Chemical Technology, Control and Management

Volume 2019
Issue 4 *SPECIAL ISSUE 4-5*

Article 10

10-26-2019

Ensuring Information Security By Multi-Criterial Restriction Of Access To Information Resources

A.I. Dusmuxamedov
State customs Committee, Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan, +99897-422-30-33;, alisher1511@mail.ru

T.T. Abduraxmonov
State customs Committee, Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan, Phone: +998 933946479;, abdutohir@gmail.ru

A.A. Saidov
State customs Committee, Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan, Phone: +998 998177303., sobirs59@mail.ru

Ensuring Information Security By Multi-Criterial Restriction Of Access To Information Resources

Cover Page Footnote

Tashkent State Technical University, SSC «UZSTROYMATERIALY», SSC «UZKIMYOSANOAT», JV «SOVPLASTITAL», Agency on Intellectual Property of the Republic of Uzbekistan

Erratum

??????

ISSN 1815-4840
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2019, №4-5 (88-89) pp.151-158
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

UDC 519. 718+ 35.085.6

ENSURING INFORMATION SECURITY BY MULTI-CRITERIAL RESTRICTION OF ACCESS TO INFORMATION RESOURCES

A.I.Dusmuxamedov[1], T.T.Abduraxmonov[2], A.A.Saidov[3]

[1]*State customs Committee*
Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan
E-mail: alisher1511@mail.ru; +99897-422-30-33;
[2]*State customs Committee*
Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan
E-mail: abdutohir@gmail.ru, Phone: +998 933946479;
[3]*State customs Committee*
Address: 3 I. Karimov st., 100003, Tashkent city, Republic of Uzbekistan
E-mail: sobirs59@mail.ru, Phone: +998 998177303.

Abstract: *The problems of ensuring information security of information systems of state bodies are considered. The analysis of possible threats from "insiders" against which technical methods of the solution of this problem are recognized not effective is carried out. The main object of the study is the information resources of state bodies and the process of monitoring the actions of employees who have access to them. The method of multi-criteria restriction of access to information resources in the form of conditions of horizontal and vertical restrictions for users of information systems is offered.*

Key words: *information systems of state bodies, information security pyramid, "insiders", users of information systems, horizontal and vertical information security conditions.*

Аннотация: *Давлат органларининг ахборот тизимларининг рассматриваются ахборот хавфсизлигини таъминлаш масалалари кўриб чиқилган. Ушбу муаммони ечишда техник усулларнинг самарасиз бўлган «инсайдерлар» томонидан йўл қуйилиши мумкин бўлган таҳдидларнинг таҳлили ўтказилган. Тадқиқотнинг объекти бўлиб давлат органларининг ахборот ресурслари ва улардан фойдалана оладиган ходимлар ҳаракатининг мониторинги жараёни ҳизмат қиладилар. Ахборот тизимлари фойдаланувчилари учун горизонтал ва вертикал чекловлар шарти сифатида ахборот ресурслардан фойдаланишга кўп мезонли чекловларни ўрнатиш усули таклиф этилган.*

Таянч сўзлар: *давлат органларининг ахборот тизимлари, ахборот хавфсизлиги пирамидаси, «инсайдерлар», ахборот тизимлари фойдаланувчилари, ахборот хавфсизлигининг горизонтал ва вертикал шартлари.*

Аннотация: *Рассматриваются задачи обеспечения информационной безопасности информационных систем государственных органов. Проводится анализ возможных угроз со стороны «инсайдеров», против которых технические методы решения данной проблемы признаны не эффективными. Основным объектом исследования являются информационные ресурсы государственных органов и процесс мониторинга действий сотрудников, имеющих доступ к ним. Предлагается методика многокритериального ограничения доступа к информационным ресурсам в виде условий горизонтальных и вертикальных ограничений для пользователей информационных систем.*

Ключевые слова: *информационные системы государственных органов, пирамида информационной безопасности, «инсайдеры», пользователи информационных систем, горизонтальные и вертикальные условия информационной безопасности.*

Introduction.

In 2018, a number of policy documents of the Republic of Uzbekistan were adopted on the development of information and communication technologies, the introduction of electronic government, the formation of the information society and the digital economy. In particular, in the Decree of the President of the Republic of Uzbekistan "On measures to further improve the field of information and communication technologies" No. PP-3832 dated February 19, 2018 and the Decree of the President of the Republic of Uzbekistan No. UP-5349 dated July 3, 2012 "On measures for the development of digital of economy in the Republic of Uzbekistan "the development vectors of this direction are identified that meet modern requirements.

We can say with confidence that at present there are practically no ministries or departments of the Republic of Uzbekistan under which a separate decree or resolution of the President of the Republic of Uzbekistan on introducing modern information technologies into their activities would not be adopted.

At the same time, given the relevance of the task of creating information systems and electronic databases for various sectors of the economy, covering a wide range of public services, ministries and departments make decisions on the creation and implementation of information resources using various technical and technological platforms. This poses problems of ensuring information security in the integration of these resources at the state level.

In Decree of the President of the Republic of Uzbekistan dated February 19, 2018 No. 5349, this issue is defined as a "*systemic problem*" and emphasizes that: "*poor organization of work to ensure information security and information protection in state information systems and resources increases the possibility of unauthorized access to information, violations database integrity and confidentiality*."

As a solution to the problem, this directive adopted a decision on the need for "*comprehensive measures to ensure cybersecurity and the introduction of modern technologies for protecting networks, software products, information systems and resources, participation in the regulation of the application of technologies for the collection, processing and storage of personal and biometric data* " [1].

The implementation of comprehensive measures to ensure cybersecurity and the introduction of modern technologies for protecting networks, software products, information systems and resources of government bodies includes several interrelated tasks. At the State Customs Committee, comprehensive measures to ensure cybersecurity are implemented in the form of an 8-layer "*Information Security Pyramid*" [2]. At the top of this pyramid is a "*user*" who is granted access to information resources. (Fig. 1.). Users of information systems are the most vulnerable points of information security, and for them separately adopted technical solutions do not give effective results.

In view of the foregoing, it is necessary to apply a systematic approach to working with users of information systems, and the task of developing multicriteria restrictions on access to information resources in the form of special conditions for ensuring the information security of state bodies is relevant.

Main part.

As noted above, users of information systems are the most vulnerable points of information security. A special category of users includes those who are offended for any reason by existing or former customs officers or employees from organizations that develop special software, telecommunication interaction tools and systems. Knowing the characteristics of the software, the organization of its development, owning the means of its modification and having access to it, they are able to introduce various kinds of software bookmarks into it. These can be software developers, operating personnel, special services, terrorist elements, external subscribers, hackers and others [8].

Violators of this class can be classified as follows:

1st level - an external intruder or a group of external intruders, independently creating methods and means of implementing threats, as well as realizing threats (attacks);

2nd level - an internal violator who is an official or employee of the customs authorities, but who is not allowed to work at the information security facilities of the customs authorities independently carries out the creation of methods and means of implementing threats, as well as implements threats (attacks);

Level 3 - an internal violator who is an official or employee of the customs authorities who is allowed to work at the information security facilities of the customs authorities to independently create methods and means of implementing threats, as well as implement threats (attacks);

4th level - a group of violators that creates methods and means of implementing threats, as well as implements them with the involvement of individual specialists with experience in developing and analyzing information security tools used at information security facilities of customs authorities;

Level 5 - a group of intruders that creates methods and means of implementing attacks, as well as implements attacks with the involvement of research centers specializing in the development and analysis of information security tools;

6th level - special services of foreign countries, implementing the creation of methods and means of implementing threats, as well as implementing them with the involvement of research centers specializing in the development and analysis of information protection tools [6].

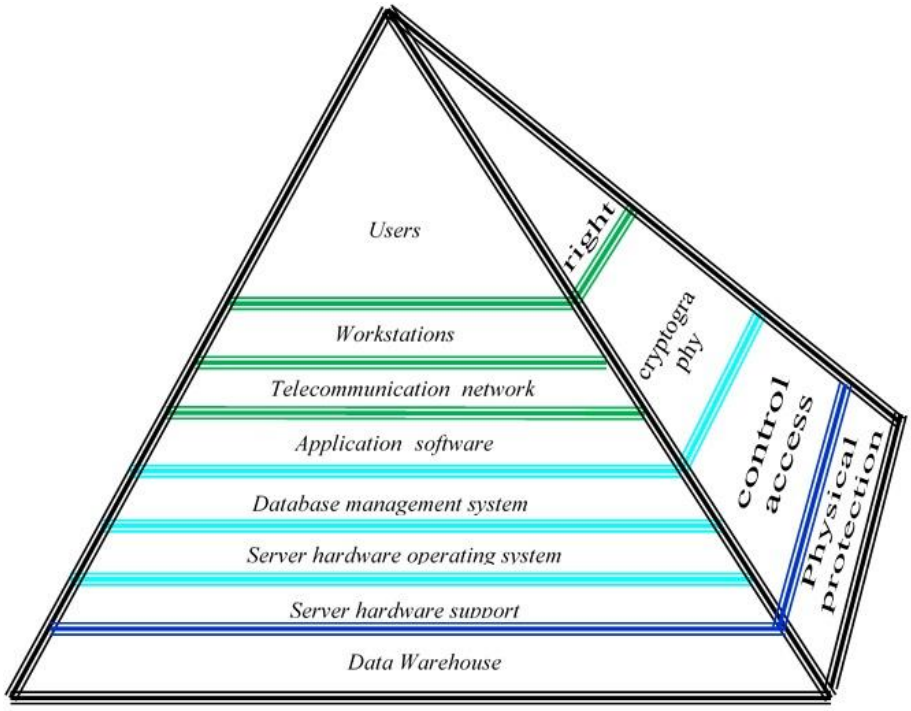

Fig. 1. ***"The pyramid of information security".***

It should be noted that non-compliance with information security requirements of information systems of private companies can lead to failure of business plans or bankruptcy of the company. However, such actions by “client” companies authorized to use the state’s information systems flagrantly violate laws and may damage the state’s economic security[3].

To date, large-scale studies have been conducted to study the activities of users of information systems that do not meet the requirements of information security, and they are called "insiders" in the scientific literature [3-5].

1. Conditions for protecting information resources from insiders.

The term "insider" is an English term and has different interpretations in different sources. In general, this means "a member of a group of people who have access to information publicly available to the public" [3]. From the point of view of information security, an “insider” is understood as an

employee who has access to the enterprise's information network and gets access to confidential information. Generally speaking, an insider is understood as the director or senior manager of the enterprise, as well as citizens with a share of at least 10 percent of the shares of the enterprise. However, it is possible that those who are not responsible for their work are secretaries, employees with bad intentions or those specially trained to steal information.

Insiders are usually divided into four groups: "Obedient servants", "Troublemakers", "Criminals", "Mole traitors" [4].

"Obedient employees" are loyal employees who rarely violate company policies and do not endanger security. At the same time, according to statistics, 80-90% of all data that is damaged or damaged by information security is due to their negligence or neglect.

"Troublemakers" can be top managers or company executives. They allow you to violate information security requirements yourself - to play computer games, make purchases on the Internet and use personal emails on business matters. Such insiders can undermine information security with their own carelessness, but their actions, as a rule, are unplanned and unintended, taking into account special interest. Nevertheless, it is necessary to remember, in many cases, external attacks on information systems can occur by e-mail of these employees.

"Criminals" are those who engage in activities that do not require much of the work day. As a rule, these are senior officials, top managers who have access to the Internet and have the right to install and use their own programs without permission on the computer. In addition, such employees may send confidential information to other interested customers or modify them to their advantage. Insiders in this class pose a serious threat to information security.

"Moles are traitors" are usually employees who knowingly and regularly steal confidential information from the financial accounts of interested parties. Such personnel are the biggest threat to information security, and they are difficult to capture because they are often very experienced users who muddle their tracks. Such users of information systems are compared with the name of a mammal known as the Mole, 12-13 cm in diameter, which is a source of infectious diseases.

According to research conducted by the Russian SearchInform, the majority of information thieves - line managers - and middle managers (31%). After that, top managers accounted for 19% (Fig. 2.) [5].

In general, the violation of information security should be avoided and prevented to users of the information system, regardless of which group they belong to, and the danger that they may face. At the same time, such measures should not create difficulties for "honest" users of information systems and, therefore, should not seriously undermine the effectiveness of such systems.

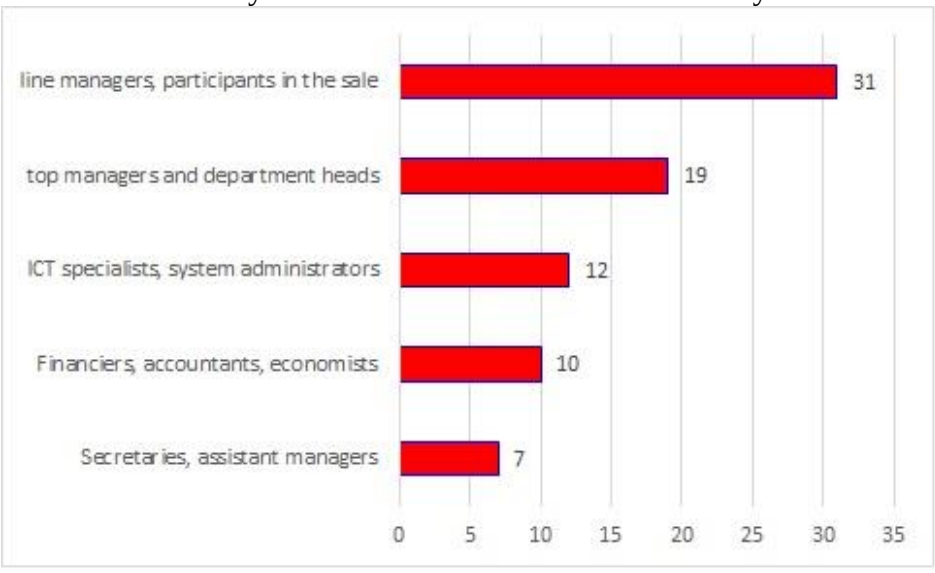

Fig. 2. ***Percentage of "probable insiders" representing a threat to information security.***

Taking this into account, the following priority areas of information security should be taken into account when developing and implementing information systems:

- the ability for users of the information system to receive the necessary information in real time in full and without any difficulties;
- integrity, reliability, relevance of information, protection against external influences and protection against unauthorized access and modification;
- protection of information from illegal transmission of information.

Despite the fact that there are no guaranteed technical solutions for users of information systems that prevent their threat to information security, a number of conditions can be created to protect the database or prevent theft or alteration of information. The following is an incomplete list of conditions for protecting information from "insiders":

1. User identification: digital signature;
2. User authentication;
3. User authorization;
4. Delineation by territorial affiliation;
5. Differentiation of functional responsibilities;
6. Separation according to the area of responsibility of the user;
7. Monitoring and analysis of user risks.

These conditions, in turn, form a pyramid of conditions for the “client” of information systems (Fig. 3.).

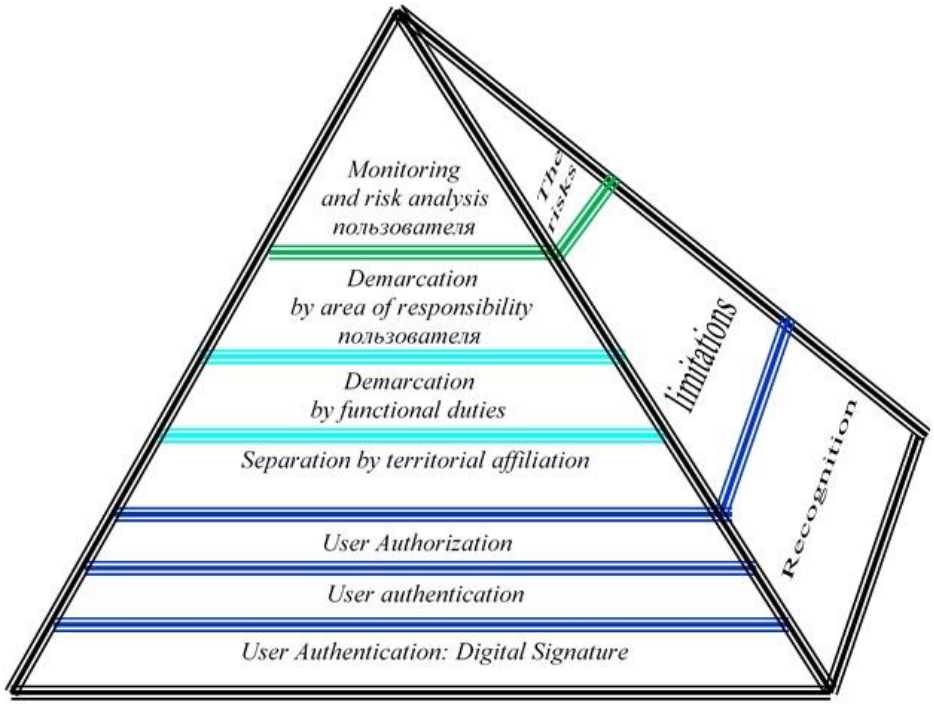

Fig. 3. ***The pyramid of conditions for protecting information from "insiders".***

2. Recognition of users of information systems.

The first layer of the user confidence control pyramid consists of three parts: user identification: digital signature, authentication and user authorization.

Identification means confirming the authenticity of an identity by establishing a name or any other signs that can be used as an identifier [7]. Identification does not yet prove that a person really bears the name that he is called. Identification is just an announcement of the name of a particular person. Therefore, to ensure the reliability of this process, an electronic digital signature of the user is

used. An electronic digital signature may include a user identification number, name, tax identification number.

Authentication means checking or proving that the user is indeed the person whose name he named. Confirm the identity of something or someone with evidence that is legally significant, for example, a business card, driver's license or some details of the life of the person whose name was named. It is important that the evidence proving the identity of the user is clearly associated with him, a photograph on the certificate, fingerprints or something else that is specific only to him, not allowing for an ambiguous interpretation.

For example, when a user first logs in to an information system, his identity is determined by his electronic digital signature. However, it can also work through the digital signature of another user. A password is mainly used for this, and the password complexity should be high enough to ensure information security.

Authorization means providing access to specific resources or services in accordance with the characteristics or properties of the person whose authenticity is established. Authorization is a sequence of successful authentication procedures and the further determination of the characteristics or rights of an established person. Thus, authorization is always the result of determining, according to some predetermined rules, the characteristics and / or properties of the person established before this using the authentication procedure.

3. The boundaries of the actions of users of information systems.

The second layer of the users authenticity control pyramid consists of three parts: delimitation of rights by territorial affiliation, delimitation by functional responsibilities and delimitation by users of information systems by area of responsibility.

The distinction between *the territorial affiliation* of users of information systems is determined by the features of the restrictions imposed on users in the information systems of customs authorities. Depending on their territorial affiliation, the concepts of horizontal and vertical conditions for access to information resources of customs authorities appear here (Fig. 4.).

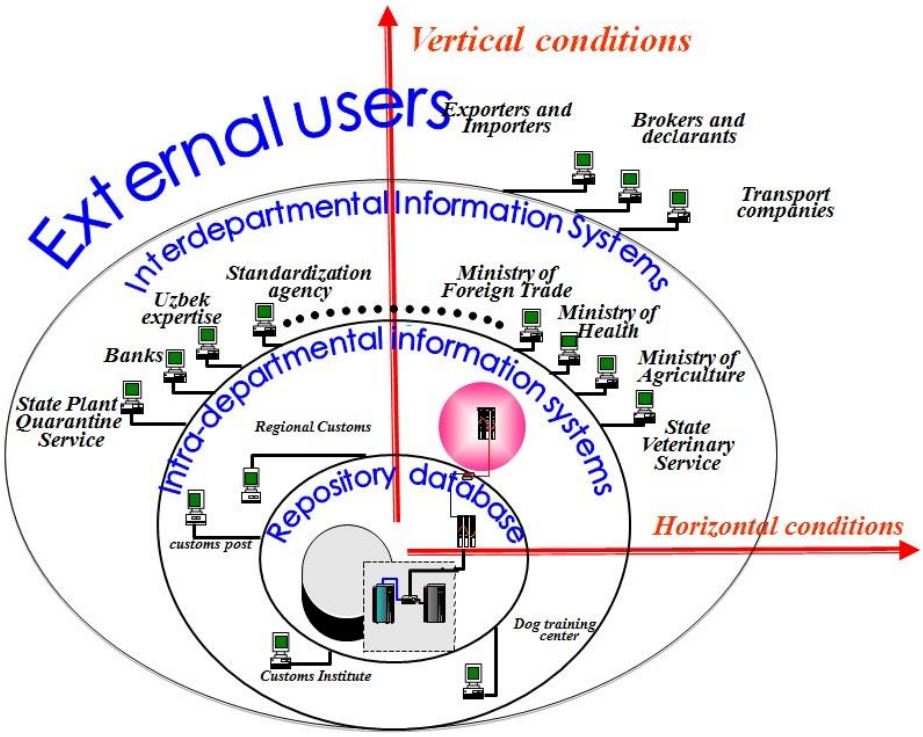

Fig. 4. ***Horizontal and vertical conditions for access to information resources of the State Customs Committee.***

Moreover, the access zones of users of information resources of the customs authorities are considered in the form of a "propagating radio wave", a ring that is located inside each other. Users of information resources that have access to resources located inside the ring have the highest priority. As rings become wider, the number of users increases, but their access to information resources decreases.

Here, *the vertical conditions* for users of information resources are defined as follows: users of the information resources of the inner rings are allowed access to the information resources of the outer rings, but users of the outer ring are not allowed access to the resources of the inner rings. In this case, an exception is access to standard user directories and classifiers.

The vertical conditions for access to information resources of the customs authorities are most clearly reflected in the hierarchical management structure of the State Customs Committee.

Since the State Customs Committee of the Republic of Uzbekistan is part of the largest system of administrative public administration with large volumes of information transmitted and received, the presence of a multi-level algorithm of work and complex infrastructure, a vertical management system is clearly observed in its management structure.

The State Customs Committee of the Republic of Uzbekistan has a three-level management system (Fig. 5.):

- The Central Office of the State Customs Committee of the Republic of Uzbekistan;
- Territorial departments of the state customs committee of the Republic of Uzbekistan for the Republic of Karakalpakstan, regions, the city of Tashkent and special structural units;
- Customs complexes and posts.

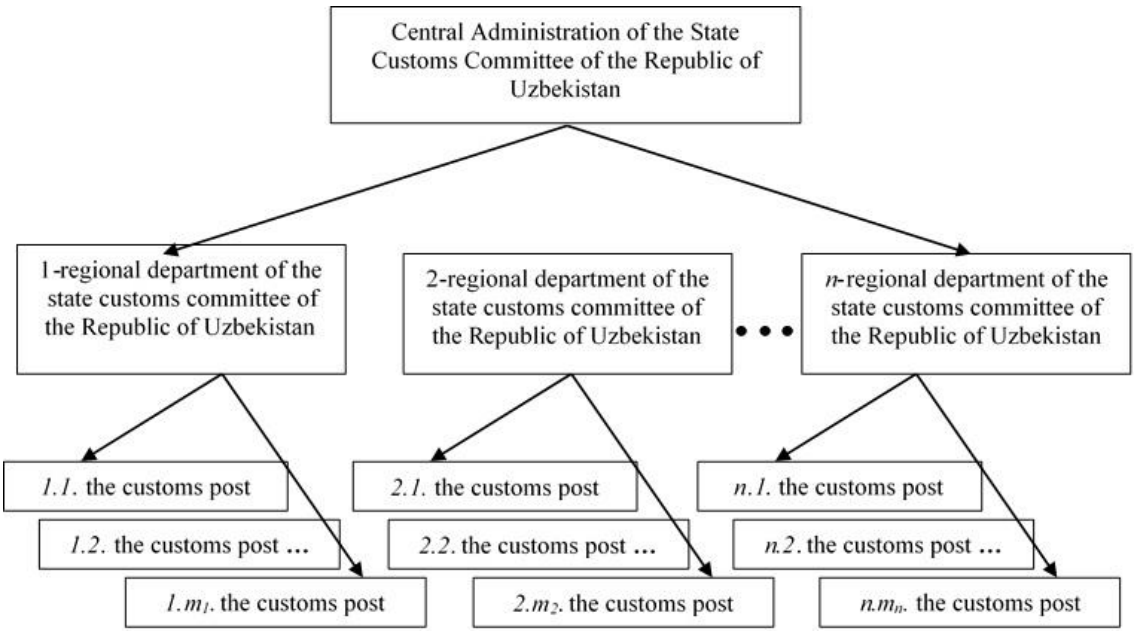

Fig. 5. ***Hierarchical management system of customs authorities.***

At the level of the Central Administration of the State Customs Committee of the Republic of Uzbekistan, users have a high level of access to information resources of customs authorities. They have the opportunity to see all the system information, make changes to the allowed part and receive reports at the national level.

At the level of territorial administrations of the state customs committee for the Republic of Karakalpakstan, regions, the city of Tashkent and special customs complexes, users have the opportunity to use centralized information resources of a reference nature only. For the rest of the information resources of the customs authorities, users of this category have access only to data for their territorial division.

Users of information resources of customs authorities at the level of a customs post have access only to data on their customs post.

At the same time, *the horizontal conditions* for users of information resources of the customs authorities are as follows: each user within one ring is allowed access only to those information resources that were created only by himself or his subordinate employees. In other words, access to information resources provided to the head of the department for the Republic of Karakalpakstan is closed not only to employees of lower posts, but also to customs officers of Khorezm, Navoi and other regions, which are on the same level.

Differentiation according to the functional duties of users implies access to information resources to a customs officer, in accordance with the position held for the performance of their official duties. In particular, if there are several information systems of the customs authorities, each employee is granted a separate permit for each information system based on his functional responsibilities. For example, employees serving at a customs border crossing point by rail are not allowed to access information resources for organizing customs control of road transport.

Differentiation by area of responsibility implies differentiation of access to information resources for users holding the same positions, but with different functional responsibilities. For example, two officers serve at a border customs post at a border crossing by rail. One of them is responsible for the organization of customs control over freight cars, and the other passenger. Each of them does not have access to information entered by the other.

Conclusion.

Given that users of information systems are the most vulnerable points of information security, regulatory methods are used to ensure security. In particular, in accordance with the Law of the Republic of Uzbekistan dated December 25, 2007 No. ZRU-137, a separate article was introduced in the Criminal Code, "Part XX. Crimes in the field of information technology", which provides for criminal liability for violation of information security requirements [9].

Nevertheless, many years of experiments have shown that multicriteria restrictions on access to information resources for such threats can provide effective results. In particular, the use of this method in information systems over the past 10 years has made it possible to exclude attempts of unauthorized access to the information resources of the State Customs Committee.

References:

1. Ukaz Prezidenta Respubliki Uzbekistan «O merah po dalnejshemu sovershenstvovaniyu informacionnyh tehnologij i svyazi» ot 19 fevralya 2018 goda №UP-5349. // Nacionalnaya baza dannyh zakonodatelstva Respubliki Uzbekistan. - Tashkent. -2018. - №06/18/5349/0792.
2. Saidov A.A., Dusmuhamedov A.I. Informaciya o piramide informacionnoj bezopasnosti tamozhennyh organov. // Nauchno-prakticheskij i informacionno-analiticheskij zhurnal «Pokolenie Muhammada al-Horezmij». -Tashkent. -2018. - № 2 (4)/2018. - s. 7-10.
3. Preobrazhenskij E. Insajderskie ugrozy v Rossii. // M: «Korporativnaya periodika». Nauchnyj zhurnal «Upravlenie personalom». - 2009. - №7 (209). - s. 6-10.
4. Kroshilin S.V. Vozmozhnye ugrozy bezopasnosti ekonomicheskih informacionnyh sistem upravleniya i metody ih ustraneniya. // Materialy mezhvuzovskoj nauchnoj konferencii «Metody i problemy upravleniya ekonomicheskoj bezopasnostyu regionov» - Kolomna: KGPI. - 2006. - s. 240-244.
5. Goreleva E. Sotrudniki kazhdoj vtoroj rossijskoj kompanii kradut dannye. // Elektronnyj zhurnal «Vedomosti». -URL: https://www.vedomosti.ru/management/articles/2016/05/17 /641362. (data obrasheniya 05.04.2019).
6. Afonin P. N. Informacionnye tamozhennye tehnologii // SPb. «Troickij most». - 2012. - 352 s.
7. Dresher D. Osnovy blokchejna: vvodnyj kurs dlya nachinayushih v 25 nebolshih glavah // M.: «DMK Press». - 2018. - 196 s.
8. Skiba V. Yu. Obektno-funkcionalnaya verifikaciya informacionnoj bezopasnosti raspredelyonnyh avtomatizirovannyh informacionnyh sistem tamozhennyh organov // Dissertaciya na soiskanie uchyonoj stepeni doktora tehnicheskih nauk po specialnosti: 05.13.19 - «Metody i sistemy zashity informacii, informacionnaya bezopasnost». SPb.: - 2009. - 365 s.
9. Ugolovnyj kodeks Respubliki Uzbekistan // Nacionalnaya baza dannyh zakonodatelstva. URL:<http://lex.uz/docs/> (data obrasheniya: 5.04.2018).