are:

1) selfish considerations - 66%;
2) political goals - 17%;
3) research interest - 7%;
4) hooligan motives and mischief - 5%;
5) revenge - 5%.

At the same time, as a rule, 52% of crimes are related to the theft of funds; 16% - with the destruction and destruction of computer equipment; 12% - with the substitution of the original data; 10% - with theft of information and programs and 10% - with theft of services.

As a rule, the beginning of the investigation depends on how the crime was detected - based on the statement of the owner of the IP, EIR, while there is information about the person involved:

- the same as above, but there is no information about involvement
- there are no statements by the victims, but there are publications in the media or statements by third parties, etc.
- As a result of operational-search activities, law enforcement agencies independently revealed the fact of a crime.

In all the above cases, the investigation process and its initial tasks usually come down to establishing information that makes it possible to judge the method of committing a crime; the procedure for regulating a particular IS, EIR, etc. by its owner; circle of persons working with IS, EIR and having access to it, etc. To establish this, such initial investigative actions are most often carried out as: interrogations of owners and owners of IP data and witnesses; inspection of APK IS; seizure and inspection of the necessary documentation, etc. At the same time, as noted earlier, inspections and seizures should be carried out with the participation of specialists in the field of IT or even information security. Such actions usually allow the identification of other necessary witnesses who need to be questioned; determine the circle of persons involved in this act, as well as the approximate amount of damage caused to the owner of the IP, EIR, etc. Further investigative actions are related to the seizure of the agro-industrial complex or its parts, devices, their inspection and, if necessary, expert research, interrogation of new witnesses, etc.

Within the framework of this lecture, we will not be able to fully cover all the regulated sequences of actions and features at each stage of the investigation, and even more so the subsequent trial due to their narrow legal specificity. Employees of IT departments and information security, as a rule, participate in the investigation at the initial stage, less often - in the production of examinations and giving opinions, even more rarely - directly give explanations in court. But in any case, it is the initial stage - the reaction to the incident, the investigation of crimes and bringing the perpetrators to justice - i.e. those legal aspects that are established in the state in relation to this are a necessary component of the existence of information security as an independent industry and field of activity not only in the Republic of Kazakhstan, but also in the world.

Control Questions

1. What are the main roles of law enforcement agencies in the field of information security?
2. Which national and international laws regulate the investigation of cybercrimes?
3. What are the main stages of investigating crimes in the digital sphere?
4. What methods and tools are used in digital forensics?
5. What challenges do law enforcement agencies face in cybercrime investigations?
6. How is international cooperation organized in the fight against cybercrime?
7. What principles should guide law enforcement activities in information security?

Recommended Literature

1. Criminal Code of the Republic of Kazakhstan (2014, with amendments).
2. Law “On Informatization” (2015).
3. Law “On Personal Data and Their Protection” (2013).

4. Budapest Convention on Cybercrime (Council of Europe, 2001).
5. NIST SP 800-86. *Guide to Integrating Forensic Techniques into Incident Response.*
6. Casey, E. (2020). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.
7. Ciardhuáin, S. Ó. (2004). *An Extended Model of Cybercrime Investigation Process.* International Journal of Digital Evidence.
8. Interpol (2023). *Cybercrime Directorate Reports and Best Practices.*