Practical work 1

Topic: Developing an access control clause in an information security policy for an organization.

Job objective: to gain the skills to develop an organization's information security policy.

Theoretical part

Information protection should ensure the prevention of damage caused by the accidental loss of information. Information protection measures should be organized on the basis of current laws and regulations on information security and in the interests of information users. To ensure a high level of information protection, it is necessary to regularly solve complex scientific and technical problems and improve protection tools. Information security policy involves the systematic use of technical means aimed at ensuring confidentiality.

A security policy is a high-level document or set of documents that describes the security controls implemented to protect an organization .

Security policies maintain confidentiality, usability, integrity, and asset value.

Without a security policy, it is impossible to prevent an organization from potential criminal activity, loss of profits, and bad publicity. However, that security policy does not address the underlying security attacks.

Advantages of security policies:

- enhanced information and network security;
- reduce risks;
- monitoring and control of device usage and data transfer;
- high network performance;
- rapid response to problems and less downtime;
- reduced stress levels in management;
- cost reduction;
- The main stages of ensuring security are as follows;
- determining the importance of the enterprise's information and technological assets;
- determine the level of security for each asset, as well as the risk of threats to the assets that cost-effective security measures will pose for each asset;
- attracting the necessary financial resources to ensure the security policy, as well as purchasing and configuring the necessary security equipment;
- Strictly monitor the phased implementation of the security plan, as well as take into account changes in external factors, further modifying the necessary security methods;
- Conducting explanatory work for employees and other responsible personnel.

Security policy features:

- short and clear;
- to be useful;

- to be understandable;
- to be practical;
- to be stable;
- to be mentally resilient;
- be economically justified;
- Must comply with cyber and legal laws, standards, regulations, and instructions.

The main stages of policy development are:

- creating a sufficient team to formulate policies;
- resolve questions about features that arise during the development process;
- address questions about the scope and purpose of the policy;
- resolve questions about the persons responsible for the creation and implementation of this document.

Security policy development - is a joint or collective operation of the entire organization that is affected by the organization's rules. In general, a security policy should not be developed by the IT team, as everyone involved in the security policy should be involved in its development.

Security policies can be informative, regulatory , and advisory, generally falling into the following categories:

• Physical security: This requires both employees and management to understand what safeguards are in place to protect physical assets, including doors, entry points, surveillance, alarms, and more.

• Employee management: they need to tell their employees how to conduct or manage their daily activities securely, such as password management, confidential information security , etc.

• Hardware and Software: It shows the administrator what type of technology to use, what network management should be done and how it should be configured, and is applicable to system and network administrators.

Practical part

Below is an example of an information security policy for an organization that manages access to a credit center.

CREDIT CENTER
INFORMATION SECURITY POLICY

Table 1.1

Contract sheet

No.	**Position**	**Name and surname**	**signature**
1.	Head of Legal Department	Music by A.Ch.	
2.	Head of Automation Department	Avilkin I.A.	
3.	Head of Network and Information Security Department	Shaptsov V.E.	
4.	Acting Head of Internal Control Service	Striganina O.S.	

TABLE OF CONTENTS

General concepts

1.1. The information security policy of the issuing enterprise “Credit Center” is developed in accordance with the legislation of the Russian Federation and the legal norms of information security, the requirements of regulatory documents of the Central Bank of the Russian Federation , the authorized federal executive body in the field of security, the authorized federal executive body in the field of countering technical intelligence and technical protection of information. General rules and recommendations of the Bank of Russia in the field of standardization Ensuring information security of organizations of the banking system of the Russian Federation . 100 Methodological recommendations on documents on ensuring information security in accordance with the requirements of AXTT -1.0 (RF AXTT -2.0-2007).

1.2. The policy is a high-level document that defines the overall goals and objectives of the bank, including methods for monitoring the implementation of policy requirements. The policy defines the content, objectives and requirements of the bank's information security activities .

1.3. The policy is a convenient document for bank employees and customers, and represents the officially adopted position of the bank's management on the issues of ensuring the bank's information security, building information security. The policy must be applied by all employees and bank management, as well as users of bank information resources.

1.4. and norms regulating banking activities , as well as the development of implemented banking technologies and the prospects of bank customers and other stakeholders. Compliance with information security requirements allows the bank to create competitive advantages, ensure its financial stability, compliance with legal, regulatory and contractual requirements.

1.5. The Bank is the owner of documents, information systems, technologies and means of their provision, produced at its expense, legally purchased, received by gift, inheritance or in any other legal way.

1.6. The Bank, as the owner of information resources, information systems, technologies and means of their provision, fully exercises the powers to own, use and dispose of these objects and determines the conditions for the use of these products.

1.7. The Bank, as the owner of information constituting a commercial secret of the Bank, has the right to sell and resell it as a commodity to other legal entities and individuals, provided that this transaction does not contradict the obligations of the Bank, does not violate the rights and does not harm the Bank, its employees, clients or correspondents.

1.8. In the course of banking activities , there is a risk of unauthorized access and use of information that is the property of the bank , which may result in material, moral or other damage to the bank, its customers and correspondents.

1.9. prevent threats and eliminate their consequences.

1.10. Specific policies detailing the provisions of this policy relating to various areas of information security are formalized in the form of separate internal regulatory documents of the bank.

I. Terminology and definitions

Automated banking system - an automated system that implements the technology for performing banking functions.

An asset is anything that is of value to the bank and is at its disposal.

Bank information security audit is a periodic, independent and documented process for obtaining audit certificates and objectively assessing them in order to determine the level of compliance with established requirements for ensuring information security by the bank.

Banking technological process - a technological process that performs operations to change and (or) determine the state of assets used in the implementation of banking activities or necessary for the implementation of banking services .

Bank information technological process - a part of the bank's technological process that performs operations to change and (or) determine the status of information assets that are necessary for banking activities and that do not contain payment information.

Bank payment process – a part of the banking process, associated with the implementation of banking operations on the bank's information assets , the transfer of funds from one account to another and (or) the control of these operations.

Information - messages, regardless of the form of presentation of data.

Information asset - information with details that allow it to be identified; important for the bank.

Personal data information system - a set of personal data contained in a database , as well as an information system that allows processing such personal data using automation tools or without the use of such tools.

Bank information security is the state of protecting the interests (goals) of the bank in the face of threats in the information sector.

An information security incident is an event that indicates that a threat has been or may be implemented .

Classification of information assets - the division of the bank's existing information assets by type , carried out in accordance with the degree of severity of the consequences arising from the loss of their important characteristics.

Bank information security monitoring (BAX monitoring) – continuous monitoring of BAX monitoring events, collection, analysis and generalization of monitoring results.

Information security policies are documents that define the high-level goals, content , and main directions of the bank

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

Risk is a measure of the probability of a threat occurring and the amount of harm (loss) from the realization of this threat.

Information security breach risk – information security breach risk – the risk associated with an information security threat.

A bank's information security self-assessment is a systematic and documented process for obtaining self-assessment certificates for ensuring information security in banking activities and determining the level of fulfillment of the information security self-assessment criteria in the bank.

Information security system - protective measures, means of protection and processes for their use, including resource and administrative (organizational) support.

Information security management system - a part of bank management designed to create, implement, use, monitor, analyze, support and improve an information security management system.

Information security system - Bank AXT and AXBT Society.

Loss - loss of assets, damage to assets and (or) infrastructure.

Other damage to the bank or the bank's assets and (or) infrastructure occurred as a result of the implementation of information security threats through information security vulnerabilities.

A threat is a risk with the possibility of loss (damage) .

Information security threat – the risk of violating the information security features of the availability, integrity, or confidentiality of the bank's information assets.

II. Symbols and abbreviations

ABT -automated banking system.
AX -information security.
ShMAT- personal data information system.
RK -unauthorized access.
BVDBH - actions defined within the scope of the delegated powers.
Personal information.
RF -Russian Federation.
ISMS - information security management system.
AXT - information security system.
ISSS - information security management system.
FXX -Federal Security Service.
TENBFX -Federal Service for Technical and Export Control.
EXM -electronic calculating machine .

III. Preliminary conceptual scheme for ensuring bank information security

4.1 The conceptual scheme of the Bank's information security is aimed at protecting its information assets from threats arising from illegal actions of attackers, reducing risks and potential damage from accidents, employee

misconduct, technical failures, incorrect technological and organizational solutions in the processes of processing, transmitting and storing information, and ensuring the normal operation of technological processes.

4.2 The greatest potential for harm to the bank lies with its own employees. The actions of employees may be malicious (the attacker may have accomplices inside and outside the bank) or may be of a purely negligent nature. The risk of accidents and technical failures is determined by the condition of the technical fleet, the reliability of energy supply and telecommunications systems, the qualifications of employees and their ability to adequately act in an abnormal situation.

4.3 To combat information security threats in the bank, a predictive model of suspected threats and an offender model are created based on existing experience. The more accurate the forecast (the threat model and offender model are created), the lower the risk of information security breaches in the bank.

4.4 An information security policy developed based on the forecast and in accordance with it is the most appropriate and effective way for the bank to achieve minimization of the risk of information breaches. The bank periodically updates threat and offender models based on monitoring and audit data.

4.5 Compliance with information security policies is primarily an element of corporate ethics, therefore, the bank pays serious attention to issues of managing relationships between the team, co-owner or owner.

4.6 The "Credit Center" credit center is a structural unit responsible for ensuring information security, which is tasked with implementing the information security policy developed by the management and owners, coordinating information security management processes, and identifying and preventing information security incidents.

4.7 Bank employees shall comply with the requirements of the current legislation of the Russian Federation and the bank's internal documents on information security, and shall also inform their immediate superiors of all events related to information security violations (which may lead to violations). The head of a structural unit at any level shall comply with the requirements of the current legislation of the Russian Federation and the bank's internal documents, and shall also monitor the implementation of such requirements by employees of his units.

4.8 The Bank's information security strategy consists of effective use and regular review of IT models and policies and correction of IT security in accordance with a pre-developed information security plan against attacks by attackers.

4.9 The basis for building an AML bank is the requirements of the legislation of the Russian Federation , regulatory documents of the Bank of Russia , contractual requirements of the bank, as well as business conditions expressed on the basis of identifying bank assets, creating a model of offenders and threats.

VI. Goals and objectives of information security

5.1 The main purpose of information security is to ensure the stable operation of the bank and protect information assets of the bank, its shareholders,

investors and customers from accidental (incorrect) and unlawful attacks, disclosure, loss, leakage, corruption, modification and destruction of protected information.

5.2 *The main tasks of ensuring information security in the Bank are:*

- prevention of leakage, theft, loss, corruption, falsification of information;
- prevention of threats to personal security;
- prevention of unauthorized actions to destroy, modify, damage, copy, or block information;
- prevent other forms of unlawful interference with information resources and information systems;
- ensuring the legal status of documented information as an object of property;
- protection of citizens ' constitutional rights to maintain the privacy of their personal information and the confidentiality of personal data contained in information systems.

5.3 Organizational, technological and technical measures to protect information in the Bank are implemented in accordance with the requirements of the current Legislation, TENFX, FAX, regulatory and methodological materials of the Central Bank of the Russian Federation (Central Bank of the Russian Federation) and organizational and administrative documents of the Bank on ensuring information security.

VI. Protection of facilities

6.1 *The main objects of protection in the bank are:*

- other information resources constituting commercial, banking secrets, sensitive to accidental and unauthorized influences and violating their security, including open (open) data carriers presented in the form of documents and information arrays, regardless of the form and type of presentation);
- information technology, procedures for collecting, processing, storing and transmitting information, bank employees;
- information , technical and software means for its transmission, storage, processing and display, including information exchange and telecommunication channels, information protection systems and means.

VII. Threats to bank information security

7.1 In order to successfully implement measures to secure a bank, it is necessary to understand the potential threats to it.

7.2 Threat and attacker models (AS forecast) are crucial in deploying, maintaining, and improving a bank's security system.

7.3 The activities of the bank are supported by its information infrastructure, which ensures the implementation of banking technologies and can be presented as a hierarchy of the following main levels:

- physical (communication lines, hardware, etc.);
- network (network hardware: routers, switches, hubs, etc.);

- network applications and services;
- operating systems (OS);
- database management systems;
- banking technological processes and applications;
- bank's business processes.

may include disrupting the operation of a bank’s business processes by, for example, compromising the availability or integrity of information assets, such as by distributing malware or by violating the rules for using computers or their networks .

7.5 The following are considered the main sources of threats to the Bank :

- External information security violators (former bank employees), representatives of organizations that interact with the bank on issues of technical support, bank customers, visitors to bank premises and buildings, competitors, terrorists and criminal organizations, hackers;
- internal information security offenders (registered users of the banking system, service employees, administrators, information security managers, etc.);
- common threat sources: external and internal, acting together and/or acting together);
- interruption, rejection, destruction/damage of software and hardware;
- dependence on suppliers/providers/partners/customers;
- supervisory and regulatory authorities and applicable legislation.

VIII. Bank's information security system

8.1 Compliance with information security requirements serves as the basis for ensuring the proper level of security.

8.2 The Bank's information security system is designed for several regions of the Bank.

8.3 *Ensure information security when assigning and distributing trust roles to employees :*

- hiring , the identity of the person, the declared qualifications, the accuracy and completeness of biographical facts, and the availability of recommendations are checked;
- bank employees correspond to the tasks performed. The qualifications of employees are ensured through information security training processes, regular checks of the level of employee awareness and competence;
- all bank employees provide a written commitment to comply with confidentiality, corporate ethics, including the requirements for preventing conflicts of interest;
- external organizations are regulated by the rules included in contracts (agreements).

IX. Bank's information security management system

includes the deployment, implementation and improvement of the AX management system, which is a coordinated system of activities for the management and control of the bank.

9.2 The scope of application of information security rules to information resources is determined based on the classification of resources. At the same time, the composition (list) of information assets and their significance, as well as the continuity of banking processes, are mandatory.

9.3 The distribution, implementation and use of AXTM is carried out by the Network and Information Security Department.

9.4 Planning – Implementation – Review – Improvement – Planning:

9.5 The main processes related to the ACM are being implemented in the Bank:

- With planning processes to fulfill AX requirements;
- implementation and use of protective measures;
- With the verification of processes for fulfilling AX requirements;
- Improving processes for fulfilling AX requirements.

X. Procedure for implementing and reviewing the information security policy

10.1 This policy is approved by the bank's management.

10.2 Reasons for revising the policy may include:

- Information security bank policy changes;
- Changes in the current legislation of the Russian Federation , as well as industry standards in the field of ensuring the functioning of the Bank of Russia .

10.3 This policy should be reviewed at least every three years.

XI. Responsible persons

11.1 Violations related to non-compliance with local regulations on ensuring bank security are divided into two groups depending on the level of risk:

- violations that led to the onset of unnecessary consequences for the bank (information leakage or destruction);
- which could lead to unnecessary consequences for the bank (threat of destruction or loss of information).

11.2 Violation of the requirements of the bank's local regulatory documents on bank collateral is an extraordinary event and entails the consequences stipulated by the current legislation of the Russian Federation , local regulatory documents, agreements concluded between the bank and employees, and agreements concluded between the bank and counterparties.

11.3 The level of liability for violation of the requirements of local regulatory documents in the field of banking is determined based on the amount of damage caused to the bank.

11.4 This policy applies to all counterparties, employees and bank officials.

11.5 Managers at all levels are personally responsible for complying with the provisions of this policy and maintaining the level of AX in the units under their control.

each employee of the bank who has access to information constituting a commercial secret and who has allowed its leakage, is responsible for the disclosure of confidential information.

11.7 For disclosure of confidential information, loss of media containing such information, as well as other violations in handling confidential information, perpetrators are held liable up to and including dismissal .

11.8 Types of liability provided for in certain federal laws on the management of restricted information:

- civil liability;
- disciplinary liability;
- administrative responsibility;
- criminal liability.

may be held criminally liable in accordance with the current legislation of the Russian Federation for disclosure of information constituting banking secrecy (Article 183 of the Criminal Code of the Russian Federation).

Assignment

In the table below, the student develops an information security policy based on the options listed in alphabetical order.

Option number	Institutions
1.	Commercial bank branch
2.	Polyclinic
3.	College
4.	Insurance office
5.	Recruitment agency
6.	Online store
7.	State Services Agency
8.	Internal Affairs
9.	Auditing company
10.	Design firm
11.	Internet provider
12.	Advocacy
13.	Real estate agency
14.	Travel- agency
15.	Charity fund
16.	Publisher
17.	Consulting firm
18.	Advertising agency
19.	Tax Committee
20.	Notary office
21.	Scientific and design enterprise
22.	Civil Registry Office
23.	Newspaper editorial office
24.	Hotel
25.	Travel company
26.	City archive
27.	Taxi dispatch service
28.	Railway ticket office
29.	Contact Bank Branch
30.	State Testing Center

Control questions

1. What is information security?
2. What do you understand by information security policy?
3. What do you mean by usage management?

used literature

1. https://ipb.ru/doc/about/%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%2022.04.2016.pdf (accessed 8.01.22).
2. https://www.ccb.ru/download/doc/ITSec.pdf (accessed : 8.01.22).