KHAZAR UNIVERSITY

Faculty: Graduate School, Arts and Science

Department: Physics and electronics

Qualification: Electronic devices and appliances

MASTER THESIS

SECURITY AND PRIVACY IN INFORMATION PROCESSING

Student: __________________ Rahim Rahimli Shirzad

Supervisor: __________________ assos. of professor, PhD in Technical Sciences Elchin Hasanov

Baku - 2025

XƏZƏR UNİVERSİTETİ

Fakultə: Təbiət elmləri, Sənət və Texnologiya yüksək təhsil

Departament: Fizika və Elektronika

İxtisas: Elektron cihazlar və qurğular

MAGİSTR DİSSERTASİYA İŞİ

İNFORMASİYA EMALINDA TƏHLÜKƏSİZLİK VƏ MƏXFİLİK

İddiaçı: ___________________ Rəhim Rəhimli Şirzad oğlu

Elmi rəhbər: ___________________ Texniki elmlər üzrə fəlsəfə doktoru, dosent

Elçin Həsənov Qafar oğlu

Bakı – 2025

TABLE OF CONTENTS

INTRODUCTION

Relevance of the topic and degree of development is security and confidentiality of information during its processing is a very relevant and important topic, especially in the modern world, where information is a key resource. The relevance is due to the growing volume of information, its importance for various areas of activity, as well as the increasing number of threats and abuses in the digital space.

The transfer of most information archives, funds and communications into electronic form has created an independent type of asset – information. Like any value, it is subject to attacks by various fraudsters. Significant risks also arise in the area of ensuring state security in the sphere of information; the main threats are named in the Doctrine of State Information Security. Ignoring emerging problems leads to a loss of competitiveness both at the state and corporate levels. Citizens also suffer from crimes committed in the information sphere.

Object and subject of the research:

The object of research is what the researcher's attention is directed at. In the context of security and confidentiality in information processing, the object of research can be:

Information:

This is data in any format (text, numbers, audio, video, etc.) stored or transmitted in an information system.

The concept of ensuring information security identifies the following areas of protection:

economic sphere, including monetary and credit and the securities market. ...

▼ foreign policy

▼ domestic policy

▼ education, science, technology.

▼ spiritual.

▼ judicial and law enforcement.

Research goals and objectives:

Information security (IS) is a key aspect of data and system protection in the digital age. The main goal is to ensure confidentiality, integrity and availability of information. The procedure includes protection against unauthorized access, changes, leaks and destruction of data.

The use of information security systems sets specific tasks for preserving key characteristics of information and ensures:

▼ data confidentiality – access is only available to persons authorized to do so;

▼ availability of information systems with the data contained therein to specific users who have the right to access such information;

▼ data integrity implies blocking unauthorized changes to information;

▼ authenticity – completeness and general accuracy of information;

▼ non-repudiation – the ability to determine the source or authorship of information.

Research hypothesis:

Research hypotheses in the field of security and privacy in information processing may vary and depend on the specific area of study. For example, it can be assumed that the use of modern data encryption methods (e.g., AES or RSA) effectively reduces the risk of confidential data leakage during their transmission over the network. Another hypothesis may be that the implementation of multi-factor authentication (e.g., the use of biometric data and one-time passwords) significantly increases the security of the system and reduces the likelihood of unauthorized access to data. Yet another hypothesis may be related to the influence of information culture on security in an organization. The assumption is that raising the level of awareness of employees about cybersecurity and training them in security rules reduces the likelihood of making mistakes that lead to data leaks.

Research methods

Cryptographic methods, access control and authentication mechanisms are used to ensure data confidentiality. Data integrity is also an important principle.

To ensure complete confidentiality in an information system, four methods are used, which are relevant for any information format:

♦ restricting or completely blocking access to information;

♦ encryption;

♦ splitting into parts and disparate storage;

♦ concealing the very fact of the existence of information.

Scientific innovation of the research

The significance of the work for the science of information law is that for the first time, taking into account the documents of strategic planning adopted in recent years in the field of development of the information society:

▼ taking into account the innovations in the formation of the legislative base regulating the development of the institute of personal data in Russia, a comprehensive study of the legal regulation of relations on ensuring the security of personal data processing on the Internet, their legal nature and the status of subjects was conducted;

▼ a new classification of personal data was developed, taking into account their circulation in the information and telecommunications network Internet;

▼ proposals were formulated to improve the legislation regulating the security of personal data processing on the Internet.

Confidentiality and protection of personal data in our modern globalized world is an extremely important aspect in all areas; in economics, in the military industry, in science, of course, in the field of ICT.

Protection of personal data is a set of measures of a technical, organizational and organizational-technical nature aimed at protecting information relating to a specific individual (subject of personal data) or determined on the basis of such information.

Confidentiality of personal data is a mandatory requirement for the designated responsible person who has access to personal data to not allow their distribution without the consent of the subject or other legal basis.

Rapid advancements in information technologies have led to an exponential increase in the volume of data being processed daily. This data often includes sensitive personal information, financial records, medical data, and confidential communications, all of which require secure processing and transmission mechanisms. Therefore, ensuring the security and privacy of such information has emerged as a fundamental concern across multiple disciplines — including computer science, telecommunications, law, and public policy.

At the same time, it is important to note that the digital transformation of society has brought both opportunities and challenges in terms of privacy. While technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) have increased efficiency and connectivity, they have also created new vectors for cyberattacks, data leaks, and mass surveillance. Malicious actors are constantly inventing new methods to exploit vulnerabilities in information systems, which requires robust, proactive security measures. (Davis D., Barber D., Price W., Solomonides S. 1982)

Specific information related to topic

This thesis explores the fundamental aspects of information security and privacy in data processing environments. It delves into the legal, organizational, and technological frameworks that govern data protection, while also addressing the threats posed by cybercrime and the strategies used to counteract them. A particular focus is given to the mechanisms for securing personal data, such as cryptographic techniques, data anonymization, and access control policies.

The objectives of this study are to:

· Analyze the principles of personal data confidentiality and legal regulations in Azerbaijan and other jurisdictions;

· Examine the technical methods for secure data storage, transfer, and destruction;

· Investigate cryptographic solutions that ensure data integrity and confidentiality;

· Explore the rights of individuals as data subjects and how these rights are protected by law;

· Propose practical recommendations for improving security practices within organizations handling sensitive information.

In this context, the study employs a multi-method approach, combining legal analysis, technical review, and policy evaluation. By examining real-world cases of data breaches and successful security implementations, the research aims to offer insights that can be applied in both theoretical and practical domains. (Anshina M.J. Tsymbal A.A. 2003.)

CHAPTER I. LITERATURE REVIEW

OBJECTIVES AND SCOPE OF APPLICATION

These Principles of Confidentiality and Personal Data Protection (“Principles”) govern the manner in which its business partners and Group companies (hereinafter referred to as the “Company” or “Data Operator”) protect personal data and determine the principles for processing personal data of applicants for positions in the company , visitors, customers, prospects, suppliers, third parties, online visitors (“Groups of Persons”) and notices to these groups of persons.

PRINCIPLES FOR PROCESSING PERSONAL DATA

As a Data Controller, the Company processes your personal data in accordance with the following principles.

◦ Processing in accordance with legal requirements and principles of good faith

When processing your personal data, we act in accordance with the principles established by law and generally accepted standards of good faith.

◦ Ensuring the accuracy and, if necessary, relevance of personal data

Taking into account your legitimate interests, we carry out periodic checks and updates to ensure that the data we process is accurate and up-to-date and to take appropriate action. In this regard, the Company has created systems aimed at monitoring the accuracy of personal data and making the necessary corrections.

◦ Processing data for specific, explicit and legitimate purposes

Your personal data is processed for explicit, specific and legitimate purposes.

◦ Relatedness to the purpose of processing and proportionality (Beketov N.V 2003)

We process your personal data only to achieve the intended purpose(s) and to a limited extent, and personal data that is not relevant to the purpose will not be processed.

◦ Storage for the period required by law or necessary for processing

Your personal data will only be stored for the period required by applicable law or necessary for processing.

We first check whether or not the applicable laws provide for a certain period of time, and then, depending on the results of the check, we comply with the specified period or store the data for the period necessary for the purpose of data processing.

When the established period expires or the reasons for processing personal data disappear, then in the absence of legal reasons to extend the period for processing personal data, such data is deleted, destroyed or anonymized in accordance with the Company's Personal Data Storage and Destruction Policy. (Black Yu. 1990)

1.1. Principles of confidentiality and protection of personal data

As a Data Controller, the Company processes your personal data in accordance with the following principles.

♦ Processing in accordance with legal requirements and principles of good faith

When processing your personal data, we act in accordance with the principles established by law and generally accepted standards of good faith.

♦ Ensuring the accuracy and, where necessary, relevance of personal data

Taking into account your legitimate interests, we carry out periodic checks and updates to ensure that the data we process is accurate and up-to-date and to take appropriate action. In this regard, the Company has created systems aimed at monitoring the accuracy of personal data and making the necessary corrections.

♦ Processing of data for specific, explicit and legitimate purposes

Your personal data is processed for explicit, specific and legitimate purposes.

♦ Relatedness to the purpose of processing and proportionality

We process your personal data only to achieve the intended purpose(s) and to a limited extent, and personal data that is not relevant to the purpose will not be processed.

Storage for the period required by law or necessary for processing

Your personal data will only be stored for the period required by applicable law or necessary for processing.

We first check whether or not the applicable laws provide for a certain period of time, and then, depending on the results of the check, we comply with the specified period or store the data for the period necessary for the purpose of data processing.

When the established period expires or the reasons for processing personal data disappear, then in the absence of legal reasons to extend the period for processing personal data, such data is deleted, destroyed or anonymized in accordance with the Company’s Personal Data Storage and Destruction Policy. (Broydo B.J.I 2002.)

1.2. Conditions for processing personal data

Personal data is processed by the Company under the following conditions.

♦ Direct legal requirement

Your personal data is processed in cases where processing is expressly required by law.

Actual impossibility of obtaining the express consent of the person concerned

Your personal data may be processed when it is necessary to process personal data to protect the life or health of the person concerned or another person, if such persons are unable to give their explicit consent due to actual impossibility or their consent may be invalid.

♦ Directly related to the conclusion or fulfillment of the terms of the contract

Personal data may be processed as part of the necessary processing of personal data of the parties to the contract if it is directly related to the conclusion or fulfillment of the terms of the contract.

Fulfillment by the Company of legal obligations

Personal data may be processed if processing is a necessary condition for fulfilling the Company's legal obligations as a data controller.

♦ Public personal data

Personal data can be processed if it is in the public domain.

- Data processing is necessary for the establishment, exercise or defense of rights

Personal data may be processed in cases where data processing is necessary for the establishment, exercise or defense of a right.

♦ Data processing based on legitimate interests

Personal data may be processed if it is required to protect the legitimate interests of the Company.

- Data processing based on express consent

Where your personal data cannot be processed on the basis of any of the conditions set out in these Principles, it will be processed on the basis of express consent. (Davis D., Barber D., Price W., Solomonides S. 1982)

1.3. Methods and legal basis for collecting personal data

Personal data of groups of persons transmitted to the Company electronically is processed as indicated below.

- CLIENT

The client's personal data is processed automatically, through written or oral means of data transmission, as part of a system for recording data received directly from the client or a third party, in physical and electronic form, on the basis of the legal grounds set out in the relevant documents, providing for "the need to process personal data of the parties to the contract, provided that this is directly related to the conclusion or execution of the contract", "if this is necessary for the data operator to fulfill its legal obligations", "if data processing is necessary to protect the legitimate interests of the data operator, when provided that this does not prejudice the fundamental rights and freedoms of the person concerned."

- APPLICANT FOR A POSITION IN THE COMPANY

In the context of the likely conclusion of an employment contract, provided for in Article 5 of Law No. 6698, the personal data of an applicant for a position is processed automatically if such personal data is obtained directly from that person or from a third party within the framework of a data registration system, by filling out a questionnaire in electronic or paper format, based on the legal grounds provided for by the provisions that "it is necessary to process the personal data of the parties to the contract, provided that this is directly related to the conclusion or performance of the contract", "if this is necessary for the data operator to fulfill its legal obligations", "if the processing of data is necessary to protect the legitimate interests of the data controller, provided that this does not prejudice the fundamental rights and freedoms of the person concerned." (D. B. Baker, 2006)

-POTENTIAL CLIENT

Personal data of a potential Client is processed automatically, through written or oral means of data transmission, as part of a system for recording data received directly from a potential Client or a third party, in physical and electronic form, on the basis of legal grounds set out in legal articles and providing that “personal the data must be disclosed to the public directly by the person concerned”, “data processing is mandatory for the establishment, exercise or protection of rights”, “data processing is necessary to protect the legitimate interests of the data operator, provided that this does not prejudice the fundamental rights and freedoms of the person concerned persons”, “if this is necessary for the data operator to comply with its legal obligations”.

- VISITOR

Visitor personal data is automatically processed by recording on CCTV cameras at the entrances to the building, at the external facades of the building, conference rooms and event venues, in canteens, cafeterias, waiting areas, parking lots, elevators, corridors, floors and areas service, guided by the legal grounds provided by law, which state that “where it is necessary for the data operator to comply with its legal obligations”, “data processing is necessary to protect the legitimate interests of the data controller, provided that this does not prejudice fundamental rights and freedoms interested person."

- - THIRD PERSON

Personal data of a third party is processed automatically, through written or oral means of data transmission, as part of a system for recording data received directly from that person or a third party, in physical or electronic form, based on the legal grounds provided for by regulations, if “data processing is necessary to protect the legitimate interests of the data controller, provided that this does not prejudice the fundamental rights and freedoms of the person concerned” and the conditions for the processing of personal data specified in the legal article are based on legitimate reasons.

- SUPPLIER / BUSINESS PARTNER / TENANT

The personal data of the supplier/business partner is processed automatically, through written or oral means of communication, as part of a system of recording data received directly from that person or a third party in physical and electronic form, based on the legal basis of “the need to process the personal data of the parties to the contract , provided that it is directly related to the conclusion or performance of a contract”, “if this is necessary for the data controller to fulfill its legal obligations”, “if the processing of data is necessary to protect the legitimate interests of the data controller, provided that this does not prejudice the fundamental rights and freedoms of the person concerned."

- ONLINE VISITOR

Personal data of the online visitor is processed automatically on the basis of the laws “On the regulation of publications on the Internet and the fight against crimes committed through such publications”, as well as the relevant article of the Law, “if data processing is necessary to protect the legitimate interests of the data operator, provided that that this does not prejudice the fundamental rights and freedoms of the person concerned”, “if this is necessary for the data operator to comply with its legal obligations”. (Simonsen.T. 2008)

CHAPTER II. METHODS AND METHODOLOGY

In today's information society, personal data has become a particularly valuable asset. Companies, governments, and ordinary citizens store and process enormous amounts of personal information. However, as the importance of personal data increases, so does the need to ensure its security. The theft or unauthorized access of such information can result in serious consequences, including financial loss, loss of customer confidence, and penalties for violating the law.

According to analytical centers of scientific associations, 38% of our citizens experienced a leak of personal data and its use by unscrupulous individuals for spam calls and advertising (see source). In this chapter, we will look at measures to ensure the security of personal data in an organization.

The following concepts are used in this Policy:

- Information - information (messages, data) regardless of the form of their presentation.

- Information system of personal data - a set of personal data contained in databases and information technologies and technical means that ensure their processing.

- Processing of personal data - any action (operation) or set of actions (operations) performed using automation tools or without the use of such tools with personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, changing), extraction , use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data.

- Operator - a state body, municipal body, legal or natural person, independently or jointly with other persons organizing and (or) carrying out the processing of personal data, as well as determining the purposes of processing personal data, the composition of personal data to be processed, actions (operations), performed with personal data.

- Personal data - any information relating directly or indirectly to a specific or identifiable individual (subject of personal data).

- Providing personal data - actions aimed at disclosing personal data to a certain person or a certain circle of persons.

- Dissemination of personal data - actions aimed at disclosing personal data to an indefinite number of persons.

- Destruction of personal data - actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and (or) as a result of which material media of personal data are destroyed. (Kaluts T.A., Sushchansky V.I. , 1985)

2.1. Storage and transfer of personal data

What information is considered personal data?

Personal data should be understood as any information that directly or indirectly relates to a specific or identifiable individual (subject of personal data).

In other words, a full name + phone number or state identifier (medical policy, passport) is enough to establish a person's identity.

All this applies to personal data, which the company, as the operator of this data processing, is obliged to protect from leaks and unauthorized access. An operator is any legal entity that carries out actions with this information: collects, systematizes, uses, stores, distributes, etc.

Properly organized storage of documents containing personal data is a guarantee that confidential information about employees, clients and the organization's activities in general will not fall into the hands of unauthorized persons. Responsibility for determining the rules, location and protection of information falls, according to the law, on the employer, but not everyone clearly understands what nuances need to be taken care of. Adding to the complexity are the constant additions and adjustments to regulations, which have to be monitored in order not to receive a fine or get caught in the middle of a scandal related to the dissemination of citizens' personal information.

- Target

Respect for the fundamental rights and freedoms of individuals whose personal data is processed is the basic principle of our personal data processing policy. Therefore, we conduct all our personal data processing activities in compliance with the principles of protection of privacy, confidentiality of correspondence, freedom of thought and religion, as well as the right to effective legal remedies. We take all administrative and technical protection measures in accordance with the law and modern technology to protect personal data in accordance with the nature of the data concerned.

This Policy describes how we process, store, transfer and delete personal data provided, within the framework of the principles set out in the Personal Data Protection Law (Personal Data Law), during our business or socially responsible activities and similar activities. (Kaluts TI.A., Sushchansky V.I. 1979)

- APPLICATION AREA

All personal data processed by the Company and relating to our clients, business relationships, business partners, employees, suppliers, potential clients and other third parties are included in the scope of this Policy.

This Policy applies to all personal data processing activities owned or operated by the Company and has been developed and drafted taking into account the Personal Data Protection Law and other applicable regulations, as well as international standards in this area.

Are there clear rules for storing personal data?

Many novice businessmen believe that in order to resolve issues related to transactions with personal data, there are clear instructions, using which it will be possible to formulate clear rules and bring activities in accordance with legal requirements. In practice, there is no single approach to solving the issue. This means that each manager independently (or delegating responsibilities to a deputy or head of the HR department):

- develops regulations for the storage of personal data;

- determines where they will be located;

- selects and approves the protection measures taken and access restrictions;

- appoints employees who will be responsible for monitoring transactions with personal information;

- chooses certain types of punishments for violations of the rules;

- signs internal orders

Important nuances related to the procedure for storing personal data

In order to guarantee the safety and secrecy of personal data, it is necessary:

- Clearly define the conditions for storing personal data on paper and in electronic form. We are talking not only about the location, but also about establishing access regimes there for different categories of employees.

- Select people who will be responsible for specific aspects related to the preservation of information.

- Conduct explanatory work with staff, explaining the importance of restrictions and rules for using personal data within the framework of professional activities, as well as giving clear instructions on how to act in a given situation.

- Consider security measures for safes, cabinets with locks, and also implement specialized software.

- If you are working with biometric data, then additionally consider mechanisms for controlling and limiting access in accordance with the Government Decree.

When resolving the issue of storing personal information, it is necessary to understand that this is not a one-time job, but a continuous effort aimed at maintaining information security. Every year new threats and requirements appear that must be met in order, firstly, not to pay huge fines, and secondly, in order not to be worse than competitors and to count on the trust of clients and partners. (Kleinrock P 1979)

Cross-border transfer of personal data is the transfer of personal data to the territory of a foreign state to an authority of a foreign state, a foreign individual or a foreign legal entity.

When to use cross-border transfer

In practice, cross-border transfer occurs in the following cases:

- sending documents containing personal data by email to a person located outside of Azerbaijan, for example a foreign partner;

- booking rooms for employees when sending them on business trips abroad;

- use of foreign mailing services, platforms for storing personal data;

- other situations when it is necessary to transfer personal data outside Azerbaijan.

How is cross-border transfer carried out?

Before starting the transfer of data outside Azerbaijan, the operator is required to obtain a number of information specified in the Law on Personal Data from the authorities of a foreign state, foreign individuals or legal entities to whom the transfer is planned:

- information on measures taken by authorities of a foreign state, foreign individuals, foreign legal entities to protect transmitted data and the conditions for terminating their processing;

- information on legal regulation in the field of personal data of a foreign state (in case of transfer to countries that are not party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and not included in the list of foreign states that provide adequate protection of the rights of personal data subjects) ;

- information about the authorities of a foreign state, foreign individuals, foreign legal entities to which the transfer of data is planned;

In what cases will State supervision prohibit the transfer

The agency may prohibit or restrict the provision of information to other countries. The criteria by which the supervisory authority may prohibit or restrict such transfer are approved by the Government; of Azerbayan

The transfer will be prohibited if:

- the country, foreign individuals or organizations to which the operator wants to send information do not protect this information, and the conditions for terminating their processing are not defined;

the court banned the activities of a foreign legal entity in Azerbaijan and this decision came into force;

- a foreign organization was included in the list of undesirables in Azerbaijan;

- cross-border transfer and further processing of data do not meet the purposes of their collection;

- the data that is planned to be sent cannot be processed.

Can

Transfer personal data to the territory of the foreign states specified in the notification that are parties to the Council of Europe Convention or are included in the List of foreign states that provide adequate protection of the rights of personal data subjects.

It is forbidden

Transfer personal data to the territory of the foreign states specified in the notification that are not parties to the said Convention of the Council of Europe and are not included in the mentioned List. Exception: when such transfer is necessary to protect life, health, or other vital interests.

In addition, you should know the following

The transfer of personal data to the territory of such foreign states is prohibited by law, except in cases where:

♦ the consent of the subject of personal data is given, provided that the subject of personal data is informed of the risks arising from the lack of an adequate level of protection;

♦ personal data was obtained on the basis of an agreement concluded (to be concluded) with the subject of personal data in order to perform actions established by this agreement;

♦ processing of personal data is carried out within the framework of the implementation of international treaties of the Republic of Azerbaijan;

♦ such transfer is carried out by the financial monitoring body in order to take measures to prevent the laundering of proceeds from crime, the financing of terrorist activities and financing. (Коротченко А.В 2003)

2.2. Security of personal data

Privacy is the right of people to know and influence how and why their personal information is collected and processed. In addition, privacy laws apply almost everywhere we do business.

- Transparency: We inform customers about how we plan to use their data.

- Fair and Lawful Use: We use customer personal data only in accordance with applicable law and only in cases where we have legal grounds to do so.

- Purpose limitation: We use customer information only for specifically identified purposes and in no other way.

- Data minimization: We do not store any customer data for longer than necessary to provide the requested service or to pursue our legitimate interests. No copies of applicant data are made or stored, either digitally or physically.

- Privacy by Design: We ensure that our services and technologies are designed with our clients' privacy in mind.

- Data Accuracy: We strive to maintain appropriate data quality standards.

- People's rights: We respect people's right to privacy.

- Data Security: We maintain appropriate standards for the protection of personal data and delete it as soon as it is no longer needed, in accordance with personal data protection laws.

- Data transfer: If we need to transfer customer information to a third party, we ensure that such transfer is secure and complies with the law. For example, paper documents are sent only by reliable courier services.

Measures to ensure the security of personal data:

- Physical storage media are securely protected for the purpose of restricting access, and any electronic data is encrypted.

- Data is transmitted securely only in encrypted form and only through encrypted transmission channels.

- All data is deleted at the end of the order processing period. After expiration of the legally established periods, we delete all data.

Disaster recovery plan

The main goal of a disaster recovery plan is not only to ensure data recovery, but also to minimize the impact of a disaster on business processes and enable the company to quickly return to normal life after a natural disaster.

The disaster recovery plan determines which applications are most critical to the operation of the business. Recovery Time Objective (RTO) describes the target amount of time that a business application can be down. The recovery point objective (RPO) describes the age of the files that must be restored from the backup storage before normal operation can be resumed.

Roles and Responsibilities for Implementing the Disaster Recovery Plan

- List of potential risks to critical systems and confidential information

- Procedures for reporting disasters, escalating events, restoring critical operations and resuming normal operations

- Requirements for ensuring information security throughout the entire process

Inventory of backups and remote storages

- Contingency plans for different types of emergency situations

- Availability of planning documentation (Костыченко В 2008)

2.3. Rights of a personal data subject

First of all, let's note the main attributes of this topic.

Rights of personal data subjects

Let's list them:

The right to access your personal data. The right to demand clarification, blocking or destruction of personal data.

The right not to receive advertising and political promotion without prior consent.

The subject’s right to access his personal data includes a number of powers that correspond to the corresponding responsibilities of the operator.

Firstly, the right to receive information about the processing of his personal data by a specific operator in volume. Moreover, based on the literal content of the above norm, this right is not conditioned by any reasons.

That is, a citizen at any time can request information of interest to him, and the operator is obliged to provide information to the citizen or his representative within 10 working days from the date of application or receipt of the request, or within the same period to send the applicant a reasoned refusal with reference to a specific rule of law. This period may be extended by no more than 5 working days.

In this case, the operator must send a reasoned notification to the subject about the delay in response, indicating the reasons for extending the deadline for sending the requested information. (Корман А 1977)

The subject or his representative may contact the operator in person or by sending a written or electronic request. The written request must include the following information:

- number of the main document identifying the subject of personal data or his representative, information about the date of issue of the specified document and the issuing authority;

- information confirming the relationship with the operator (contract number, date of conclusion of the contract, conventional verbal designation and (or) other information), or information otherwise confirming the fact of processing of personal data by the operator;

- signature of the subject or his representative.

The right of the subject of personal data to access his personal data may be limited in accordance with federal laws, including if processing is carried out for the purposes of national defense, state security and law enforcement, that is, in the public interest, and also if such processing is carried out by bodies who detained the subject of personal data on suspicion of committing a crime, or brought charges against the subject of personal data in a criminal case, or applied a preventive measure to the subject before filing charges, with the exception of cases provided for by the criminal procedural legislation of Azerbaijan that allow the suspect or accused to become familiar with such personal data .

Secondly, the right to demand clarification of the personal data processed by the operator. This right arises for a person when the personal data at the disposal of the operator is incomplete, outdated or inaccurate.

We emphasize that in this case we are not talking about obtaining new ones, but about updating the operator’s existing data. The latter is obliged to make the required changes within a period not exceeding 7 working days from the date of receipt of a reasonable request from the subject about existing defects in the personal data being processed. In addition, the operator is obliged to notify the personal data carrier about the changes made or take reasonable measures to notify third parties to whom this data was transferred.

Thirdly, the right to block personal data. Blocking means temporary termination of the processing of personal data. If inaccurate personal data is identified when the subject or his representative contacts him or at their request or at the request of the supervisory committee, the operator is obliged to block personal data related to this subject or ensure their blocking (if the processing of personal data is carried out by another person acting on behalf of the operator) from the moment of such application or receipt of the specified request for the period of verification, if blocking of personal data does not violate the rights and legitimate interests of the subject of personal data or third parties.

Fourthly, the right to demand the destruction of personal data, which implies the commission of actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and (or) as a result of which the material media of personal data are destroyed. This right can be exercised in relation to information that was obtained by the operator illegally or is redundant in relation to the purposes of processing. The operator is obliged to destroy the relevant personal data within a period not exceeding 3 working days from the date of receipt of a reasoned request from the subject.

If it is impossible to ensure the legality of the processing of personal data, the operator, within a period not exceeding 10 working days from the date of detection of unlawful processing of personal data, is obliged to destroy such personal data or ensure its destruction.

If it is impossible to destroy personal data, then the operator blocks such information or ensures its blocking (if data processing is carried out by another person acting on behalf of the operator) and ensures its destruction within a period of no more than 6 months.

In addition, as in the case of clarifying personal data, the operator is obliged to notify the personal data carrier, government structure (depending on who made the corresponding request) about the actions taken or take reasonable measures to notify third parties to whom this data was transferred. (Кристолапов Т 1978)

In addition, it is important to note the following.

The subject of personal data has the right to receive information regarding the processing of his personal data, including containing:

1) confirmation of the fact of processing of personal data by the operator;

2) legal grounds and purposes of processing personal data;

3) the purposes and methods of processing personal data used by the operator;

4) name and location of the operator, information about persons (except for the operator’s employees) who have access to personal data or to whom personal data may be disclosed on the basis of an agreement with the operator or on the basis of state law;

5) the processed personal data related to the relevant subject of personal data, the source of their receipt, unless a different procedure for presenting such data is provided for by the relevant law;

6) terms of processing of personal data, including periods of their storage;

7) the procedure for the exercise by the subject of personal data of the rights provided for by this legal law;

8) information about completed or intended cross-border data transfer;

9) name or surname, first name, patronymic and address of the person processing personal data on behalf of the operator, if the processing has been or will be entrusted to such a person;

Next we will talk about access to classified information.

The right of the personal data subject to access his personal data may be limited in accordance with laws, including if:

1) the processing of personal data, including personal data obtained as a result of operational investigative, counterintelligence and intelligence activities, is carried out for the purposes of national defense, state security and law enforcement;

2) the processing of personal data is carried out by authorities that detained the subject of personal data on suspicion of committing a crime, or brought charges against the subject of personal data in a criminal case, or applied a preventive measure to the subject of personal data before bringing charges, with the exception of cases provided for by the criminal procedural legislation of Azerbaijan if the suspect or accused is allowed to become familiar with such personal data;

3) the processing of personal data is carried out in accordance with the legislation on combating the legalization (laundering) of proceeds from crime and the financing of terrorism;

4) the personal data subject’s access to his personal data violates the rights and legitimate interests of third parties;

5) the processing of personal data is carried out in cases provided for by the legislation of Azerbaijan on transport security, in order to ensure the sustainable and safe functioning of the transport complex, protect the interests of the individual, society and the state in the field of the transport complex from acts of illegal interference.

In addition, I would like to note the following important point, namely: these or those events for the development of the digital economy of Azerbaijan are aimed at making electronic services more accessible to citizens. At the same time, the scope of personal data circulation will expand, the number of operators who will process citizens' data will increase. But the fundamental approaches to data protection remain the same. The main thing is that all operators have legal grounds for such processing, and that confidentiality and security requirements are met, regardless of the emergence of new business models and processes inherent in the digital economy.

Typical violations are: failure by the operator to comply with the established requirements for processing personal data after achieving the purpose of processing; processing of personal data in cases not provided for by the Law "On Personal Data"; discrepancy between the content of the written consent of the subject of personal data for their processing and the requirements of the law; processing of excessive personal data in relation to the stated purposes.

And there is one common violation associated with failure to provide notification of the processing of personal data. The reasons for this can be different - incompetence of employees who considered that notification was not necessary in their situation. And some simply forget to provide notification. In short, the human factor is present here. (Кульманов M, 2000)

2.4. Legal measures to protect personal data

First, I noted a list of measures to protect personal data, namely:

- establishing restrictions on personnel access to personal information;

- selection of the person responsible for the security of personal data;

- preparation and approval of local documents;

- informing staff about the requirements for working with digital or paper personal data;

Leakage, unauthorized use, loss or illegal use of personal information of customers or partners can cause serious damage to the company's reputation and lead to the imposition of significant penalties for violation of legal requirements. Azerbaijani legislation obliges all operators to protect processed and stored personal data, so business must be adapted to the established requirements, not forgetting to monitor changes in regulatory documents. However, due to the large number of nuances (technical, organizational, legal), it can be difficult to achieve the desired result. Let's consider the most important aspects, knowledge of which will make taking measures to protect personal data as fast as possible, and the likelihood of hacking the system or gaining unauthorized access will be minimal.

Main requirements for measures to protect personal data in an organization

Characteristic of the current regulatory framework of Azerbaijan in the field of information security is the provision of the right to companies and entrepreneurs to independently decide how to prevent illegal actions with the personal data used. There are, of course, exceptions; for example, an organization must appoint an employee responsible for compliance with protective measures.

Otherwise, you can choose those means that:

- will be sufficient to prevent attackers or unauthorized employees from performing any actions with confidential information;

will allow you to effectively perform assigned work tasks;

- will comply with laws and other regulations governing the work of personal data operators;

- will take into account the features of the information system used.

There are technical and organizational, as well as legal measures to protect personal data.

The first includes methods and means that make it possible to make the process of obtaining, using and storing personal data safe, and the second is associated with documenting the rules for working with personal information.

In some cases, special requirements will need to be taken into account, in particular if the operator is subject to international regulations such as the GDPR. For those who do not often deal with information security issues, it is quite difficult to navigate the rules. It will be easier and faster to trust the professionals. By investing time and money in bringing your business into compliance with legal regulations, you are making a successful investment, since in the future you will not have to constantly modify anything, buy more or retrain staff. (А. А. Абдуманонов, М. К. Карабаев, 2013)

Even if all the work on building a personal data protection system will be carried out by outsourcers, the manager needs to be aware of the main provisions of the law on this issue. The necessary information is presented in the relevant law, in particular, it states that:

- the operator is obliged to prevent any risks associated with illegal transactions with personal data at all stages of processing;

- security threats must be clearly identified and measures (technical and organizational) taken to neutralize them;

it is necessary to develop a procedure for analyzing the compliance of the protection system with potential risks;

- all personal data carriers must be accounted for and protected from unauthorized physical and information influence;

- a clear plan of action is required in case of server hacking, hacker attack, corporate espionage, including methods and procedures for restoring lost or damaged information;

- any operation with personal data must be recorded, and the process of compliance with the security measures taken must be controlled by the employee responsible for this;

- it is necessary to strictly adhere to the rules established by the Government of Azerbaijan regarding personal data of different levels of security and requirements for material carriers of biometric information;

- the security system must be constantly modernized - if desired, operators can use additional tools and techniques, if this does not contradict the basic law regarding personal data.

From the point of view of the law, there is no difference between the measures to protect the personal data of employees, clients and suppliers - all categories are subject to uniform requirements regarding the personal data of individuals that must be observed. (Липунов Г. 2009)

Depending on the specifics of implementation, two groups of protective measures are distinguished: external and internal.

The first includes the development of a procedure for receiving and recording visitors to the organization, the introduction of a access system and technical means, as well as specialized software that allows you to protect digital data from unauthorized processing.

The second ones are related to the regulation of activities in the field of personal data within the organization and include:

- establishing restrictions on personnel access to personal information;

- selection of the person responsible for the security of personal data;

- preparation and approval of local documents;

- informing staff about the requirements for working with digital or paper personal data;

- planning the correct location of workplaces;

- creating lists of employees who may be in premises with PD carriers;

- establishing a procedure for destroying confidential information;

- integration of control mechanisms, prevention and counteraction to computer attacks.
(Липунов Г. 2009)

Features of technical protection of personal data

If previously the main efforts had to be made to limit physical access to media of confidential information, now technical measures to protect personal data are coming to the fore.

When working with large arrays of personal data, their development and integration should be carried out by professionals to ensure the achievement of the following goals:

- prevention of illegal use, dissemination and modification of information about citizens;

- eliminating the risk of leakage at all stages of processing, from receipt to storage and destruction;

- prevent secret data from becoming available to third parties without the consent of the owner.

There are the following groups of methods for protecting personal data:

Passive ones are the most expensive both in terms of financial investments and in terms of time. These include treatment with soundproof materials, installation of fences and other protective structures, installation of high-strength door and window systems, as well as the use of reinforced concrete structures to minimize the likelihood of burglary. Radical methods, despite their effectiveness, are mainly used partially, since there are not always the means and the technical ability to create the necessary conditions for working with personal data.

On the other hand, there are cheaper and fairly effective options for providing protection, for example, installation of modernized shut-off valves, electrical distribution panels and power supply filters.

Active - a set of means that allow you to protect personal data in a network, the zone of which extends beyond the area of the facility. They are also used if passive information protection equipment is extremely unprofitable to implement economically or is impossible from a technical point of view. We are talking, first of all, about linear and spatial noise, noise and pulse generators (allowing you to neutralize all kinds of bugs), ultrasonic or electromagnetic suppression systems for voice recorders.

Combined (considered equally active and passive). These include sound amplifiers and soundproofing devices, remote controls in a protected version, microphones, anti-bugs and noise generators, magnetic field indicators, surge protectors with an interference suppression option, as well as highly specialized equipment that makes it safe to transmit information through grounding circuits, vibroacoustic and acoustic channels.

Organizational - verification activities to detect lines and communication channels, determine the degree of current network security, identify leaks, integrate data destruction means.

Technical methods are divided according to their operating principle into:

- hardware (passive, active);

- software (everything related to ensuring information encryption);

- physical - do not allow a person to penetrate directly into the location of personal information.

Processing personal data does not require prior obtaining a license, however, at the stage of implementing measures to protect confidential data, the employee must fulfill the obligations prescribed in regulations and laws. (Мартин М 2002)

CHAPTER III. INFORMATION SECURITY PROBLEMS

In the modern world, technologies for processing, storing and transmitting information are rapidly developing. The use of information technology requires increased attention to information security issues. The destruction of information resources, their inaccessibility or unauthorized use due to information security violations cause serious problems for citizens, social groups, companies and states.

Information security problems can be divided into three large groups:

1. Problems of a humanitarian nature - information security problems arising in connection with the uncontrolled use and dissemination of personal data of citizens, invasions of privacy, slander and identity theft.

2. Problems of an economic and legal nature - information security problems arising as a result of leakage, distortion and loss of commercial and financial information, theft of brands and intellectual property, disclosure of information about the financial situation of citizens, industrial espionage and the dissemination of materials damaging the reputation of companies.

3. Problems of a political nature - information security problems arising from information wars, cyberwars and electronic intelligence in the interests of political groups, compromise of state secrets, attacks on information systems of important defense, transport and industrial facilities, incomplete information and disinformation of the heads of large institutions.

Let us briefly explain the main components of information security.

What is the problem of information security?

It lies in the fact that, under certain conditions, all information owned by organizations, firms, corporations and other economic units needs constant protection. Among the threats are unauthorized ones: destruction, modification, copying, blocking of authorized access to data, etc.

What is information security for different users of computer systems?

Information security tools protect data from leakage, programs, systems and networks from hacking, unauthorized access, file corruption or other types of attacks. If we are talking about commercial or government structures, the information also protects against spies or possible attackers within the team itself. (Мельниченко С.Б. 2008)

There are three components of information security.

Its main components are described below - confidentiality, integrity, availability.

What are the threats to information security?

The most common information security threats are:

♦ DDOS attacks;

♦ Introduction of malicious code;

♦ Data leak;

♦ Spam, phishing, worms;

♦ Replacement of the access subject;

♦ Attacks on web applications.

What are the most serious violations in the field of information security?

♦ Related threats

♦ Objectionable Content

♦ Potentially dangerous programs

♦ Unauthorized access

♦ Cyberwars

♦ Information leaks

♦ Data loss

♦ Fraud

At the same time, it must be emphasized that the main task of information security is the balanced protection of confidentiality, integrity and availability of data, taking into account the expediency of application and without any damage to the productivity of the organization.

Information security solves its problems by creating a system for authentication and authorization of users, separation of access rights to information and access control. It is also important to create a system in which employees or attackers would not be able to hide their actions.

Main types of information security threats

♦ Pirated software

♦ Human factor

♦ Computer viruses

♦ Insider leaks

♦ Problems with law

♦ Backup

♦ Physical protection

♦ DDOS protection service

In recent years, the issue of information security has been supplemented with such complex tasks as:

– development and implementation of reliable electronic digital signature systems, electronic elections, procurement and payments

♦ creation and implementation of advanced authentication tools (biometric and others)

♦ development and implementation of new methods for ensuring reliability and fault tolerance (innovative technologies of clustering, virtualization, etc.)

♦ protection of wireless connections, mobile devices and smart electronics

♦ ensuring the security of web services and cloud technologies

Solving these pressing problems in the field of information security is possible only if:

♦ attention to these issues and appropriate, targeted actions of company leaders and representatives of the public and government authorities

♦ coordinated activities of national and international bodies involved in information security standardization and the fight against cybercrime.

Information security in networks includes a wide range of issues. Information security is fundamental to the well-being of a business, so we will consider all the problems it solves.

So, the first direction is to ensure data integrity. Today, all commercial information, accounting data, financial statements, client databases, contracts, innovative ideas of company employees, plans and strategy for its development are stored in a local information and computer network.

Not all documents are always duplicated on paper, because the volume of information is very large. In such conditions, information security provides a system of measures that are designed to ensure reliable protection of servers and workstations from failures and breakdowns leading to the destruction of information or its partial loss. A serious approach to this issue means that information security should be based on a professional audit of the entire IT infrastructure of the company.

An IT audit allows you to assess the state of the network and equipment, analyze potential threats, identify and promptly eliminate “weak” points in the cable system, server and workstations, disk systems and violations in equipment configuration. Thus, the technical risks of possible loss of information are reduced. Incorrect operation of archiving systems, network and application software also leads to data damage. Ensuring the information security of your company, our employees test the software and check its compliance with modern requirements. (Миленков Ю.В , 1999)

The next most important task is to ensure the confidentiality of information. The protection of trade secrets directly affects the competitiveness of the company and its stability in the market. Here, information security and network protection faces external and internal deliberate threats aimed at data theft. Hackers, industrial espionage and information leaks due to the fault of our own employees pose the greatest threat. The temptation to sell valuable business information is great not only among employees who are being laid off, but also among those whose ambitions in the workplace are unfulfilled.

In this case, information security takes preventive measures aimed at controlling insiders and multi-stage protection of servers from hacker attacks.

Therefore, measures to counter unauthorized access should be aimed at achieving two goals:

♦ Create conditions where accidental or intentional actions leading to data loss become impossible. Information security solves this problem by creating a system for authentication and authorization of users, separation of access rights to information and access control.

♦ It is also important to create a system in which employees or attackers would not be able to hide their actions. Here, a system for monitoring security events and auditing access to files and folders comes to the aid of an information security specialist.

Network information security also involves protection from external attacks aimed at stopping the operation of servers, computers or network components.

And the most important thing for which information security is needed is the availability of information for legitimate users. All information security measures are useless if they hinder or block the work of legitimate users. Here, reliable authentication and well-implemented separation of user rights come to the fore.

Our company will make every effort to ensure that the information security of your company is organized at a level that makes it practically invulnerable. (Моисеенко Л.Т. 1981)

3.1. Methods and means of ensuring information security

What are information security methods?

Information protection methods include means, measures and practices that should protect the information space from threats - accidental and malicious, external and internal.

The purpose of information security activities is to protect data, as well as to predict, prevent and mitigate the consequences of any harmful effects that could cause damage to information (deletion, distortion, copying, transfer to third parties, etc.)

What methods of ensuring information security exist? Methods for ensuring information security are divided into technical, administrative, legal and physical. Let's tell you more about each of them.

Technical

Technical means of protection include firewalls, anti-virus programs, authentication and encryption systems, regulation of access to objects (each participant has a personal set of rights and privileges, according to which they can work with information - get acquainted with it, change it, delete it).

Administrative

This group of protective measures includes, for example, a ban on employees using their own laptops to solve work problems. A simple measure, but thanks to it, the frequency of infection of corporate files by viruses is reduced, and cases of leakage of confidential data are reduced.

Legal

An example of a good preventative measure from the legislative sphere is tougher penalties for crimes in the field of information security. Legal methods also include licensing activities in the field of information security and certification of informatization objects.

Physical

Physical security measures include security systems, locks, safes, and surveillance cameras. It is enough to compare which information is protected better - that which is recorded on the hard drive of a computer running on the network or that which is recorded on removable media locked in a safe.

Build comprehensive protection

To maintain information security at a high level, an integrated approach is required. In most cases, it is not enough to simply install antivirus software on work computers and install a video surveillance camera at the entrance of the enterprise. For effective protection, you need to combine and apply various means of protection (administrative, technical, legal, physical).

It is worth mentioning separately about backup. Thanks to it, you can quickly restore original data if it was lost or corrupted as a result of a cyber attack or an employee error. Backup is a simple and versatile tool that increases the stability of any system.

Typically, backups are written to removable media (which are stored separately and locked up) or stored in the cloud, or a combination of both. Encryption is often used as an additional security measure. (M. A. Ameen, J. W. Liu, K. Kwak, 2012)

Security policy

Basic principles of information security policy:

♦ Provide each employee with the minimum required level of access to data - exactly as much as he needs to perform his job duties. This principle allows you to avoid many problems, such as leakage of confidential data, deletion or distortion of information due to irregularities in working with it, etc.

♦ Multi-level approach to security. Separation of employees into sectors and departments, closed rooms with key access, video surveillance, regulations for the transfer of information, multiple backups of data - the more levels of protection, the more effective the information security activities.

Firewalls play an important role in such a security system. These are “checkpoints” for traffic that will filter out many potential threats at the entrance and will allow you to establish rules for access to the resources used by employees.

Maintaining a balance between the potential damage from the threat and the costs of preventing it. When determining an enterprise's security policy, it is necessary to weigh the losses from a violation of information security and the costs of protecting it.

It is important to understand that no security system can provide a 100% guarantee of data protection. But a multi-level comprehensive information security system is definitely more effective than the use of individual methods of ensuring information security. (Назарович О М 2000)

3.2. Practical aspects of cryptography

Cryptography (from the English cryptography) is an advanced field of cybersecurity that deals with encryption and data protection. In simple terms, it uses complex algorithms to convert information into encrypted form, ensuring confidentiality and data integrity in the digital world. Cryptographic encryption plays an important role in protecting personal and financial data, providing online security and protection from cyber threats. This is the main task of cryptography.

Cryptography is the art and science of encryption. At least that's how it started. Today, the concept of cryptography has expanded significantly to include authentication, digital signatures, and many other basic security features.

Cryptography is still an art and a science: to build a good cryptographic system, you need to have deep scientific knowledge and a decent amount of that “black magic” that is called experience. Cryptography is a very broad field of science.

The variety of aspects of cryptography is what gives it its truly unique charm. By and large, cryptography is a mixture of various fields of science. There is always something to learn, and new ideas come from literally everywhere. On the other hand, such diversity is also one of the reasons for the complexity of cryptography. It is impossible to understand it completely.

In real life, even a poorly implemented cryptographic method will always be much better than the rest of the security system. Everywhere there is a door to a bank vault (at least in the movies) - a sort of thick thirty-centimeter door made of hardened steel with huge bolts. Of course, she looks very impressive. In the digital world, however, security often resembles installing a similar door in a camping tent. Many people stand near the door and argue about how thick it should be, but no one thinks to look at the tent itself. People love to talk about key length in cryptographic systems, but they don't like debugging buffer overflows on Web servers. The result is quite predictable: attackers achieve a buffer overflow and do not burden themselves with unnecessary worries about cryptography. Cryptography is only really useful if the rest of the system is also secure.

Cryptographic information security is the process of using cryptographic methods and algorithms to ensure confidentiality, integrity, authentication and availability of data. It is used to protect information from unauthorized access, changes and other types of cyber threats. (Рябкова У.С. 2009)

Cryptography Basics

Despite the fact that cryptography is primarily associated with the achievements of modern science, its use stretches back several thousand years of history. In the past, this technology was mainly used by government officials and intelligence agencies, but today it has become firmly established in the lives of everyone who has access to the Internet.

The main method used in modern cryptography is the encryption process, which transforms information into an encrypted format that can only be deciphered using the appropriate key. If only the sender and recipient have a code, the transmitted data remains unintelligible characters for everyone else.

Table 3.2.1. Basic Cryptography Concepts

Concepts	Description
Encryption	The process of converting data into encrypted form to ensure confidentiality.
Decryption	Reverse process in which encrypted data is returned to its original form
Key	Secret information used in an encryption algorithm to transform data
Cryptographic protocol	A set of steps and rules for performing secure cryptographic operations
SSL/TLS protocol	Protocols provide encryption of data transmitted over the Internet, providing a secure connection
Key management	The process of generating, storing and managing encryption keys for security
Cryptographic means	Tools, methods and algorithms for implementing cryptographic information protection

Encryption algorithms

In cryptography, there are two main types of encryption algorithms.

Symmetric algorithms that use the same secret key to both encrypt and decrypt data. An example of symmetric encryption is its application in financial transactions and online payments. However, such algorithms are vulnerable to key sniffing attacks. In this case, attackers gain access to encrypted data.

Asymmetric algorithms that solve the security problem using two keys: public and private. Initially, the sender encrypts the message using his public key and sends it to the recipient. The recipient uses his private key to decode the message. The unique pair “sender’s public key – recipient’s private key” ensures reliable data protection and prevents theft. Asymmetric algorithms are used to create digital signatures and other tasks. (Нейман В.И 1975)

Table 3.2.2. Types of cryptography in brief

Type of cryptography	**Description**	**Examples of methods and algorithms**
Symmetrical	Uses one key to encrypt and decrypt data	AES, DES, 3DES, Blowfish
Asymmetric (RSA)	Uses a pair of keys: public and private. The public key is used for encryption and the private key is used for decryption	RSA, ECC
Hashing	Converts data to a fixed hash length. Hashes are used to check data integrity	MD5, SHA-256, SHA-3
Digital signatures	Used to authenticate the sender and ensure data integrity	RSA (for signatures), ECDSA (elliptic curves for signatures)
Authentication protocols	Provide secure identification of subjects	OAuth, Kerberos, OpenID
Quantum cryptography	Uses the properties of quantum mechanics to create secure cryptographic systems	Quantum cryptography based on single-photon sources, quantum key distribution (Quantum Key Distribution)

The origins of cryptography and its development until the beginning of the 20th century

The first records of deliberately altered symbols date back to 1900 BC, when modified hieroglyphs were discovered in archaeological finds from the tomb of the ancient Egyptian aristocrat Khnuphotep II. The researchers suggest that the symbols were not used for encryption, but rather were intended to attract attention and provide those interested with the opportunity to practice deciphering the encoded text.

Over time, cryptography found use among government officials for military purposes and to enable trusted communications. During this period, the Caesar cipher appeared, named after the Roman emperor. History suggests that he transmitted his orders to the generals at the front in encrypted form. One of the methods used by Caesar was the monoalphabetic cipher, or simple substitution cipher. The principle of operation of this cipher is to replace letters with the next ones in the alphabet after a certain step. For example, in triple shift encryption, the letter A is replaced by D, B by E, and so on. During World War II, British mathematician Alan Turing and his colleagues at the British Government Code School were tasked with the critical task of learning how to intercept and decipher encrypted messages from the German command. As a result of the efforts, the Bomb computer was created, specially designed to decipher codes created by the Enigma mechanism.

At the end of hostilities, Winston Churchill reported to King George VI that it was thanks to the Turing project that the country was able to gain a competitive advantage over the enemy. This success, and the computing devices that followed it, similar to modern computers, ushered in a new era in computing technology. (Никитский Г.В., 2010)

Principles of modern cryptography

Modern cryptography methods rely on a number of key principles, adherence to which is integral to ensuring security.

♦ Confidentiality. The data remains accessible only to those who have the appropriate authorization keys for decryption.

♦ Integrity. Keeping data unchanged during transmission. When transmitting information over open networks such as the Internet, a cryptographic algorithm must ensure that the data is delivered to the recipient without distortion.

♦ Impossibility of disclaiming liability. Use of mechanisms to determine the source of data. This prevents message attribution from being denied, since each message is tied to a specific sender. You can delete a message, but you cannot change the authorship.

♦ Authentication. Confirmation of the user's identity in the system. This principle ensures that the user truly is who they claim to be online.

Compliance with these principles is integral to ensuring reliable data protection using modern cryptographic transformation methods.

The original concept of open algorithms was formulated by the Dutch cryptographer Kerghoffs at the end of the 19th century. He proposed the idea that the security of a system should not depend on its secrecy, since if one of its components is disclosed, a complete compromise is possible by revealing key information about key generation. According to

Kerghoffs, a reliable algorithm consists of constantly changing the decryption keys, thereby ensuring data protection, even if the principle of its operation is known. (L. O. Gostin, J. G. Hodge, 2002)

Where is cryptography used?

Cryptography is invisibly permeating many of the operations we perform every day, and in fact has already become part of our daily routine. Let's look at a typical day for an office worker.

After waking up, he checks social networks and email. Even before the start of the working day, he manages to submit an application for government services via the Internet using a digital signature. On the way to work, he fills up the car, paying for fuel with a card, then arrives at the place of work. Then he parks and pays for parking, and then goes to the nearest cafe for a cup of coffee. As a regular customer of this establishment, he can pay with bonuses accumulated in his profile. The entire workday, from messaging in corporate chats to video conferencing on Zoom, is accompanied by cryptographic operations that ensure the protection of personal data. Upon returning home in the evening, he selects a movie to watch in the online cinema using his personal account. All steps involve the use of cryptographic methods that guarantee the safety and security of personal information. (Николаев В.И., Брук В.М. 1985)

Authentication

Authentication is a process that is used to confirm the truthfulness of information. To provide a user with access to a virtual account, the system authenticates his or her identity, for example using a password or biometric data such as a fingerprint or retina scan. To verify the authenticity of documents, digital signatures are used, which can be compared to electronic fingerprints. In the case of an encrypted message, a digital signature links the author to the document.

An example that demonstrates the importance of a digital signature is the case of a data leak from the computer of Hunter Biden, the son of (at that time) presidential candidate Joe Biden. Experts in the field of cryptology, collaborating with the Washington Post, were able to confirm the authenticity of some emails thanks to digital signatures and time stamps. Since the emails were sent through Google's email service, which uses trusted certificates, there was no doubt that the emails were not faked by hackers.

Secure connection between server and browser

The process is carried out mainly using SSL/TLS protocols and ensures reliable protection and confidentiality of user data on the Internet. When following a link, the user will be taken to exactly the site he expects, and not to any other.

Hard drive encryption

Hard drive encryption is the process of using cryptographic techniques to protect data stored on the hard drives of a computer or other device. This process ensures the confidentiality and security of information, preventing unauthorized access to data in the event of loss or theft. With hard drive encryption, data is recorded in encrypted form and you must provide the appropriate key or password to view or edit it. This provides protection in case of physical access to the device or a hacking attempt.

End-to-end encryption

This method of data transfer is based on the use of keys known only to both users, which ensures a high level of confidentiality and security of information. During the communication process, both users use keys to encrypt and decrypt messages. Even the server operator does not have access to the contents of the messages, as they remain encrypted.

Modern instant messengers such as WhatsApp* and Telegram offer the method as one of the most secure methods of communication. It becomes especially important in an environment where the sharing of personal data and sensitive information is becoming more common. Such applications use encryption protocols, such as the Signal protocol, to ensure reliable data protection when users communicate.

The key exchange system for data encryption helps minimize the risks of information leakage and unauthorized access to it. This method allows users to be confident that their private conversations remain private and secure, even if they take place over public networks.

Electronic money

Encryption is important in the field of data security during transactions. This is especially true for sensitive data such as account numbers and payment amounts. Due to the use of encryption, transaction information becomes inaccessible to third parties and attackers, which ensures a high level of confidentiality.

Digital signatures, such as PINs or one-time codes, play an important role in authorizing credit card payments. The mechanisms provide an additional level of security by confirming that the cardholder is indeed authorizing the payment. This helps prevent unauthorized transactions and fraud. The modern era of online shopping is inseparable from attention to information security. With the development of online trading, users have become increasingly demanding regarding the safety of personal and financial data. The use of encryption and digital signatures increases the level of trust between customers and online stores. Without reliable protection, many would doubt the safety of their financial transactions in the online environment.

Quantum cryptography

Quantum cryptography is an innovative information security technology based on the principles of quantum mechanics and is often considered the future of cryptography. The methodology uses the properties of quantum particles, such as quantum superposition and quantum entanglement, to ensure a high degree of security in data transmission. Quantum cryptography allows the creation of cryptographic keys that can be transferred between a sender and a recipient and are guaranteed not to be eavesdropped or spoofed. This became possible thanks to phenomena that are characteristic only of the microcosm, where the states of particles can change during observation.

Although quantum cryptography is still in the research and development stage, leading technology companies are already making significant strides in this direction. For example, IBM, Google and other information industry giants talk about their successes in creating quantum computers and security systems based on quantum principles. However, despite the promise, the cost and complexity of implementing quantum cryptography remain significant challenges. But the possibility of using quantum properties to ensure data security makes this an exciting area for future innovation in cybersecurity. Cryptographic information security plays a critical role in the modern world of information technology and cybersecurity, helping to ensure the privacy and security of data online. (Олифер В.Г 2001)

3.3. Directions for the development of information security

At first I wanted to write about the 9 most promising areas of information security for the next 5 years

♦ Development of cyber weapons

♦ Cloud security

♦ Voluntary certification in the field of information security and new tools of “trust”

♦ Anti-financial fraud

♦ Protection of personal data.

♦ Information security management automation systems

♦ Mobile device security

♦Virtualization protection

..

Development of cyber weapons

Unlike other topics, this is the creation and implementation of “attack” systems, including solving infrastructure, personnel, legislative and other problems. This also includes developments similar to those of Ntrepid (the essence of their solution boils down to manipulating discussions on social networks). The flywheel of the arms race in the cyber environment has been launched and it can no longer be stopped (the effectiveness of this type of weapon in the modern world is very high). It is difficult to predict the activity of the state in this direction, but I think that by the next elections we will see something interesting.

Cloud Security

This direction will develop to the benefit of the corporate sector. There are a huge number of unresolved legal, organizational and technical issues in Azerbaijan, so a lot of work remains to be done in this direction.

Voluntary certification in the field of information security and new tools of “trust”

The most thankless job and at the same time the most necessary. Existing certification systems for law enforcement agencies, unfortunately, do not meet modern market needs. An alternative certification system is needed. Now such work is being carried out within the framework of the security project, I really hope for success. This also includes new trust tools, in particular projects like ISM:MARKET and Information Security Market Research, which is currently being actively prepared. (Партыка Т.Л., Попов И.И 2002)

Anti-financial fraud

Security of electronic money in general. A large and serious area that is developing very quickly. The main driver of the market now is fraud in remote banking.

Personal data protection

Oddly enough, the topic will continue to develop. We, in Azerbaijan, have not yet even reached the point of realizing the criticality of medical information. We rarely encounter Identity Theft. We are waiting for a rethinking of the topic of personal data, and I hope, a change in approach. By the way, the initiative to create a council to protect the rights of citizens in terms of personal data on the basis of the state is an extremely logical decision, and it was worth starting with this.

Information security management automation systems

This strange name refers to the development of automation tools for risk management, document management, etc. In other words, certain software products that make it possible to simplify work with a management system.

Comprehensive security of medical systems

It is actively developing in the West, within companies developing medical systems. Perhaps the topic will not reach us in 5 years, because... We are seriously behind in the "technological medicine" market. Although in terms of service and integration, serious growth is possible.

Mobile Device Security

Although the topic is applied, I think it is necessary to highlight it as a trend. I doubt that in 5 years the main share of this market will be taken and retained by independent players. Most likely, functionality for managing mobile devices will include solutions from major players.

Virtualization protection

The topic is not new, but there is virtually no market for virtualization security tools in Azerbaijan. There are not many specialists. So this direction is also promising.

Ensuring cybersecurity in modern conditions is a complex, multi-stage process that provides for various directions of development of the digital world. At the same time, the field of information security itself is developing. Many areas of information security, which only yesterday were only in projects and in the ideas of developers, are already finding their direct implementation today.

If we consider the issue from a practical point of view, the very concept of cybersecurity and information protection is changing as the world changes - many types of data protection and information security are gradually becoming obsolete, but new ones are taking their place. Taking into account the active development of information security, IT technologies, AI technologies and other areas of the digital world, experts identify several current areas in which the information security industry will develop in the coming years. (Петровский С.П., 2007)

RegTech and SupTech projects

Improving the external information security audit system. Ensuring the quality of information security compliance assessment in financial institutions is defined as part of the initiative within the framework of the Main Directions for the Development of SupTech and RegTech Technologies for the period 2023–2025.

When developing a concept for improving the system of external audit of information security, it is planned to study the issue of creating additional legal mechanisms for improving the quality of assessment of compliance with information security in organizations in the credit and financial sector and increasing the quality of services of inspection organizations. These mechanisms will be used to formulate requirements for ensuring the reliability of external audit results by involving auditing organizations that have confirmation of compliance of their activities with national standards identical to international ones. The external audit system is planned to be implemented in relation to:

♦ audit on information security and operational reliability;

♦ audit of cloud service providers;

♦ application security audit.

An important direction will be a qualitative transition to the systematic use of advanced analytics methods for analyzing the operational risks of credit institutions, taking into account the data generated as part of the activities:

♦ based on the results of the analysis of information security incidents and operational reliability;

♦ by calculating the risk profile of organizations in the credit and financial sector and financial associations;

♦ on supervision, including in the form of cyber exercises;

♦ analysis of data obtained within the framework of reporting forms on the topics of operational risk management and ensuring operational reliability.

Azerbaijani banks plan to integrate the results of monitoring and analysis of operational risks of credit institutions into the assessment of the economic situation, plans for restoring financial stability, as well as the quality of internal procedures for assessing the capital adequacy of credit institutions in terms of: - information security risk; – information security risk associated with the possible execution of transactions without the consent of clients; – information security risk associated with a possible violation of operational reliability. Additionally, issues of development, testing and subsequent adjustment of the methodology for assessing the capabilities of supervised financial institutions to identify incidents of information security and operational reliability, respond to them and recover in the event of their implementation, as well as methods for assessing the organization of the risk management system for information security and operational reliability will be worked out.

Cyber exercises

The financial system of Azerbaijan plans to continue the development of supervisory stress testing of financial institutions in order to ensure information security and operational reliability as part of expanding the list of scenarios, issues and tasks considered during cyber exercises. The implementation of this direction will ensure control over the operational risks of credit and financial organizations in these areas in the context of the transition to technological sovereignty, as well as control over the level of quality of IT services provided to clients and counterparties.

The following activities are planned to be carried out as part of the cyber exercise:

♦ conducting cyber exercises (stress testing) of the activities of organizations in the credit and financial sector;

♦ cyber risk assessment for the purpose of integration into the supervisory assessment of operational risk in terms of:

♦ information security risk;

♦ information security risk associated with the possible execution of transactions without the consent of clients;

♦ information security risk associated with a possible violation of operational reliability

Goals and directions of ensuring information security in the field of state and public security

What are the goals and directions of ensuring information security in the field of state and public security?

The strategic goals of ensuring information security in the field of state and public security are protecting sovereignty, maintaining political and social stability, the territorial integrity of Azerbaijan, ensuring fundamental rights and freedoms of man and citizen, as well as protecting critical information infrastructure. (Пятибратов А.П 2001)

The main directions of ensuring information security in the field of state and public security are:

a) countering the use of information technologies to promote extremist ideology, spread xenophobia, ideas of national exclusivity in order to undermine sovereignty, political and social stability, forcibly change the constitutional system, and violate the territorial integrity of Azerbaijan
b) suppression of activities harmful to the national security of Azerbaijan carried out using technical means and information technologies by special services and organizations of foreign states, as well as individuals;
c) increasing the security of critical information infrastructure and the stability of its functioning, developing mechanisms for detecting and preventing information threats and eliminating the consequences of their manifestation, increasing the protection of citizens and territories from the consequences of emergency situations caused by information and technical impacts on critical information infrastructure objects;
d) increasing the security of the functioning of information infrastructure facilities, including in order to ensure sustainable interaction between government bodies, preventing foreign control over the functioning of such facilities, ensuring the integrity, stability of operation and security of the unified telecommunication network of Azerbaijan, as well as ensuring the security of information transmitted through it and processed in information systems on the territory of Azerbaijan;
e) increasing the operational safety of weapons, military and special equipment and automated control systems;
f) increasing the effectiveness of preventing offenses committed using information technologies and combating such offenses;
g) ensuring the protection of information containing information constituting state secrets, other information of limited access and distribution, including by increasing the security of relevant information technologies;
h) improvement of methods and methods of production and safe use of products, provision of services based on information technologies using domestic developments that meet information security requirements;

i) increasing the efficiency of information support for the implementation of state policy of Azerbaijan;

j) neutralization of information impact aimed at eroding traditional Azerbaycan spiritual and moral values. (Ретана А., Слайс Д., Уайт Р. М)

…

Experts have compiled a list of the 8 main cybersecurity forecasts for the coming years

On March 28, 2024, the Gartner company presented a report that examines key trends in the development of the global information security market. It is noted that the current macroeconomic situation and uncertainties pose new challenges for business representatives and various organizations, the successful solution of which will determine operational efficiency. Experts identify eight key trends in cybersecurity for the coming years. It is expected that these forecasts will help companies implement the optimal strategy for protecting their information infrastructures

By 2027, 50% of CISOs will implement employee-centric approaches to their cybersecurity programs. This will help minimize operational friction and improve the effectiveness of controls. A Gartner survey shows that more than 90% of workers who admitted to performing potentially dangerous activities knew that their actions would increase the risk to the organization, but did it anyway.

In 2024, modern privacy regulations will cover the bulk of customer data. However, less than 10% of organizations will be able to successfully use privacy controls as a competitive advantage. Gartner recommends implementing solutions in compliance with the General Data Protection Regulation (GDPR). (Риордан Дж. 1966)

By 2026, 10% of large enterprises will have a comprehensive and mature zero trust infrastructure. For comparison: as of the beginning of 2023, this figure was less than 1%.

In 2027, approximately 75% of company employees will acquire, modify, or create technology outside the purview of the IT department. In 2022, the value was 41%. In this situation, organizations are encouraged to rethink their cybersecurity operating model to better engage with employees.

By 2025, 50% of cybersecurity leaders will have unsuccessfully attempted to use cyber risk measurement to inform corporate decision-making. Subject matter experts should focus on the quantitative assessments that decision makers are asking for, rather than performing threat analysis on their own.

In 2025, nearly half of cybersecurity executives will change jobs. Moreover, 25% will move to other positions solely because of the numerous stress factors associated with their professional activities. Moreover, due to the COVID-19 pandemic and staff shortages in the industry, the situation is only getting worse. By 2026, 70% of companies will have one member with cybersecurity experience on their board of directors. Gartner recommends that CISOs proactively promote their initiatives to the board level of their organization.

In 2026, more than 60% of detection, investigation and incident response (TDIR) tools will use risk management data to review and prioritize detected threats. In 2022, this figure was less than 5%. TDIR capabilities provide a single platform to provide a complete picture of the risks and potential impact of threats on a company's IT infrastructure. (Рябкова У.С. 2009)

As a result, I would like to touch on the 3 main principles of information security, namely the three basic principles that information security must comply with

♦ confidentiality,

♦ integrity,

♦ availability.

RESULTS

Analysis of methods for organizing the processing and protection of personal data showed that the proposed methods and the protection systems created on their basis require significant resources for implementation, have a strong dependence on the type of data and are highly redundant in practical application for working with small-sized data arrays. Therefore, in some cases, it is advisable to use methods that remove the requirements for confidentiality of personal data, which significantly reduces protection costs.

It has been shown that one of the effective and promising approaches to protecting personal data in information systems is depersonalization. A mathematical model of PD has been developed, which has made it possible to determine sufficient conditions for

depersonalization. compare known depersonalization methods, explore the properties of anonymized data depending on the features of their storage by various operators.

Quantitative assessments of the safety of personal data during depersonalization have been developed, allowing comparison of different methods of depersonalization from a unified perspective.

An anonymization algorithm based on data mixing using permutations has been developed and theoretically justified. The advantage of the algorithm is the minimum amount of specified algorithm parameters necessary for carrying out depersonalization and de-depersonalization, which makes its use effective when working with large volumes of PD. (Саати Т.А 1971)

Historically derived from the institution of privacy, this legal institution is a new, separate entity. But the need to determine the constitutional and legal framework for the protection of personal data in Azerbaijan is long overdue.

We have to admit, however, that the level of development of issues of constitutional and legal protection of personal data in the domestic doctrine, as well as in the practice of the Constitutional Court of Azerbaijan, does not meet modern realities. Research into relevant issues using the modeling method and the development of a Azerbaijan model of constitutional and legal protection of personal data seem promising.

So, the protection of personal data is a complex technological process that prevents violation of the confidentiality of personal data and ensures the security of information in the process of management and production activities of the company.

And the responsibility for organizing such a complex process rests entirely with the employer (operator). For violation of the provisions of the legislation on personal data when processing personal data of employees, the perpetrators are subject to disciplinary, material, civil, administrative and criminal liability.

The establishment of personal data belongs to the public branch of law. At the same time, the norms of this institution are reflected in such an industry traditionally classified as private law as labor.

It is obvious that this legal institution regulates social relations related to several branches of law, i.e. located at the intersection of industries, therefore, in the author’s opinion, this legal institution should be considered as intersectoral.

From a practical point of view, the importance of the institution of personal data lies in the fact that: Firstly, any individual is a carrier (subject) of personal data, whose interests are related to the fact that personal data “belonging” to him should not be distributed in an arbitrary manner and should their protection is ensured. (Садовский В.Н. 1974)

Secondly, any legal entity, from the moment it enters into an employment relationship with at least one employee, becomes a personal data operator, who is charged with ensuring the confidentiality, integrity and availability of the specified data, as well as responsibility for violations of the legislation on personal data. Judicial practice on the processing and storage of personal data is one of the most common categories of labor disputes.

The processing of personal data is subject to general requirements, which are based on the principles of voluntariness, ensuring equality of opportunity, legality, and non-discrimination in labor relations. Accordingly, these requirements contained in the regulatory legal acts of the labor legislation of Azerbaijan must be met and not contradicted by local regulatory acts of various organizations and enterprises, so as not to infringe or violate the legitimate interests of a citizen of our republic.

In general, despite the presence of a number of fundamental documents, in the existing regulatory and legal field there are no unified and comprehensive provisions related to the organizational and legal protection of personal data of employees. Recently, the vicious practice of distributing and illegally using both the personal databases themselves and various illegal methods of obtaining them (mostly software) has become widespread in Azerbaijan.

Confidential databases of personal data, with varying levels of confidentiality - illegally obtained both from commercial structures (protected in accordance with the secrecy regime of commercial or professional secrets), and from government bodies, in which personal data is protected in accordance with the regime of official secrecy - are freely sold on the markets and on the Internet. The indicated diversity of legal regulation at the same time, the lack of practice in interpreting regulations governing this area, its poor knowledge, as well as the inability to consider the entire range of problematic issues related to the protection of personal data allow us to believe that this dissertation only reveals the problems of the issue, which is in constant development.

As a result, when protecting confidential information, there is always a cyber project, for this you need to know the following: (Саксонова П.Н., Шаумдин Н.З. 2010)

When the goals of personal data processing are achieved, as well as in the event of the personal data subject's withdrawal of consent, personal data are subject to destruction if:

♦ Cyberprotect does not have the right to process without the User's consent;

♦ otherwise provided by the agreement to which the User is a party, beneficiary or guarantor;

♦ otherwise provided by another agreement between Cyberprotect and the User.

The User has the right to demand that Cyberprotect clarify his personal data, block it or destroy it if the personal data is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the stated purpose of processing, and also to take measures provided by law to protect his rights.

In particular, the User has the right to revoke his consent to the processing of personal data at any time in the manner prescribed by the rules of this Privacy Policy. Consent may also be revoked by written notice sent to Cyberprotect. by registered mail. In addition, upon achieving the purposes of processing personal data, as well as in the event that the subject of personal data revokes his consent, personal data are subject to destruction if:

- Cyberprotect has no right to process without the consent of the User;
- otherwise not provided by the agreement to which the User is a party, beneficiary or guarantor;

- otherwise not provided by another agreement between Cyberprotect and the User. (Саксонова П.Н., Шаумдин Н.З. 2011)

It is very important to know some points about cybersecurity, namely 3 things that organizations should think about:

Is your purchasing manager choosing unencrypted devices

If the decision to purchase unencrypted USB drives, SSDs, or IoT devices is based solely on price, without considering whether they are secure or have hardware encryption, then these unencrypted devices create a cybersecurity vulnerability. This puts the entire organization at risk of a data breach.

Do employees reuse passwords or use shortcuts to bypass security measures

If employees do not follow basic cybersecurity practices and are careless with passwords or email attachments, they are putting the entire organization at risk. Cybercriminals actively use weak or known passwords and employ phishing tactics to compromise the security of their victims. These are some of the most common vectors of cyber attacks.

Does the marketing director use personal data from time to time?

The EU General Data Protection Regulation states that personal data may only be collected with the consent of its owner and only for the specified purpose. If you collect or share data illegally, you expose everyone to the risk of large fines and lawsuits. (Семенов Ю.А. 1998)

At our core, we all need to take cybersecurity and data privacy seriously

If you see unencrypted USB drives, SSDs, or unsecured IoT devices being used in your organization, you need to speak up. If you notice your colleagues not following cybersecurity practices, you need to speak up. If you witness a marketing employee misusing customer data, you need to speak up. (S. Brands., 2015)

Changing the culture is key to success

If we want to change attitudes and get people to take cybersecurity and data privacy seriously at all levels of the organization, we need to change the mindset. Organizations have many incentives to do this. There is clear evidence that customers will be happy to do business with organizations that they believe will take care of their data, and more reluctant to do business with those that do not. Maintaining customer trust and preventing any cybersecurity incidents that could undermine that trust should be a top priority for all of us.

There are also many disincentives for organizations to take data protection seriously. Firstly, the GDPR imposes a maximum fine of €20 million or 4% of annual global turnover (whichever is greater) for EVERY incident. The cost of resolving an incident can run into the millions of euros, and if it is a ransomware attack, the cybercriminals may demand a multi-million dollar ransom on top of that. You may also face legal action from the people whose data was compromised.

In addition to such sanctions against the organization as a whole, sanctions against individuals are also emerging. A recent case in the US set a new precedent in cybersecurity when board members and the CISO were individually named as defendants. A report from analyst firm Gartner predicts that CEOs will soon likely be held personally liable for cyberattacks.

As citizens and as customers, we want organizations to protect our data. And when we are responsible for the data of others, the standards must be just as high. We should be concerned, both collectively and individually, that we may all be held accountable. But we should also strive to protect data because it is the right thing to do. (Советов Б.Я. 1995)

,,,

Modern companies use a multi-level security model from the very beginning of development. Even at the design stage, we use the principles of secure coding and architectural solutions that protect against potential threats. We look for our own solution for each project: somewhere we need to create several user roles with different access levels; somewhere we need to provide protection for file storage, somewhere - secure data transmission channels. But there are also methods that we use in each project: regular audits and thorough code reviews. They allow us to find and eliminate vulnerabilities even before the final stage of development.

They carefully monitor operating system, software and plugin updates, ensure they are up-to-date and respond to all vulnerability reports. We use static code analyzers integrated into our automated processes to ensure that errors, flaws and potential vulnerabilities do not penetrate the main repository. All their development and data access occurs over secure VPN channels. In addition to all these technical measures, modern enterprises work on the "human factor" - they teach developers the basics of computer hygiene and security. The most important principles:

♦ Use of licensed software,

♦ Two-factor authentication for all used accounts and services.

Real specialists pay special attention to protection against threats related to social engineering. They conduct regular trainings on recognizing and preventing phishing attacks and other types of manipulation. These employees learn to identify suspicious messages and requests that may come from attackers impersonating managers, colleagues, or clients.

I would like to say a few words about

Cyber Backup Software

To solve complex problems, Softline experts offer Cyber Backup software. It allows you to create backup copies of the entire IT infrastructure, including your data, applications and operating systems. In the event of equipment failure, you can deploy a backup copy on any hardware platform in a matter of minutes. (Советов Н.Я., Яковлев С.А. 1990)

The advantages and key features of this software:

♦ Recover data and virtual machines on bare metal servers or heterogeneous hardware.

♦ Protection against ransomware attacks, keeping your data safe and secure.

♦ Reduced downtime with best-in-class RTO: moving data to the host in the background speeds up recovery by 2 times.

♦ One solution for all workloads: protect hypervisors, applications and clouds, over 20 operating systems, including Windows, Linux, as well as known OS, hypervisors and applications.

♦ Work with local, network and removable media and storage devices; deduplication and compression save up to 90% of storage capacity.

♦ Simplified and automated administration, instant protection in three clicks.

♦ Possibility of remote monitoring and recovery outside the host.

As an additional bonus, you will receive the following:

Domestic software product (Cyber Backup software is included in the Unified Register of Enterprises and has a version certified by FSTEC). Low cost of ownership, simple and flexible licensing without hidden payments. Regardless of your organization's IT infrastructure, Softline can offer a solution for its comprehensive, effective protection and rapid recovery, as well as train your employees in certified courses for users and system administrators. (Спортак М., Паппас Ф 2002)

In any case, when protecting private confidential information, competent work is required when virtualizing data.

Here it is important to understand the key criteria for choosing a virtualization system

The choice of a virtualization system is complicated by the variety of different solutions from international developers. This is partly due to the fact that the threshold for entering the market is low. You can build your own virtualization system based on open source code. And in the future, subject to a number of conditions, this product can be included in the corresponding Software Registry. It was assumed that over time the number of virtualization system developers would decrease by weeding out weak players in the market, but on the contrary, their number has only increased. New companies and products appear every now and then, virtualization ecosystems are expanding, and it is becoming increasingly difficult for the customer to choose the right solution.

It is important to consider that virtualization is the foundation around which most of the company's services are built. Therefore, having chosen an unreliable virtualization system, you can face many failures in the operation of services. There are key criteria here that will help you better understand the features of the virtualization systems available on the market and make an informed decision. (Степанов Е.А. Корнеев И.К 2001)

Hyperconverged virtualization system or classic?

Hyperconvergence allows you to build infrastructure in cases where the customer either does not have a common data storage system, or purchasing one is too expensive or impossible.

Which hypervisor to choose a virtualization system with?

The classic virtualization system is suitable for customers who can afford to purchase expensive equipment. Despite a number of advantages of hyperconvergence, classic systems still make up the majority of customer installations.

Ecosystem of solutions around virtualization

The virtualization layer, which is located on top of the hardware, is a kind of center around which a landscape of various additional products is built, capable of solving both basic infrastructure issues and issues of developing other IT products. Accordingly, the simplest ecosystem is when a solution can be delivered within the framework of a software and hardware complex, which is tested by the vendor and for the technical support of which it is responsible.

Other options for expanding the ecosystem around virtualization connecting some backup tool within the virtualization product or beyond it connecting VDI from the same vendor container management platform - when integration of various solutions within virtualization is required and it is important to have a single system capable of managing various types of virtualization from different suppliers, including both physical and cloud resources, in a single window mode with resource allocation, billing of these resources and other functions necessary for the efficient operation of the IT infrastructure. (Г. И. Назаренко, А.Е.Михеев, П.А.Горбунов, Я.И.Гулиев,

И.А.Фохт, О.А. Фохт,, 2014)

Built-in vs. external backup of a virtualization system

Almost all many developers of virtualization systems have a built-in backup with basic functionality, which implies the ability to create backup copies of virtual machines. However, it is often not enough. The built-in backup system allows you to create backup copies of 10-20 virtual machines without high requirements for the data that needs to be restored in the event of an accident. If the customer needs a full-fledged backup system for a larger number of virtual machines and with broader functionality, we recommend purchasing solutions from third-party manufacturers. The choice in this case depends on the virtualization platform. It is important that the external backup system is supported by the virtualization system manufacturer and is compatible with it.

Hardware resource requirements when choosing a virtualization system

The minimum set of hardware requirements depends on the type of virtualization. If we are talking about a classic infrastructure, only one server is enough. For a hyperconverged one, a minimum of 3 servers will be required, including disks.

If we are talking about a fault-tolerant configuration, which customers most often use so that virtual machines are not tied to only one server, then different vendors recommend different numbers of servers that are necessary for a fault-tolerant solution. The minimum number is 2 or 3 servers, depending on the vendor, and in rare cases 5 or more.

Usually, we recommend a certain type of virtualization and a minimum number of servers to the customer for the effective functioning of the information system. However, sometimes there are cases when the customer himself determines the required number of servers, this is especially typical for small businesses. For example, the customer may request the selection of virtualization for only two servers.

In conclusion of the above and having analyzed the state of information security of Azerbaijan, forms, methods, means of identifying and predicting possible threats, it is possible to note several recommendations developed, designed to facilitate the concentration of efforts of the security forces of our republic in the search for directions for improving the provision of information security of the state and the development of methods and ways to increase its effectiveness, including the development of the Concept of information security of our country.

Ensuring information security of our country includes, first of all, normative and legal regulation, ensuring unified legal, organizational, methodological approaches to the issue of developing cooperation in the framework of maintaining information security, as well as harmonization, unification and convergence of the legislation of Azerbaijan and friendly countries. (Степанов Е.А. Корнеев 2001)

According to experts, in modern geopolitical conditions, the security of the information space of our country meets the vital interests of the entire region and in the information sphere is one of the important areas of ensuring information security, which allows us to effectively counteract the destructive influence of unfriendly states.

Based on the results of the analysis and development of the material and in accordance with the competence of the experts and the area of responsibility, the following approaches to this issue are necessary:

♦ to implement legal registration of synchronization of the single technological space and scientific and technical programs of our country with the allied states to ensure information security with national plans for import substitution (import displacement) and their implementation;

♦ in order to reliably protect the digital and information space of Azerbaijan and our partners, create stable conditions for its development, stimulate and support research and investment, create new and modernize existing production capacities, adopt legal acts of the information alliance to form a unified system for organizing scientific research and effectively implementing its results, using the results of intellectual activity, training scientific and technical personnel;

♦ create common educational standards in the field of information security with agreed priorities, including uniform requirements for the training of specialists in this field within the framework of general interstate cooperation;

♦ enterprises and organizations - developers and manufacturers of software and hardware, other organizations and specialists of Azerbaijan dealing with information security issues, to take part in filling the Threat Data Bank of our country with information on vulnerabilities and threats in accordance with the approved Regulations, as well as in using information from this Bank in practical activities to protect information resources;

♦ take into account the information provided when making changes and additions to the National Security Concept of Azerbaijan;

♦ implement prompt counteraction by the information structures of Azerbaijan to the targeted negative information impact on the authorities and the population of the participating states from unfriendly countries, as well as from some national and nationalist mass media;

♦ ensure the adoption of effective measures to counteract the information expansion of foreign countries, including support by member states of international agreements regulating the global information exchange on an equal basis;

♦ begin creating a unified regulatory framework that combines national legal requirements and interstate interest in the functioning of the Internet, since through the development of a common set of legal, organizational and technical measures developed taking into account their possible adaptation to current cybersecurity risks, the necessary level of security of information systems can be ensured.

The implementation of the recommendations presented seems possible within the framework of the conceptual document of the Azerbaijani state in the field of information security, which defines both the definition and constituent concepts of “information security of the country”, as well as the forces and means, legal mechanisms, challenges, threats and risks, and priority areas for the development of information security. (Моисеев Н.Н., Иванилов Ю.П., Столярова Е.М. 1978)

Recommendations:

The privacy policy must be clear, accessible to all employees of the organization and regularly updated in accordance with changes in legislation and technological requirements. In addition to the Personal Data Processing Policy, other acts must also be adopted that regulate the rules for processing requests, archival storage, the depersonalization procedure, etc. In the event of a violation of the requirements of federal legislation and local acts of the organization when processing personal data, the guilty person bears civil, disciplinary, administrative or criminal liability.

Basically, organizational and technical measures for information protection are distinguished.

Organizational measures include:

♦ development of local acts regulating all issues and procedures for processing personal data in a specific organization;

♦ monitoring the measures taken to ensure the security of personal data and the level of protection of information systems;

♦ training employees in information security, working with personal data and the rules of "digital hygiene";

♦ registration of carriers of confidential information;

♦ appointment of persons responsible for the process of processing personal data.

Technical measures for protecting personal data

Technical measures for protecting confidential information include the following:

♦ use of certified information security tools — antivirus programs, firewalls, access control systems, etc.;

These measures help protect personal data from access by third parties, hacking and theft, and also comply with legal requirements for the protection of personal data. (Костровский З., Попов С. 2010)

REFERENCES

In English

1. Anshina M.J.L., *Tsymbal A.A. Technologies for creating distributed systems*. For professionals. - SPb.: "Piter", 2003. - 576 p.

2. Beketov N.V. *Problems of formation and prospects of development of the regional telecommunication system* // Informatization of society, 2003, issue. 2, pp. 38-40.

3. Black Yu. *Computer networks: protocols. Standards, interfaces*. / Translated from English. - M.: Mir. 1990.-510 p.

4. Broydo B.J.I. *Computing systems, networks and telecommunications*. SPb.: Piter, 2002. 688 p.

5. D. B. Baker, *"Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety,"*Computer Security Applications Conference, 2006.http://www.himss.org/files/HIMSSorg/content/files

6. M. A. Ameen, J. W. Liu, K. Kwak, *"Security and privacy issues in wireless sensor net-works for healthcare applications,"* Journal of Medical System, vol. 36, no. 1, pp. , 2012

7. L. O. Gostin, J. G. Hodge, "*Personal privacy and common goods: A framework for balancing under the national health information privacy rule,*" Minnesota Law Review, vol. 86, pp. 1439-1449, 2002.

8. S. Brands. "*Privacy and security in electronic health.*" http://www.credentica.com/ehealth.pdf 2015

9. Davis D., Barber D., Price W., *Solomonides S. Computer Networks and Network Protocols*. M.: Mir, 1982. 562 p.

10. Simonsen.T. Review: *Internet Providers* // Delovoy Kvartal, 37, 2008.

11. Kaluts JI.A., Sushchansky *V.I. Transformations and Permutations* M., Nauka. Main Editorial Board of Physical and Mathematical Literature, 1985. -160 p.

19. Kaluts JI.A., Sushchansky V.I. *Transformations and Permutations* M., Nauka. Main Editorial Board of Physical and Mathematical Literature, 1979. -112 p.

13. Kleinrock JI. *Computing Systems with Queues*. Translated from English. Ed. by B.S. Tsybakov.- M.: Mir. 1979. 600 p.

In Russian

14. А. А. Абдуманонов, М. К. Карабаев, *"Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе Externet,"* Программные продукты и системы. №1, стр. 150-155, 2013.

15. Короткченко А.В. *Формирование и реализация государственной политики в сфере региональной информатизации* // Информационное общество. 2003, вып.2, с. 18-21.

16. Костыченко В. Обзор: *Интернет провайдеры* // Деловой квартал, 2, 2008.

17. Костровский З., Попов С. «*Большая тройка» операторов связи*: защита персональных данных // Information Security/ Информационная безопасность. 2010 (электронное периодическое издание).

18. Корман А.,. *Методы и модели исследования операций*. М.: Мир, 1977. - 432 с.

19. Кристолапов Т. *Теория графов. Алгоритмический подход*. Мир, М.: 1978. 432с.

20. Кульманов М. *Технология корпоративных сетей*: Энциклопедия. СПб.: Изд-во «Питер», 2000. 512 с.

21. Липунов Г. *Практика внедрения систем защиты персональных данных* // Information Security/ Информационная безопасность. 5, 2009 (электронное периодическое издание).

22. Маевский Т. *Алгоритмы оптимизации на сетях и графах.* : Пер. с англ. М.: Мир, 1981.-323 с.

23. Мартин Дж. *Организация баз данных в вычислительных системах*. М.: Мир, 1980. 664 с.

24. Мартин М. *Введение в сетевые технологии*.- М.: Лори, 2002. 659 с.

25. Мейер Д. *Теория реляционных баз данных*. М.: Мир, 1987. 608 с.

26. Мельниченко С.Б. *Информационная безопасность и защита информации.* Под. ред. С.А.Клейменова. М.: Издательский центр «Академия», 2008. -336 с.

27. Миленков Ю.В. *Защита от несанкционированного доступа в специализированных информационных системах.* Казань, 1999.- 199с.

28. Моисеев Н.Н., *Иванилов Ю.П., Столярова Е.М. Методы оптимизации.* М.: Наука, 1978.-352 с.

29. Моисеенко Л.Т. *Математические задачи системного анализа.* М.: Наука, 1981.-488 с.

30. Назарович О. *МВ Технические решения создания сетей.* Горячая линия-Телеком, 2000. 376 с.

31. Нейман В.И. *Структуры систем распределения информации.* М.: Связь, 1975. 264 с.

32. Никитский Г.В., *Классификация информационных систем // Качество.* Инновации. Образование., 6, 2010. С. 64 70.

33. Николаев В.И., *Брук В.М. Системотехника: методы и приложения.* Л.: Машиностроение, 1985. - 199 с.50.0безличивание персональных данных, wiki.kint.ru.

34. Олифер В.Г., *Новые технологии и оборудование 1Р-сетей*. СПб.: БХВ-Санкт-Петербург, 2001. 512с.54.

35 . Партыка Т.Л., *Попов И.И. Информационная безопасность*. М.: Инфра-М, 2002.-368 с.

36. Петровский С.П., *Информационная безопасность человека и общества*. М.: Энас, 2007. 336 с.

37. Пятибратов А.П., *Вычислительные системы, сети и телекоммуникации*. М.: Финансы и статистика, 2001.- 512 с.

38. Ретана А., Слайс Д., Уайт Р. *Принципы проектирования корпоративных 1Р-сетей*.: Пер. с англ. М.: Издательский дом «Вильяме», 2002. - 368 с.

39. Риордан Дж. *Вероятностные системы обслуживания*. М.:Связь. -1966. -184 с.

40. Рябкова У.С. *Об обезличивании персональных данных* Информационная безопасность. 5, 2009 (электронное периодическое издание).

41. Саати Т.А. *Элементы теории массового обслуживания и ее приложения*. М.: Сов. Радио. 1971. - 520с.

42. Садовский В.Н. *Основания общей теории систем*. М.: Наука. 1974. -280 с.

43. Саксонова П.Н., *Шаумдин Н.З. Центры обработки персональных данных* // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций. Материалы 16 международной научно-технической конференции. Рязань, 2010. С. 158 160.

44. Саксонова П.Н., *Шаумдин Н.З. Анализ проблемы обезличивания персональных данных* // Межвузовский сборник научных трудов. Математическое и программное обеспечение вычислительных систем. Рязань, 2011.С. 118-126.

45. Саксонова П.АН., *Шаумдин Н.З. Процедура обезличивания персональных данных* // Наука и образование: электронное научно-техническое издание. 3, 2011. Эл № ФС 77 30569. Государственная регистрация №0421100025. ISSN 1994-0408.

46. Семенов Ю.А. *Сети Интернет. Архитектура и протоколы*. М.:, изд. "Сирин". 1998. -424 с.

47. Советов Б.Я. *Моделирование ИС. М.*: Высшая школа. 1995. 372 с.

48. Советов Б.Я., *Яковлев С.А. Построение сетей интегрального обслуживания*. Д.: Машиностроение. 1990. 332 с.

49. Спортак М., Паппас Ф. и др. *Компьютерные сети и технологии сети*, ДиаСофт. 2002.-736 с.

50. Степанов Е.А. *Корнеев И.К. ИБ и протекция информации*. М.: ИНФРА-М. 2001. - 304 с.

51. Г. И. Назаренко, А.Е.Михеев, П.А.Горбунов, Я.И.Гулиев,

И.А.Фохт, О.А. Фохт, “*Особенности решения проблем информационной безопасности в медицинских информационных системах*. 2014 http://www.interin.ru/datas/documents/pib.pdf