АПИБК-2020

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КАЗАХСТАНЕ

Алматы

15 января, 2020 года

Институт информационных и вычислительных технологий МОН РК

«Ғылым ордасы»

МАТЕРИАЛЫ

Международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане»
15 января 2020 года

Алматы 2020

УДК 004
ББК 32.973.202
А35

А35 **Актуальные проблемы информационной безопасности в Казахстане:** Матер. Межд. науч. – практ. конф. (15 января 2020 г.). – Алматы, 2020. – с. 260

ISBN 978-601-332-542-2

В настоящее издание вошли материалы докладов Международной научно – практической конференции «Актуальные проблемы информационной безопасности в Казахстане».

Работа конференции проводилась при участии представителей органов государственной власти, квазигосударственных предприятий, научных сообществ и вузов, руководителей и специалистов компаний – разработчиков средств защиты информации, телекоммуникационных компаний, операторов связи, организации, осуществляющих свою деятельность в области информационной безопасности.

Рассмотрены актуальные вопросы обеспечения информационной безопасности в государственном секторе, состоялся диалог представителей отрасли и регуляторов, проведены обмен опытом и повышение информированности участников конференции о состоянии информационной безопасности в Республике Казахстан.

Материалы сборника предназначены для научных работников и преподавателей вузов соответсвтующего профиля, докторантов и магистрантов, а так же для специалистов, чьей задачей является использование средств обеспечения информационной безопасности.

УДК 004
ББК 32.973.202

ISBN 978-601-332-542-2

Программный комитет

***Председатель Международного Программного комитета*:**

- Калимолдаев М.Н., академик НАН РК, д.ф.-м.н., профессор, генеральный директор ИИВТ МОН РК, Казахстан

Зам. председателя:

- Бияшев Р.Г., д.т.н., профессор, Казахстан
- Минникаев М.Н., эксперт по информационной безопасности, Казахстан

Члены международного программного комитета:

- Абдикаликов К.А., д.т.н., профессор, Казахстан
- Аманжолова С.Т., к.т.н., доцент, Казахстан
- Бабенко Л.К., д.т.н., профессор, Россия
- Бердибаев Р.Ш., к.полит.н., доцент, Казахстан
- Исмаил Е.Е., к.т.н., профессор, Казахстан
- Ищукова Е.А., к.т.н., доцент, Россия
- Капалова Н.А., к.т.н., Казахстан
- Конявский В.А. д.т.н., профессор, Россия
- Мусиралиева Ш.Ж., к.ф.-м.н., доцент, Казахстан
- Нысанбаева С.Е., д.т.н., профессор, Казахстан
- Сейлова Н.А., к.т.н., доцент, Казахстан
- Тукеев У., д.т.н., профессор, Казахстан
- Prof. Stouraitis Thanos, Greece

Ученые секретари конференции:

- к.т.н. Юничева Н.Р.,
- PhD, Бегимбаева Е.Е.

Приглашенные участники:

- «Государственная техническая служба» КНБ РК - Медет Искаков.
- «Национальный университет обороны имени Первого Президента Республики Казахстан – Елбасы» - Кайнарбек Кожахметов.
- АО «Национальные информационные технологии» - Гани Надирханов.
- АО «Казпочта» - Айдос Сулейменов.
- ТОО «Ak Kamal Security» - Алексей Куксенко.
- АО «Транстелеком» - Анатолий Серебренников.
- «Большая четвёрка» аудиторских компаний:
    1. Ernst & Young – Канат Сарсекеев,
    2. PricewaterhouseCoopers – Олег Прокудин,
    3. KPMG – Дамир Еркин,
    4. Deloitte Touche Tohmatsu – Мирзариф Миркамилов.

Приглашенные аналитики:

- Владислав Остапенко – независимый эксперт,
- Дмитрий Черняк – АО «ЦАЭК»,
- Алексей Стрижевский – ТОО «Тенгри Секьюрити»,
- Юрий Мороз – Агентство Республики Казахстан по регулированию и развитию финансового рынка,
- Виктор Покусов – ТОО «Национальный инновационный центр».

Организационный комитет

Председатель:

- PhD, ассоц.проф. Мамырбаев О.Ж.
- к.т.н., доцент Калижанова А.У.

Заместители председателя:

- PhD Ахметжанов М.А.

Члены организационного комитета:

- Абишева А.Ж.,
- Анищенко Л.Н.,
- Ахметов Е.А.,
- Калиева Г.С.,
- Меркебаев А.Г.,
- Самрат С. М.,
- Сулейменов О. Т.,
- Тұрдалыұлы Мұса
- Усатова О.А.,
- Шахмаев Р.А.,
- Шокишалов Ж. М.

Место проведения

Республика Казахстан, г. Алматы, ул. Шевченко 28,
Ғылым ордасы, 15 января 2020 г.

Тел.:

+7 727 272-45-59;

SECURE IDENTITY ACCESS MANAGEMENT

Amanzholova S.[1], Meer Jaro Khan[2], Sagymbekova A.[1], Nurbala R.[1]
e-mail: s.amanzholova@iitu.kz, meerjk@publicist.com,
asagymbekova@gmail.com, nur.r15.96@gmail.com
[1]CE&IS International IT University,Almaty, Kazakhstan
[2]Islamic International University, Islamabad, Pakistan

Abstract. *The security of identity access management has become a hotspot in today's world. Many companies have suffered from information leakage because they ignore the importance of identity access management. In a word, we choose this topic because the essentiality of identity access management requires us to raise the right awareness of the security problems that we have been facing in this information age. To this project, the goal is to find the main elements of identity access management, different kinds of them and the ways to protect their safety. The elements we chose are instruction detection for identity access management. In a word, our task in this project is to raise people's passion for the security of identity access management. The main point is about the detection of intrusion based on data mining in the system, which we think it's the most important part of this topic.*

Keywords: *IAM, Database, Data mining*

I. Introduction

Secure Identity Access Management goes beyond password access and user management[1]. It provides end-to-end user security. According to a recent Dell global security survey, 73 percent of those surveyed experienced a data breach in the past 12 months. In today's world, a secure identity access management (IAM) strategy must move from being a nice-to-have to a must-have for organizations. It's a mistake to think of IAM strategies as one-off projects. Instead, it must be a long-term initiative, with checks and balances to continuously add or refresh integration and optimize processes.

It can be difficult to get funding for IAM projects because they don't directly increase either profitability or functionality. However, a lack of effective identity and access management poses significant risks not only to compliance but also to an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and insider threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever-evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps, and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges [2].

With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required.

This situation and request like having access like another employee rather than specific access needs lead to an accumulation of privileges known as privilege creep. Privilege creep creates a security risk in two different ways. An employee with privileges beyond what is warranted may access applications and data in an unauthorized and potentially unsafe manner.

Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

Building a secure identity and access foundation that provides dynamic security controls will reduce costs and compliance issues down the road [3]. Automation, compliance, and access are all key components to cutting costs, proving compliance and ensuring that employees have access only to the data they need to do their jobs.From all the above, it can be seen that the security of identity access management is a significant element to judge whether management is useful. No doubt that this part should be paid more attention to. So, in this project, the main purpose is to find ways of intrusion detection for identity access management.

Our first step is to find the main elements of identity access management and the roles they play in the management. We have found seven elements up to now that are important to identity access. They are the timely used to provisioning and de-provisioning, the number of the ‘ghost users’, the standard of password, login failure, manual password reset, access exception and the index of service and cost [4-5]. All these elements are closely connected to the security of identity access management. The next step is to approach the problem that how many different kinds of identity access. Different companies usually use different kinds of IAM or different versions of the same one. Collect and understand their features will help us find the breakthrough point of the detection to the intrusion.

II. Related work

To find out intrusion detection in identity access management, the first thing to do is to understand what is the intrusion detection system(IDS). An intrusion detection system (IDS) is a device or software application that monitors a network or system for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system[6]. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network [citation needed]. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyses incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS can respond to detected intrusions[7]. Systems with response capabilities are typically referred to as an intrusion prevention system. As mentioned in the introduction, we found seven main elements in identity access management. Tracking the average time of identity cancellation allows companies to understand the effectiveness of policies that revoke authority when employees leave the enterprise, to make sure that there’s nothing wrong with the access[8]. The ghost users may cause the problem that there may be a cancellation of the

supply error, or attackers may have “back door” access to the system, the rapid detection and resolution of these problems will greatly reduce the risk.

Accounts with weak passwords, old passwords, and expired passwords increase the risk of an enterprise. When there is a large number of user accounts is locked, does this mean that users to guess the other person's password? Or the password policy is too strict, users often forget their passwords because they are too frequent to change the password. These peak activities that are higher than normal levels could mean malicious activities. How long will the user manually reset the password or within a certain time needs help desk? If the number is high, it means that companies need to deploy a different program to help users lock their accounts. This standard can help detect malicious behaviour. Users who track information that they do not need to work regularly can more quickly prevent internal threats, and detect areas where companies can’t strictly restrict access. Identity Access Management problem is actually a database problem. The problem we may have in identity access management: Misuse of database accounts and permissions [8]: The lack of a monitoring mechanism for database administrators. The database administrator has the highest authority of database system management, account management, authority distribution, and other systems. If the database administrator uses their authority to steal sensitive information or destroy important business data, it will be fatal to a database system. The defects of database log audit:

It is difficult to monitor and discover problems in real-time. Log audit function of the database system itself can record all kinds of database systems, modify the permissions to use other log information, but cannot help managers find positioning problems; at the same time, it doesn’t have the function of real-time monitoring. If there are some abnormal detections happen, it can’t be reported to managers immediately, so that managers cannot raise timely effective measures to solve the problem. Although the database system provides users authentication mechanisms, users can only enter the database server for operation while they provide the correct login account and password. If someone obtains an account and password through illegal means, this illegal user can enter the database server to operate, and the user authentication mechanism can do nothing about it.

It mainly obtains behavior patterns through mining audit data to separate the intrusion behavior and effectively realize the intrusion detection rules. Audit data is composed of pre-processed and time-stamped audit records. Each audit record contains some attributes (also known as features). For example, a typical audit log file includes attributes such as source IP address, destination IP address, service type, connection state and so on. Mining audit data is an important task, which directly affects the accuracy and availability of intrusion detection. The commonly used methods include correlation analysis, classification, sequence analysis and so on.

- Correlation analysis is to find association rules, to find out the rules in a database that meet the minimum support and confidence. That is, the correlation between Item is derived by analyzing the record set for a given set of Items and a given set of records The attributes of association rules are generally described with confidence and support degree. The purpose of the association analysis is to generate association rules between sets of data from the known transaction set, that is, a relationship with audit between different fields in the record, while ensuring that rules’ support and confidence is greater than the user’s specified minimum support and trust.
- The classification map a data item to the classification of a predefined set of its output "Classifier", giving a form of decision tree or rule. In intrusion detection, a typical application is to collect enough audit data and give them to the user or program, and then they will use the

classification algorithm to learn the classifier, mark or predict new normal or abnormal invisible audit data. The key point of classification algorithm is the rule-learning problem.

- Sequence analysis is used to construct the sequence patterns to find the time series that often exists in the event of an audit. These frequently occurring event patterns contribute to the application of time statistics to intrusion detection models. For example, if the audit data contains service attacks based on DOS (Denial of Service Attack) behavior, the results of this model will test any host that works at this time.

III. Proposed instruction detection of identity access management

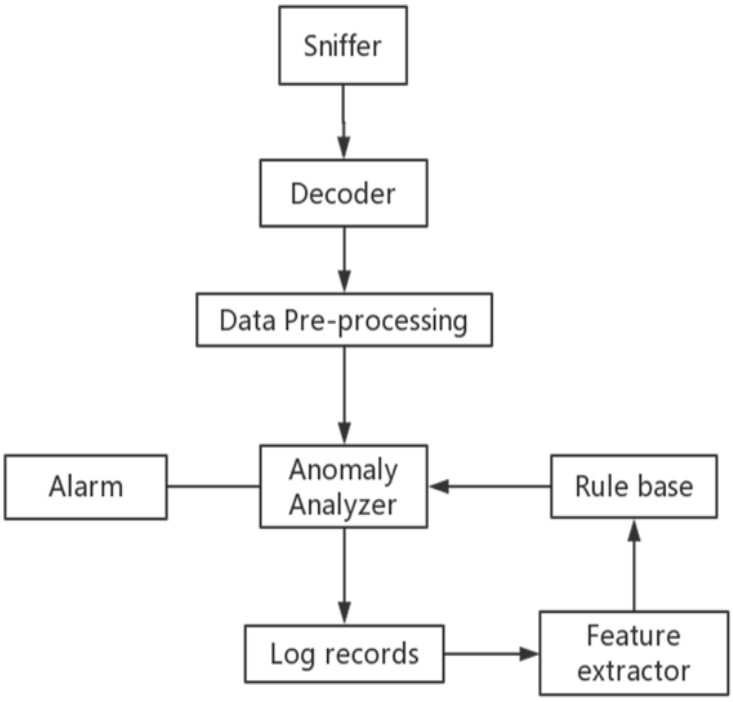


Figure1: Model of intrusion detection based on data mining

i. Sniffer mainly collects data. It is just a simple interface to grab information.

ii. Decode and analyses packets captured by the decoder, and the analysis results are stored in a specified data structure.

iii. Data pre-processing is responsible for converting network data and connection data into data formats needed for mining methods, including further filtering, noise elimination, and known attacks detected by third party detection tools. The misuse detection method is used to match the known intrusion behavior with the rule library intrusion rules, and the intrusion behavior is directly found, and the alarm is carried out.

iv. The anomaly analyzer finds new attacks by using association analysis, and sequence analysis, and sends these abnormal behaviors to the rule base by using anomaly detection method.

v. Log records keep 2 kinds of records: packet information produced by unknown network normal behavior and packet information produced by unknown intrusion behavior.

vi. Rule base keeps intrusion detection rules, which provides basis for misuse detection.

vii. When the alarm deviates from the analyzer to report the abnormal behavior, the alarm sends a notice to the administrator through the man-machine interface, and the form can be E-mail. Console alarms, log entries, and visual tools.

viii. The feature extractor in the log data recorded by the correlation analysis that association rules, added to the rule base.

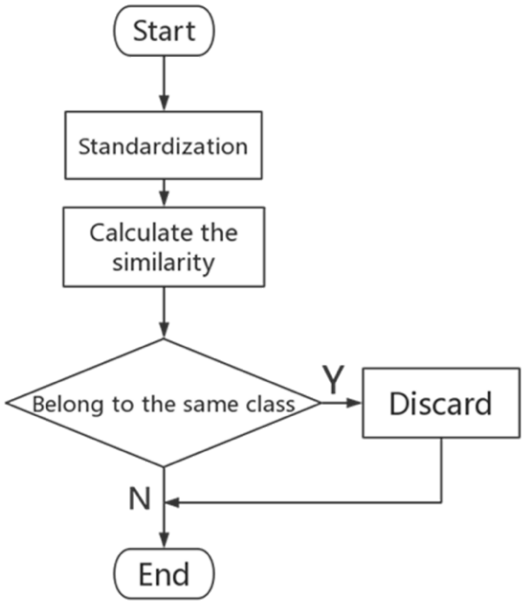


Figure2: Flow of Feature extractor

Detection of abnormal process analyzer:

i. The network or host data packet standardization;

ii. Calculating the similarity clustering centre network data packet with the main class in the list:

iii. If the network data packet with a similarity of the main class is less than the clustering radius R, it is that it is a normal network data packet that will be discarded;

iv. If the similarity of the network data packet with all the main class is greater than the cluster radius R, that is the abnormal data packets.

Anomaly analyzer uses the network or hosts a normal model to detect packets generated by the clustering analysis model. It uses K-Means algorithm as a clustering analysis algorithm. K-means algorithm is a typical distance-based clustering algorithm, which uses some distance as the evaluation index of similarity, that is, the closer the distance between the two objects, the greater the similarity.

Algorithm 1: K-means Algorithm

1. Input: Set of Data(include N elements), clustering parameter K
2. Output: K clusters
3. Begin
4. Step1: select k documents as the initial cluster center
5. Step2: repeat
6. Step3: for j = 1 to n do
7. Assign each x_j to the cluster which has the closest mean
   //give each element to the most similar cluster based on the average of the

elements in the cluster
8. Setp4: for i = 1 to k do
9. $\bar{x} = \sum_{x \in C_i} x / C_i$
//renew the average of cluster
10. Step5: compute
11. $E = \sum_{i=1}^{k} \sum_{x \in C_i} ||x - \bar{x_i}||^2$
//calculate formula function E
12. Step6: until E has no overt change
13. end

i. Select K document as the center of mass from N document randomly,
ii. Remain the distance from each measurement to the centroid for each document, and put it into the nearest centroid,
iii. Recalculate each class centroid,
iv. Iterate ii ~ iii steps until the new centroid and the original one is equal to or less than a specified threshold, the algorithm end.

There are many attributes of data packets, some of them is useless to clustering. The data we need is show in Table 1.[3]

Table 1. The Table of Clustering Attributes

Name	Description	Data Type
ip_len	the length of IP	Continuity
ip_ttl	survival period	Continuity
ip_options_len	the length of IP selection rules	Continuity
tcp_win	the size of TCP window	Continuity
tcp_options_len	the length of TCP selection rules	Continuity
dsize	load size of packet	Continuity
udp_len	the length of UDP	Continuity
ip_tos	type of IP service	Dispersion
ip_protocol	type of treaty	Dispersion
ip_src	address of source IP	Dispersion
ip_dst	address of target IP	Dispersion
tcp_flags	target TCP	Dispersion
src_port	number of source port	Dispersion
dst_port	number of target port	Dispersion

Feature extractor for abnormal data analysis of unknown packets, packet network anomaly mining potential intrusion behaviors, generating association rules corresponding to Tim. The algorithm uses the Apriori algorithm to mine association rules, and the workflow is shown in Figure 3.

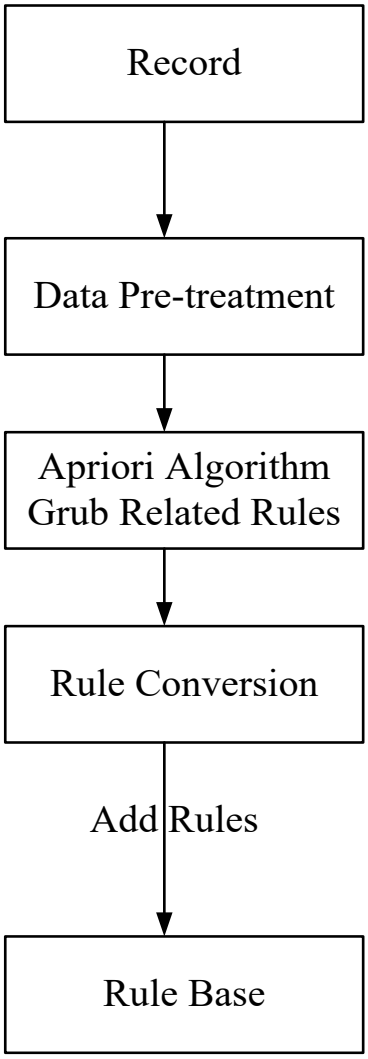


Figure3: Flow of Feature extractor

The working process of feature extractors can be divided into data preprocessing and generate association rules.

i. The input data preprocessing feature extractor for logging. It contains a lot of fields, but not all fields for correlation analysis. Then select only the fields, and the relevant rules of Snort such as SrcIP, SrcPort, DstIP, DstPort, Protocol Dsize, Flags, and CID.

ii. To generate association rules according to the set of support to find all frequent item sets, general support is set too low, and the frequent item sets will be more and higher; Setting, frequent item sets are generated. Then generating association rules from frequent item sets, setting the more general confidence low, the number of association rules are generated, but the accuracy is not high; otherwise the confidence setts higher. The number of association rules is generated but less accuracy.

If the data packet goes through the system and there are no rules can match it, this data packet may be an unknown attack. We should save this to the rule base. But before we save it in the base, we should standardize it to make the show all data in it is useful to our rules. unknown attack is shown in Table 2.

Table 2. The Structure of unknown attack

Name	Type	Length	Remark
ip	int	10	identification
ip_len	int	10	the length of IP
ip_ttl	int	10	survival period
ip_options_len	int	10	the length of IP selection rules
tcp_win	int	10	the size of TCP window
tcp_options_len	int	10	the length of TCP selection rules
dsize	int	10	load size of packet
udp_len	int	10	the length of UDP
ip_tos	varchar	45	type of IP service
ip_protocol	varchar	45	type of treaty
ip_src	varchar	45	address of source IP
ip_dst	varchar	45	address of target IP
tcp_flags	varchar	45	target TCP
src_port	varchar	45	number of source port
dst_port	varchar	45	number of target port

IV. Experiment setup and results

For reason that we don't have that knowledge of making our thought becoming true, we cannot make an application for our project, what we can down is just the K-means algorithm part. We use java to write the code of the K-means algorithm, the result will be shown in Figure 4.

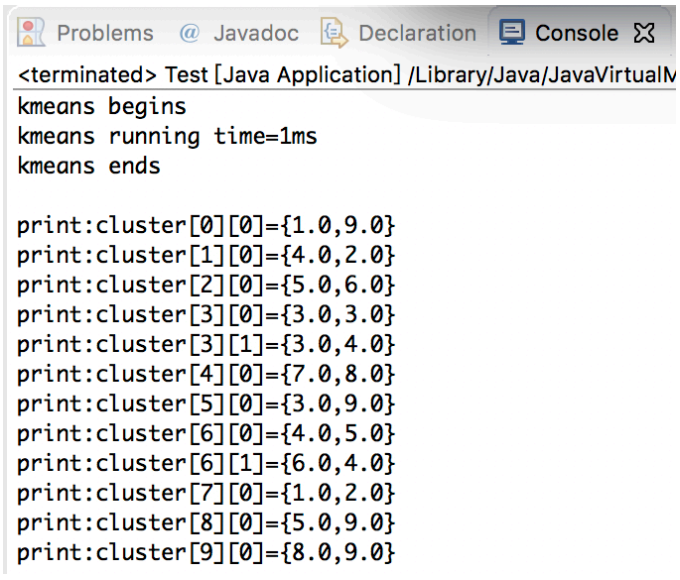


Figure 4 The Experiment Result of K-means Algorithm

V. Conclusions

The instruction detection of identity access management has become the hotspot in today's research. But there are many problems in the traditional way of detections such as low efficiency and bad self-adaptability. The technology of data mining can grub useful information through thousands and hundreds of data, it's exhibition in instruction detection is one of the best ways in this field. What's more, nobody will deny the importance of identity access's

security. The door needs a lock, the box needs the key, and today's high-tech devices need identity access. What is identity access? Before we have a password, now we have a fingerprint, face perception and speech recognition. All these technologies have the problem of being instructed. What we do in this project is to find a way to make secure identity access management for us. Instruction detection based on the technology of data mining is still young in the technology field. How to use the right data mining technology to grub the instruction model is still nodes in research. We will continue our work in our study.

Reference

1. Razaque, Abdul, and Syed S. Rizvi. "Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment." Computers & Security 62 (2016): 328-347.
2. Razaque, Abdul, Nikhileshwara Reddy Vennapusa, Nisargkumar Soni, and Guna Sree Janapati. "Task scheduling in cloud computing." In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-5. IEEE, 2016.
3. Kunz, Michael, Alexander Puchta, Sebastian Groll, Ludwig Fuchs, and Günther Pernul. "Attribute quality management for dynamic identity and access management." Journal of information security and applications 44 (2019): 64-79.
4. Razaque, Abdul, Saty Siva Varma Nadimpalli, Suharsha Vommina, Dinesh Kumar Atukuri, Dammannagari Nayani Reddy, Poojitha Anne, Divya Vegi, and Vamsee Sai Malllapu. "Secure data sharing in multi-clouds." In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1909-1913. IEEE, 2016.
5. Xin, Xiangjun, Qianqian He, Zhuo Wang, Qinglan Yang, and Fagen Li. "Security analysis and improvement of an arbitrated quantum signature scheme." Optik 189 (2019): 23-31.
6. Mahdavi, Ehsan, Ali Fanian, and Fatima Amini. "A real-time alert correlation method based on code-books for intrusion detection systems." Computers & Security 89 (2020): 101661.
7. Almi'ani, Muder, Alia Abu Ghazleh, Amer Al-Rahayfeh, and Abdul Razaque. "Intelligent intrusion detection system using clustered self organized map." In 2018 Fifth International Conference on Software Defined Systems (SDS), pp. 138-144. IEEE, 2018.
8. Brogan, Donna. "Software for sample survey data, misuse of standard packages." Wiley StatsRef: Statistics Reference Online (2014).

PROTECTION OF CONTROL FRAMES FROM DENIAL OF SERVICE ATTACKS DURING HANDOVER PROCESS

Razaque A., Amanzholova S., Sagymbekova A.
e-mail: arazaque@nyit.edu, s.amanzholova@iitu.kz, asagymbekova@gmail.com
CE&IS International IT University, Almaty, Kazakhstan

Abstract. *IEEE 802.11 remote Local Area Network (WLAN) turns out to be most important now a day. Whether it would be a straightforward extent extender for home wired Ethernet interface, or as a wireless interface, WLAN gives mobility, ease of access and moderate. The majority of the 802.11 remote system utilizes the recurrence of 2.4GHz, which*

drives the system to be unsafe and more vulnerable than conventional Ethernet networks. The most prevalent Wireless Medium Access Control (MAC) protocol is IEEE 802.11, which considers all the nodes in the network are safe & cooperative. However, attackers may make nodes misbehave the performance of the network, obtain extra bandwidth and consume resources. These MAC layer misbehaviors can be called Denial of Service (DoS) attacks which can disrupt the network operation. 802.11 wireless local access network there is no possible way to protect control frames and this leads to a range of network allocation vector-based DoS attacks are possible. It has been considered that 802.11 is highly susceptible to dangerous denial-of-service (DoS) attacks. In this paper, we propose an Internet Access point protocol (IAPP) for securing control frames. Our proposed Access point protocol features The best way for protecting control frames by generating a unique message authentication code using inter access (between different stations & clients) point protocol for key distribution and key management is proposed.

Keywords: *CTS, RTS, MAC, IAPP, WEP*

I. Introduction

Security has become an ever-important issue in the case of wireless networking. Recently, there has been huge research on security protocols and key exchange mechanisms in IEEE 802.11 networks [1][3]. However, these networks are still unsafe for DoS attacks [1][2] because these attacks commonly happen before security protocols are evoked. The main purpose of DoS attacks [1][2] is to stop the legitimate client from accessing resources.

Vulnerabilities create a weak point in IEEE 802.11 MAC protocol [3][4][8] and Countermeasures for WLAN Denial of Service attacks[1].

IEEE 802.11 MAC[3][6][7] layer classifies communication into three types of messages - Management, Data, and Control messages. Currently standards 802.11i is used to protect data frames & 802.11w[9] for protecting management frames. Control frames[5][11][12] which are mostly used for bandwidth reservation and acknowledgment purposes cannot be secured by the above-mentioned standards making the network to get attacked using these frames. The purpose of this paper is to protect the control frames[11][13] in a wireless network. Due to this, a range of network allocation vector-based denial of service attacks is possible. In this paper, we provide a solution on how to protect control frames from getting spoofed using IAPP[3].

The remainder of the paper is organized as Section II presents problem Identification. Section III gives a complete overview of the existing techniques. Section IV gives the System model. Section V gives Proposed plan & Implementation and Section VI gives References. Finally, the entire paper is concluded in section VI.

II. Problem identification

An attacker can use the control frames to provide the medium unavailable by gaining the bandwidth using RTS-CTS[11][12][13] (Request to Send – Clear to Send) or CTS to self-organization even if he is not part of the network. The attacker can replay the captured RTS frame or CTS frame or he can inject a spoofed CTS[11] frames in to the network. Due to this all the stations present in the network will update their NAV (Network Allocation vector) timers and terminate their transmissions. The proposed solution does not only protect the RTS[11] and CTS frames[12], it protects all control frames including Block Ack.

III. Related work

A lot of examination has as of now been centered around 802.11[3][6] system security. The majority of this work has concentrated on shortcomings in the wired equivalency protocol (WEP) proposed to give information protection between 802.11 customers and access points.

IEEE 802.11[3][6][10] standard proposed WEP (Wired Equivalent Privacy) which uses RC4 algorithm to protect the data messages by using a pre-shared key. Most of this work has focused on weaknesses in the wired equivalency protocol (WEP) intended to provide data privacy between 802.11[3][6][10] clients and access points. As the RC4 algorithm has been identified to have vulnerabilities and weak keys. The Wi-Fi Alliance, working in conjunction with the IEEE, has brought a strong interoperable Wi-Fi security specification to market in the form of Wi-Fi Protected Access (WPA)[10]. A scheme named WPA to protect the data messages by generating per-packet keys. Although no security solution can give us “bullet-proof,” WPA represents a quantum leap forward in Wi-Fi security. It brings forward IEEE 802.11i standard[1][3]. WPA not only gives strong data encryption to rectify WEP’s weaknesses, but it also gives user authentication which missed in WEP, IEEE 802.11w standard proposed to provide security protection for all management frames.

IV. System model

As the first step, we propose the key generation and key distribution protocol using IAPP[16] framework. Using this key we produce a message authentication code (MAC)[3][4] for control frames. To countering replay attacks, we present a method to generate sequence number which is unique. Which uses earlier transmitted RTS[11] to validate the current received CTS[13]. It also verifies whether data is being sent immediately after the received CTS[13] and if there is no data message sent after the CTS frame[13] then NAV update is not validated. The architecture of the network model comprises of several access points (AP) and stations (STA1, STA2, Rogue Station) present in the same channel. All the stations and access points present in the network must be IEEE 802.11i and IEEE 802.11w compliant.

In this paper, we propose solutions for attacks caused by outsider attackers. The goal of the attacker is to consume the entire channel and not providing for the other STAs and APs to communicate by occupying the entire bandwidth. Generally, there are various types of attacks possible on the network by the rogue stations. Attacks possible through the rogue station and their consequences are explained in the following sections. This sub-section describes the types of attacks possible and their consequences.

A replay attack[17] is where an authentication session is replayed by an attacker to confuse a computer into granting access.

RTS replay attack: If STA1 needs to transmit data to AP, then it can send an RTS[11] frame with duration field set to the time needed to send the data frame after DIFS (Distributed Inter-Frame Space – Minimum time a station /AP needs to wait before sending a frame using Distributed co-ordination function). AP verifies that the request is from a legitimate station, will transmit the CTS[13] response within SIFS (Short Inter-Frame Space – maximum time within which the response frame needs to be sent) with duration field set to the duration requested. STA1 then transmits the data frame to AP and will receive the acknowledgment in return. The rogue station can hear to the channel and acquire the RTS frame[11] sent by STA1 and retransmit it to the AP at a later time. When the AP sends CTS[13] Following STA1 will be rejected as the actual owner of this replayed RTS[11] was not STA1 but it is rogue station. STA2 once sees the CTS frame will update its NAV timer. If the attacker is an expert attacker he can change the duration field of the RTS frame[11] with a very large value making STA2

wait for a long time to start before transmitting while STA1 will still produce the packets because it hasn't updated the NAV timer.

CTS replay attack[17]: In this case, the rogue station (attacker) can hear to the channel and acquire the CTS frame sent by an AP in response to any RTS[14] sent by STA1 and replay[17] the same frame. As in the earlier case, STA1 rejects the CTS[15] frame and will not update its NAV b timer. STA2 once receives the CTS frame[15] updates bits NAV timer with the duration field indicated in the CTS frame[11]. Hence STA2 will terminate transmissions until the NAV timer expires.Injecting Spoofed CTS frames: In this type of attack, the rogue station can form spoofed CTS frames and transmit them. This type of attack is more powerful than all the above-mentioned attacks as every station (example STA1 and STA2) and APs there in the network will update their NAV timer. All the stations and APs present in the channel within the listening range will stop their transmissions as suggested by the CTS frame. An attacker can use this method to stop others from transmitting data by transmitting the CTS frame for a certain period.

V. Protecting control frames

To secure the control frames in a wireless system we begin with a technique for key generation and distribution utilizing IAPP[16] structure. Therefore, a message authentication code (MAC) is produced utilizing this key. This does not suffice to counter the replay attacks mentioned in the above section. With a specific end goal to counter this, we built up a sequence numbering scheme which will guarantee that the MAC[6] created is one of a kind. The message authentication code can be connected to a wide range of control frames even for new frames like Block ACK[13] Request and Block ACK[13]. we describe how key distribution and generation are done and after that continue to proceed with the expansions to the current control frames. In conclusion, we describe how the sequence number is redesigned to counter the replay attacks[17].

Algorithm 1: Protection of Control Frames Process

1. Generation of key 'k'
2. If ((APP ∈ C1)&&(APP= false)) then
3. beginning of key process
4. end if
5. Kr is send to other AP using IAPP
6. else if (AAP>1 && AAP ∈ C1), then
7. one AP will be selected
8. else, none of the AP's will be selected
9. end if
10. if (Ca ∈ C1), then
11. AP sends Kr to other AP's
12. end if
13. New key Ku is initiated
14. The update key 'Ku' will be sent to all the stations connected to AP's
15. If (Ku==K), the
16. updating of key is successful
17. else, not successful
18. Creation of one-time key generation by encryption using SHA-256
19. If (Ma=true), then
20. message authenticated code is appended to control frames

21. Sequence number ‘S’ is appended to message to prevent reply attack
22. For every ‘N’ micro second, stations should update sequence number
23. While (CTS frame not approved), then
24. Control packets will not be sent by AP
25. else if (Tp=long), then
26. using reply attack, the attacker can attack
27. end if
28. end if

The first Generate of the key is done where the key process is initialized when there are no active AP’s found on the same channel. Generated K is distributed to all stations connected to AP. Where generated Key would request the AP’s, when other AP’s are active in the same channel. The key request is sent to other AP using IAPP. It selects one AP if more than one active AP is present in the same channel. After the key request is done, Key transfer would take place AP sends the key request to other AP based on the authenticated channel. In Key update initiate, AP can send this request to other AP’s present in the channel and new key K is sent to all AP’s. Then Key update response where key update initiate is sent to all the stations and key update response will be sent after updating keys for stations. After the key response is done then Key updating is done whether it is successful or not once the key update is successful from all AP’s the initiator who started key update initiate will send key update response to all AP’s. Here in control frames, we use SHA-256 algorithm instead of HMAC algorithm. The message authentication code field is added to existing control frame fields that give protected control frame fields. The existing frame check sequence which is present in 802.11 RTS & CTS is removed and in place of it, we add Sequence number. The sequence number is given to all stations when it connects to AP. Then the station needs to update sequence number every N microsecond, as described in Table1. Here sequence number is 32 bit.

Control packet sent by stations or access points will be listened by all stations or else CTS frame sent by the station is not approved. If the time period is long the attacker can attack using a replay attack. Calculation of N is done by using the duration value of CTS frame if there are hidden nodes then the best value of N is the smallest size data packet. Table 1 shows used notations and definitions.

N=(SIFS+Datadur +SIFS+ACdur +CTS replay_preamble_dur)

Table 1: Notation and definition of given variables

Notations	**Definitions**
SIFS	Short Inter-frame space
Datadur	Time required for transmitting the data packet on air
Ackdur	Time required for transmitting the Acknowledgement frame for the previous data packet on air
CTS_replay_peamble_dur	CTS Packet preamble duration

Key Generation and Distribution: Initially the AP checks the whole channel for a certain scan-interval to discover other actives APs present on the same channel. During this interval, if no different APs are found on the same channel, then the Produce Key primitive is started.

If the sc result is effective (which implies that different APs are found in the same channel) then the AP sends a Key request to alternate access point utilizing IAPP. On the off

chance that more than one AP is available in the channel, the AP can decide to demand key from any AP present in the scan list. This primitive is utilized at whatever point an AP gets a Key Request. The request is validated taking into account the verification gave by the other AP and the key is transferred to the next AP utilizing a secured communication channel.

Any AP present in the channel can start this request and send an update request to the various APs present on the channel. The new key K will be produced and is sent alongside the request. On accepting the Key update initiate ask for, the AP‟s present in the channel send the way to the stations through the wireless medium. On accepting Key update response from every one of the APs the initiator who started the key update initiate request will send Key update successful message to all of the APs. In return, the AP's send the time stamp information at which the new key K should replace K to all the stations.

Message authentication code is generated by using the HMAC algorithm over the SHA-256 cryptographic hash function. The reason for using SHA-256 cryptographic hash function is that many station adapters already have this cryptographic hash function in either their software or hardware layers. Using an existing algorithm reduces the overall cost of updating the system, hence SHA-256 is preferred even though extensions for SHA-256 were proposed. The message authentication code is appended to the control frames using which the receiver validates the authenticity of the message. SHA-256 cryptographic hash function generates a 256-bit message authentication code.

To prevent replay attacks, the sequence number S is appended to the message as shown in Fig 1. 4 byte sequence number is chosen to prevent replay attacks and also the key needs to be updated. (Considering that Sequence number is updated for every 178us as derived in the next section) The frame check sequence (FCS) which is the part of the initial 802.11 RTS and CTS frame is removed to reduce the overhead as MAC can be used in the place of FCS.

The initial network sequence number is given to the station whenever it connects to the access point. From there the station needs to update the sequence number for every N microsecond. The sequence number S is a 32-bit sequence number and once the sequence number reaches (232 -1) it will wrap. The sequence number is updated based on time interval rather than using packet count. The time interval by which the sequence number is updated should not be too short as synchronization in the wireless medium is not too accurate. At the same time, the time interval should not be too long as the attacker can attack using the replay mode. We estimated the value of N considering that the station is transmitting a data packet of a very small duration immediately after transmitting the CTS. To avoid replay for this case, the N should be equivalent to the duration value in the CTS frame.

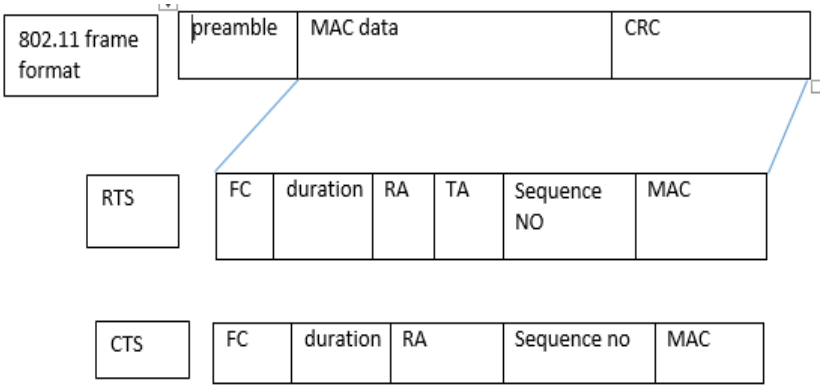


Figure 1. RTS & CTS Frame form

Where
FC- frame control
RA- receiver Address
TA- sender Address
MAC- Message Authentication Code

So the best way to approximate „N" is by considering the size of the smallest data packet and use that as a reference to calculate duration.

A novel approach to counter the replay and fake CTS frame injection DoS attacks caused by not securing the 802.11 control frames is proposed. The solution to improve the current 802.11control frame protection by generating a unique message authentication code using IAPP framework for key distribution and key management is proposed. SHA-256, the cryptographic hash function which is used in this proposed model to generate MAC for the control frames is supported by most of the current wireless station adapters which in turn makes this approach very cost-effective.

VI. Experemental result

Here, we simulated the scenario having a new control frame protection environment using NS2 on Ubuntu 14.04 operating system. The primary goal of the simulation is to generate a unique message authenticated code (MAC) using the key generated form IAPP framework. The simulation scenario consists of 10 nodes. IAPP is used in handoff and an attacker to mislead the bandwidth. The nodes are randomly placed uniformly in the area of 600 * 600 square meters. The total simulation time is 100 seconds. The results demonstrate an average of 2 simulation runs.

In our experiment depicts the Handoff mechanism is initiated where 10 nodes are created out of the 2 nodes are dedicated for access points and remaining are set to mobile nodes. The total simulation time is 100 seconds and during the specified times the mobile nodes shift or move from one access point to another access point. The mobile nodes from one AP to another AP while data is being transmitted to the receiving mobile nodes. While the data is transmitted the mobile nodes shouldn't lose the signal or messages it has to get, so IAPP which gives the handoff mechanism provides the undisturbed signal strength to user mobile nodes even when transferring from one AP to other AP.

Now, the attacker node which takes the data by not allowing to go to required user mobile nodes. Here we generate the attack by randomly generating traffic using control frame messages (RTS & CTS) of sender & receiver nodes. The random generation is done by using a random app procedure, so this assigns the traffic randomly to different nodes for each time of the simulation.

The complete simulation parameters are explained in Table 2.

Table 2: simulation parameters

Parameters	**Description**
Number of Nodes	10
Queue length	50 packets
Type of Network	Wireless
Sensing range of nodes	20 meters
Data rate	55Mbps

RTS Threshold	1000 bytes
Packet size	1500 bytes
Simulation time	100 sec
Size of Network	600*600 square meters

Based on simulation, we obtained the interesting results as

A. The Handover Accuracy

Figure 2 shows the accuracy of the handover process of the mobile nodes. The graph X-axis describes a number of handoffs taken place in the network. Here the nodes are 10 in number so there would be 18 handoffs. And Y-axis describes the accuracy of handoff/handover. Here in this scenario, there are 10% malicious nodes that would cause handoff to be reduced inaccuracy, but though the network maintains to be 99.9% handover accuracy using IAPPFC, which stabilizes the nodes in the network.

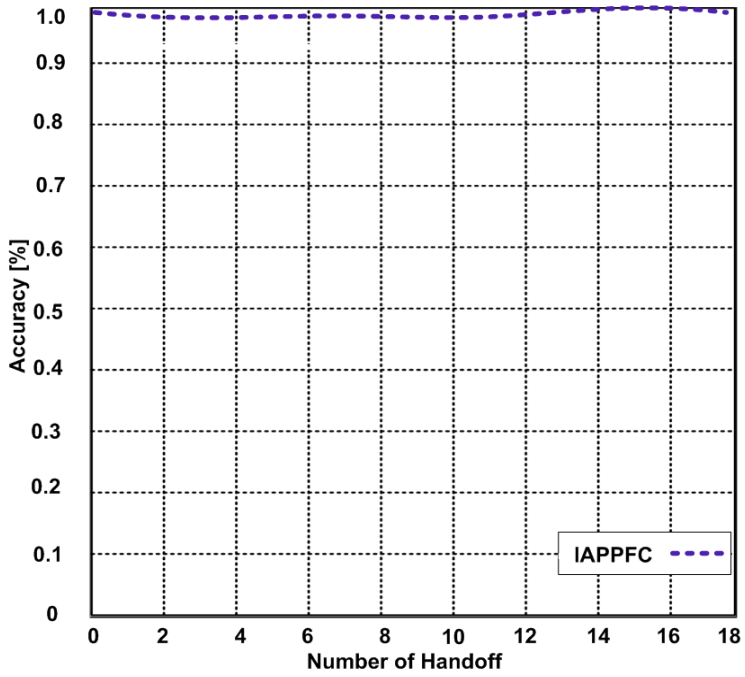


Figure 2: Handoff vs Accuracy

B. Malicious Node Detection

Figure 3 shows a number of malicious nodes that can be detected over detection time. Using the IAPPFC X-axis generates the number of malicious nodes from 0 t0 27 and Y-axis generates malicious nodes detection time in [seconds] from 0 to 1 Seconds. Here the graph increases w.r.t to the number of malicious nodes. As there are more malicious nodes time taken to detect the malicious nodes would be more at different intervals of time. Here 3 malicious nodes are detected at 0.59 seconds and 7 nodes are detected at 0.4 seconds and so on 27 malicious nodes are detected at 0.8 seconds.

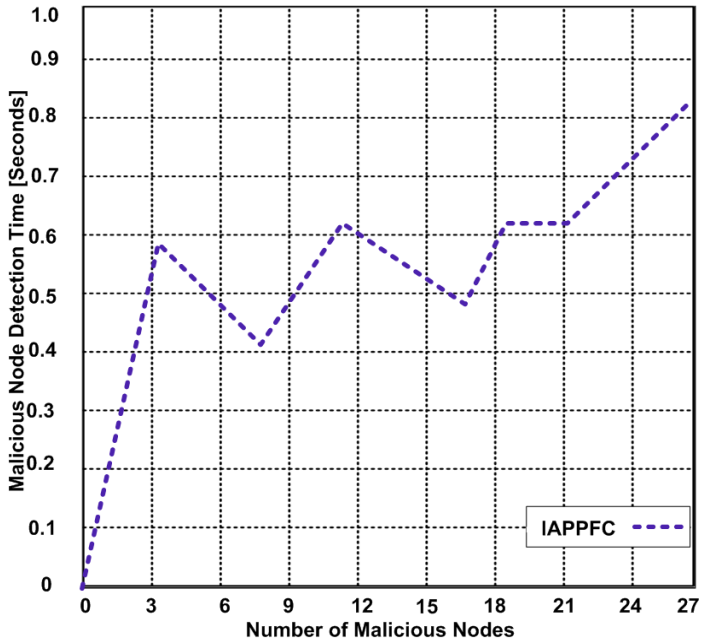


Figure 3: Malicious Node Detection

C. Control Frame with IAPP and without IAPP protection

Figure 4 reflects the difference between the control frame with IAPP & without IAPP. X-axis provides the information of a number of generated control frames and Y-axis provides the information of node detection probability [%]. Here when using without IAPP the capability of malicious node detection would be less and even the performance also decreases. Using IAPP malicious node detection capacity is more, so thereby it leads to an increase in the performance of the network. By using the proposed scheme, the results meet the expected results.

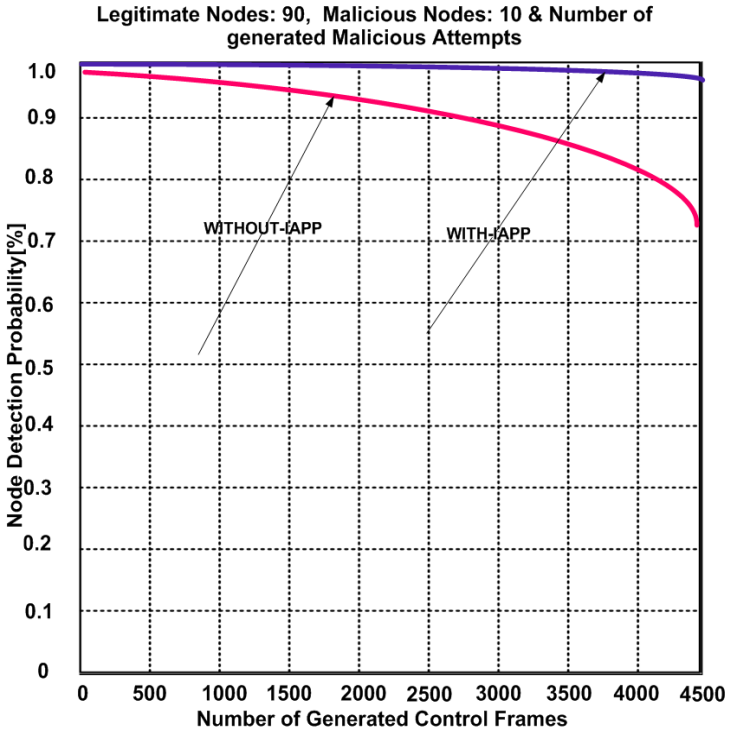


Figure 4: Control Frame with IAPP & without IAPP

VII. Conclution

An approach to counter the reply and fake CTS frames injection DoS attacks is by modifying the standard control frame to a new control frame format by appending a sequence number and message authentication code (MAC). The MAC is generated by using the key produced by IAPP framework. SHA-256 is a hash function that is being used to produce MAC for the control frames which in turn is supported by most wireless adapters and cost-effective. The IAPP (Inter access point protocol) uses the handoff mechanism to switch the nodes or users from one access point to another access point, and an attacker is created to waste or mislead the bandwidth by replaying or repeating the same RTS or CTS frames. Finally, this proposed scheme solves the issue

References

1. Razaque, Abdul, and Khaled M. Elleithy. "Low duty cycle, energy-efficient and mobility-based boarder node—MAC hybrid protocol for wireless sensor networks." Journal of Signal Processing Systems 81, no. 2 (2015): 265-284.

2. Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DoS attack and DoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34, no. 239-53

3. Sheng, Yong, Kokkiong Tan, Guanling Chen, David Kotz, and Arnett Campbell. "Detecting 802.11 MAC layer spoofing using received signal strength." InINFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

4. Razaque, Abdul, and Khaled Elleithy. "Energy-efficient boarder node medium access control protocol for wireless sensor networks." Sensors 14, no. 3 (2014): 5074-5117.

5. Unk, Niraj, Ankit Trivedi, and Abdul Razaque. "Dynamic allocation of slot using MAC protocol." In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-5. IEEE, 2016.

6. Mishra, Arunesh, Minho Shin, and William Arbaugh. "An empirical analysis of the IEEE 802.11 MAC layer handoff process." ACM SIGCOMM Computer Communication Review 33, no. 2: 93-102.

7. Cardenas, Alvaro A., Svetlana Radosavac, and John S. Baras. "Detection and prevention of MAC layer misbehavior in ad hoc networks." In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 17-22. ACM,

8. Razaque, Abdul, and Khaled Elleithy. "Scalable and energy efficient medium access control protocol for wireless sensor networks." In 2015 Long Island Systems, Applications and Technology, pp. 1-4. IEEE, 2015.

9. Sun, Min-te, Lifei Huang, Shaoyong Wang, Anish Arora, and Ten-Hwang Lai. "Reliable MAC layer multicast in IEEE 802.11 wireless networks." Wireless Communications and Mobile Computing 3, no. 4 (2003): 439-453.

10. Jorgensen, Jacob W. "Application-aware, quality of service (QoS) sensitive, media access control (MAC) layer." U.S. Patent 6,640,248,

11. Van Der Schaar, Mihaela, and Shankar N. Sai. "Cross-layer wireless multimedia transmission: challenges, principles, and new paradigms." Wireless Communications, IEEE 12, no. 4: 50-58.

12. Gerla, Mario, Ken Tang, and Rajive Bagrodia. "TCP performance in wireless multi-hop networks." In Mobile Computing Systems and Applications, . Proceedings. WMCSA. Second IEEE Workshop on, pp. 41-50. IEEE,.

13. Lei, Zhongding, and Stephen J. Shellhammer. "IEEE 802.22: The first cognitive radio wireless regional area network standard." IEEE communications magazine 47, no. 1: 130-138.

14. Xiao, Yang, Haizhon Li, and Sunghyun Choi. "Protection and guarantee for voice and video traffic in IEEE 802.11 e wireless LANs." In INFOCOM. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 2152-2162. IEEE,

15. Ni, Qiang. "Performance analysis and enhancements for IEEE 802.11 e wireless networks." Network, IEEE 19, no. 4: 21-27.

16. Ramani, Ishwar, and Stefan Savage. "SyncScan: practical fast handoff for 802.11 infrastructure networks." In INFOCOM. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pp. 675-684. IEEE.

17. Wu, Bing, Jianmin Chen, Jie Wu, and Mihaela Cardei. "A survey of attacks and countermeasures in mobile ad hoc networks." In Wireless Network Security, pp. 103-135. Springer US.

SCHOOL SECURITY SYSTEM USING RFID

Razaque A., Amanzholova S., Shevchenko Y.,
Samburskaya S., Fazylbekova R.
e-mail: arazaque@nyit.edu, s.amanzholova@iitu.kz, 23600@iitu.kz,
23625@iitu.kz, 23028@iitu.kz
CE&IS International IT University, Almaty, Kazakhstan

Abstract. *Due to the increase in the number of crimes against children, it is more important for parents to improve the security of children. RFID is a security system that is used in modern schools in developed countries. The essence of RFID is to use sensors and identification cards that allow determining the child's field, the exit and the entrance to the school and the school bus. Also, in these cases, parents receive a notification via SMS. This paper addresses a problem of SMS channel that uses SS7 protocol that has already been officially recognized as unsafe by the National Institute of Standards and Technology (NIST) due to the possibility of SMS interception and falsification. That can lead to a violation of privacy and used in the planning of crimes.*

This paper aims to solve the problem of SS7 by replacing it with telegram bot. The telegram combines the features of both notifications and additional information. These both features only provide the information to a particular recipient. The proposed solution is more secure that uses MtProto protocol based on MD5 and RSA algorithms. The proposed protocol is implemented by using JAVA platform. Based on testing results, we prove that the proposed solution performs better than the existing SS7.

Keywords*: RFID, Schools Security System, Privacy, Telegram bot, Security, SS7.*

I. Introduction

The security is of paramount significance [1]. In 2016, the rate of violent crimes upon children reached 28 per 1,000 populations, disappear from 30 to 70 children. This statistic shows the importance of establishing an effective security system. To obtain information about the movement of children fast and accurate an automation system is required. Nowadays a lot of technologies exist to accomplish that. The first example of using this technology in school security systems be-came Spring Independent School District near Houston, Texas [2]. Radiofrequency identification (RFID). RFID is a term that is used to describe a system that transmits the identity of an object or person in the form of a unique serial number, using radio waves [3]. There are also notifications for parents in case of changing the child's location. They are sent using the SS7 protocol.

In 2017, the researcher, Bill Welch, published an analysis of vulnerabilities in SMS networks. It's been told attackers might exploit the open functionality of these networks to disrupt them or cause them to fail [4]. The most serious threat is SMS spoofing, which occurs when a fraudster manipulates address information in order to impersonate a user who has moved to another network and sends messages to the home network. It's the old and known vulnerability. And using the SMS channel can lead to a violation of privacy and can be used for easier planning of crimes. The Internet PTN convergence allows at-tackers inroads via entities with poorly secured SS7 net-works [5].

For safer implementation, we suggest replacing SMS notification with Telegram Bot. Telegram is a popular instant messenger which created its own original protocol known as MtProto. MtProto protocol based on MD5 and RSA algorithms [6-7]. The protocol was developed by Nikolai Durov and other developers and is based on 256-bit symmetric AES encryption, 2048-bit RSA encryption and Diffie–Hellman key exchange [8]. We suppose this solution will be easily implemented due to the fact it has been reported that over 2.18 billion smartphone owners use alternative messaging services at least once a day [9].

The features of the bot include:

- notifications about changing a child's location;
- ability to show coordinates on the map;
- access to personal information via a bot will be protected with a password of parents given in school.

This paper contributes as:

- The telegram bot maintains the faster and accurate process about the security of children;
- Ability to obtain not only text information but also geographic coordinates.

The remainder of the paper is organized as:

Section II presents the problem identification and significance. Section III discusses the salient features of existing approaches. Section IV presents proposed telegram bot. Section V experimental results and implementation. Section VI concludes the entire paper.

II. Problem identification and significance

The main goal of RFID Security System is to offer suitable, speedy and safer access to information about the location of the child obtained by RFID tags. Such access means using SMS notifications efficiently through mobile devices. One of the major challenges in safe implementation is in the handoff process. The SS7 vulnerabilities could be a hurdle for a safer handoff process. SS7 has become an integral part of the global telecommunications infrastructure due to its ability to route text (SMS) messages, support interconnection, provide

transparent roaming, and provide information for a session, such as a caller ID. SS7 networks were originally designed to work in the trusted domain of the operator or to interact between trusted operators, providing a certain level of security. With this in mind, additional security features were not a major design consideration, and security was not properly considered in years past. Currently, with so many entry points, the SS7 has become insecure [4]. As a result, there are possibilities of data loss and security threats [5].

There are several vulnerabilities that allow an at-tacker to listen to or record a subscriber's conversation on incoming/outgoing SMS. In addition, an attacker can intercept and modify incoming text messages for the tar-get subscriber. In each of these attacks, the attacker uses legitimate call establishment processes to establish him-self as a "man in the middle", leaving the target subscriber overlooking the attack [4].

Realizing such a dynamic need for secure handoff and keeping these concerns as the priority, we deploy a secure, easy to use Telegram Bot for successful handoff to avoid data loss and minimize security threats.

III. Related work

In this section the salient features of existing approaches are summarized.

• RFID with Global System for Mobile Communications (GSM) is introduced in [10] for parent and school principal communication. The pro-posed system is used for data transmission via SMS. The microcontroller communicates with the GSM modem sequentially through the linear drive MAX 232. The system is easy to implement and produce fast transmission. However, this system does not have encryption support.

• RFID based school bus tracking and security system is presented in [11]. The introduced method is used for identifying a child in the bus or in the school by scanning of identity card, sending notification to parents and ability of viewing records of child's location. This system is easy to implement and use, but it doesn't provide secured connection.

• The use of RFID in SMART watches is de-scribed in [12]. In this method, the school bus sensor is connected to each child's GPS device. Because of the comparable coordinates using watches. The advantages are available for de-vices and location confirmation, but there are also disadvantages in the form of the possibility of falsifying messages.

• A description of the method of operation of the RFID system using recurrent cryptography and physics can be studied in [13]. Here it is pro-posed to use RFID tags to determine the location of the child, as well as offer how to improve the safety and privacy of the child. Of the minuses it can be noted that it is easy to gather in-formation and the most difficult to detect is a spying activity. If we consider the advantages, then here it is impossible not to note the light-weight functionality and RFID tag wireless capabilities.

• The method of using a cryptographic Public Key in RFID for tags and can be application read in [14]. This method indicates a lack of crypto-graphic protection due to which the child's security may be compromised. Thus, PKC has its own algorithm called Public Key, which minimizes the risks of privacy propagation. Of the advantages, it can be noted that PKC uses encryption, but the disadvantages are that the sys-tem itself is very slow and also expensive.

• Hardware Implementation of a TEA-Based Lightweight Encryption for RFID Security is presented in [15]. This implementation proposes to introduce the C1G2 standard, which supports functions for passive tags such as anti-collision, 16-bit cyclic redundancy code (CRC) check-sum, and 10-bit pseudorandom number genera-tor (PRNG), along with ensuring consumer privacy with a simple Kill command. This method protects children and parent's privacy, but dynamic data updates and analysis can be lost.

IV. Proposed telegram bot

To implement our solution, we will create a Tele-gram Bot API (application programming interface).

Bots are third-party applications that run inside Telegram. Users can interact with bots by sending them messages, commands, and inline requests. You control your bots using HTTPS requests to our bot API. At the core, Telegram Bots are special accounts that do not re-quire an additional phone number to set up. Users can interact with bots in two ways:

- Send messages and commands to bots by opening a chat with them or by adding them to groups. This is useful for chat bots or news bots like the official TechCrunch bot.
- Send requests directly from the input field by typing the bot's @username and a query. This allows sending content from inline bots directly into any chat, group or channel.

Messages, commands, and requests sent by users are passed to the software running on your servers. Our intermediary server handles all encryption and communication with the Telegram API for you. You communicate with this server via a simple HTTPS-interface that offers a simplified version of the Telegram API. We call that inter-face our Bot API.

In our bot we will implement the keyboard with the following functions:

- the location of the child;
- the history of the child's movements.

There will also be a notification system through notifications about the movement of the child. This system will be linked to the SQLite database, which will include in-formation about all students and their locations.

Algorithm 1: Telegram bot for notification about change location of the children

1. Initialization: {$N: Notification$; L: Location ; H: History; A_u: Authorized user; C: Children; P: Parent; Pa: Passwords; T_b: Telegram bot; T_m: Telegram messenger; V_u: Valid user; u_u : Unauthorized user; D_b: Database}
2. Input: {C , Pa}
3. Output: { N, L,H}
4. Set T_m & T_b
5. If $P \in V_u$ then
6. Set status as A_u
7. Else Set status as u_u
8. Endif
9. End else
10. If $A_u \cong D_b$ then
11. Set N, L and H
12. Endif

In algorithm 1, step-1 shows the initialization process of used variables. Steps 2-3 show input and output processes. In step-4, the opening process of telegram messenger and telegram bot is explained. Steps-5-7 shows the validity of the parent as a valid user, if the parent is a valid user then the parent is declared as an authorized user. In case, the parent is not authorized to access the database then the parent is not allowed to access the database and will be declared as an unauthorized user. Steps 10-11 show once parents are allowed to have access to the database then parents are capable to receive a notification, location status and history regarding their children. Working process of the telegram bot is explained in the figure 1.

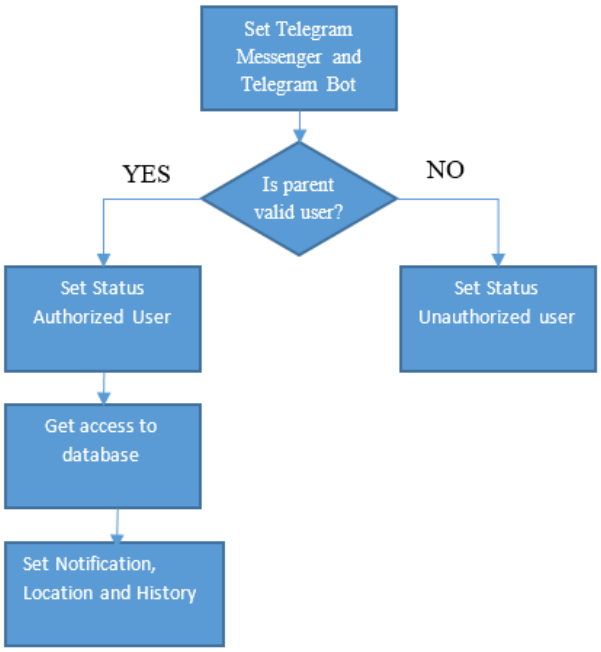


Figure 1: Algorithm of telegram bot

Algorithm 2: Authentication and Authorization process

1. Initialization: { U_n: Username; P: Password; A_U: Authorized user; D_b: Database; U: User; U_u: Unauthorized User; T_b: Telegram bot; T_m: Telegram messenger;}
2. Input: {U_n, P}
3. Output: {T_b }
4. Set T_m
5. $If\ (U_n\ \&\ P) \in\ D_b$ then
6. Set status as A_u
7. $Else\ Set\ status$ Else Set status as U_u
8. Endif
9. End else
10. If $A_u \cong D_b$ then
11. Set T_b
12. Endif

In algorithm 2, step-1 shows the initialization process of used variables. Steps 2-3 show input and output processes. In step-4, the opening process of telegram messenger is explained. Steps-5-7 shows the validity of a password and username. If password and username are in the database, then set status as an authorized user. In case, password and username are not in the database, then set status as an unauthorized user. Steps 10-11 show once the user is allowed to have access to the database then the user is capable to access Telegram Bot. Figure 2 also illustrates the authorization process.

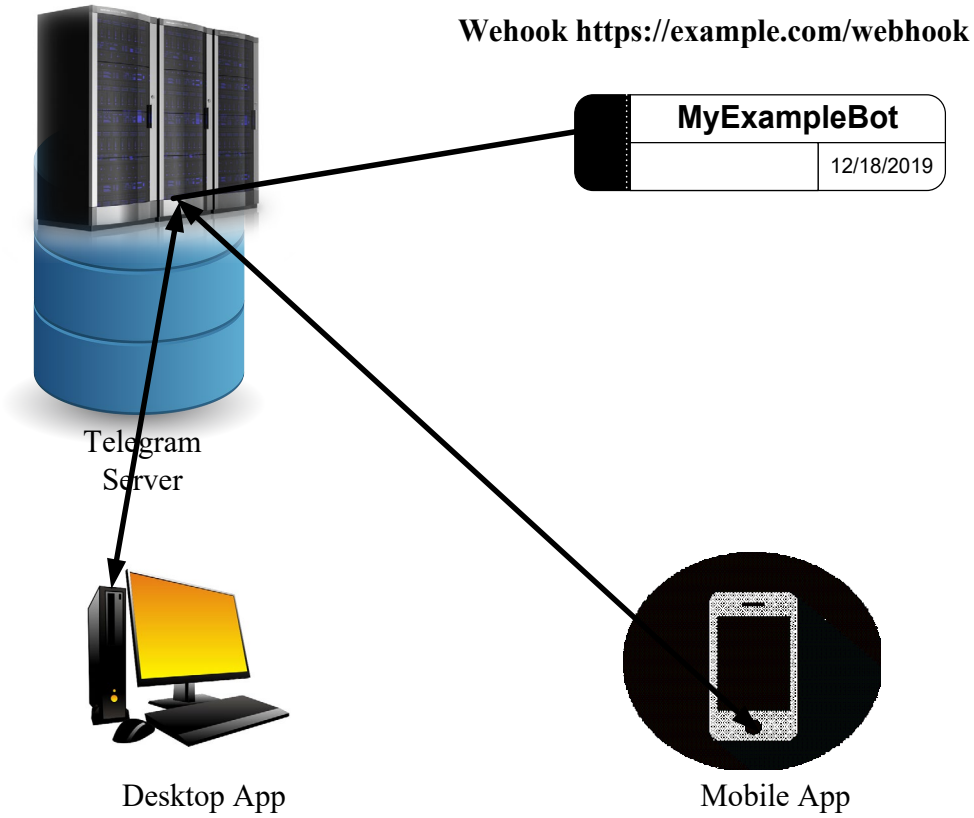


Figure 2: Authorization process

When user logs in Telegram bot, Telegram messenger sends request to security system database to verify ability to access. Telegram messenger compares entered username and password with stored in database. Then the system sends answer to user and allows or disallows access to Telegram bot.

V. Implementation and result

In the beginning, we imported libraries for telegram bot, initialized API and imported Token of Bot and created a function for the update, which can be seen in Table 1.

Entering the getBotUsername () and getBotToken () methods, we launch the bot. It all works efficiently: when we start the application, it starts sending the number of seconds to the Telegram GET server using URL: https://api.telegram.org/BotToken/getMe, where BotToken is our bot's token. In response, JSON, which contains all the messages. Each message is processed by the library and comes to the OnUpdateReceived (Update update) method by the Up-date object.

Table 1: Pseudocode for Update

```
import org.telegram.telegrambots.api.objects.Update;
import org.telegram.telegrambots.bots.TelegramLongPollingBot;

public class Example extends TelegramLongPollingBot{
      public static void main(String[] args) {
            ApiContextInitializer.init();
            TelegramBotsApi botapi = new TelegramBotsApi();
            try {
```

```
                botapi.registerBot(new Bot());
        } catch (TelegramApiException e) {
                e.printStackTrace();
        }
        }
        @Override
        public String getBotUsername() {
                return "USER";
        }
        @Override
        public void onUpdateReceived(Update e) {

        }
        @Override
        public String getBotToken() {
                return "YOUR_BOT_TOKEN";
        } }
```

Further, we created a function, which replays on incoming text. Also, we configured bot to distinguish users, which can be seen in Table 2.

Table 2: Pseudocode for distinguishing the users

```
private void sendMsg(Message msg, String text) {
                SendMessage s = new SendMessage();
                s.setChatId(msg.getChatId());
                s.setText(text);
                try {
                        sendMessage(s);
                } catch (TelegramApiException e){
                        e.printStackTrace();
        }
```

Then we configured hello message of our bot after command /start. Hello message. It performs the following functions:

- the notification about location of the child;
- the history of the child's movements."

Creation of hello message can be seen in Table 3.

Table 3: Pseudocode for Hello message creation

```
Message msg = e.getMessage();
        String txt = msg.getText();
        if (txt.equals("/start")) {
                sendMsg(msg, "It is a part of school security system.      \n
It will perform the following functions:
\n- the notification about  location of the child;
\n- the history of the child's movements.");
        }
```

Then for comfortable usage, we have created keyboard for log in, which can be seen in Table 4.

Table 4: Pseudocode for User friendly Keyboard Login

```
public synchronized void setButtons(SendMessage sendMessage) {
    ReplyKeyboardMarkup replyKeyboardMarkup = new ReplyKeyboardMarkup();
      sendMessage.setReplyMarkup(replyKeyboardMarkup);
      replyKeyboardMarkup.setSelective(true);
      replyKeyboardMarkup.setResizeKeyboard(true);
      replyKeyboardMarkup.setOneTimeKeyboard(false);

      List<KeyboardRow> keyboard = new ArrayList<>();
      KeyboardRow keyboardFirstRow = new KeyboardRow();
      keyboardFirstRow.add(new KeyboardButton("Log in"));
```

It requires the password from user to ensure the authentication process. Then we have configured answers for other commands, as notifications about changing a child's location, ability to show coordinates on the map, access to person-al information via the bot. Interface of the bot can be seen in Figure 3. Table 5 shows used tools and specifications.

Figure 3: Showing Bot Interface

Table 5: Used tools and specifications.

Tools	Specification
Programming Language	Java
IDE	IntelliJ IDEA
Operating System	Windows 10
CPU	Intel Core i5-8250U
RAM	8 GB
ROM	SSD 250 GB

By implementing a telegram bot, we overcame ss7 vulnerability in RFID Security System and provided se-cure transmission of data. During testing process, Bot successfully performed its functions like sending notifications, providing history and location, results are depicted in the figure 4. However, there were some delays observed during testing process which are the limitations of the project.

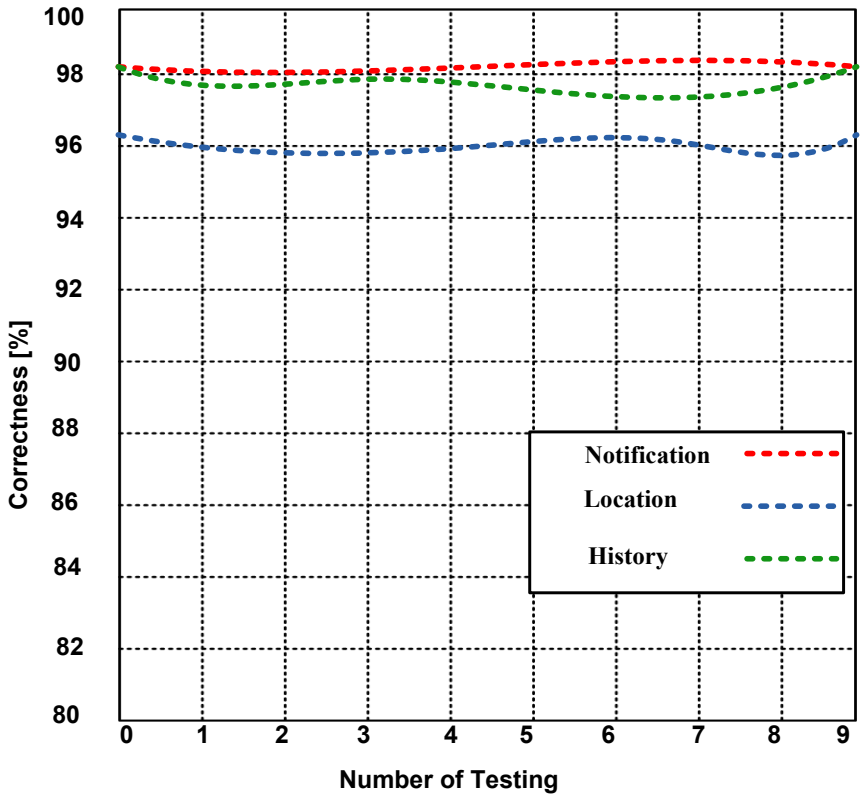


Figure 4: Showing test process

VI. Conclusion

The student monitoring system using RFID has been introduced in this paper. The developed school administration system is a good example of RFID technology usage in the educational domain. It is expected to reduce the manual effort spent on school management and facilitate the student-supervision by providing school administrators with an alternative tool. With the aid of the proposed system, time-consuming and repetitive tasks, human-made mistakes are reduced and security is improved. Thus, it can be concluded that this system can help schools and parents to monitor their children. In today's world, the most important is to maintain the safety. Therefore, Telegram Bot is one of the best solutions of protection in combination with the widely used RFID system.

References

1. Tastan, Nurbek, Abdul Razaque, Mohamed Ben Haj Frej, Amanzholova Saule Toksanovna, Raouf M. Ganda, and Fathi Amsaad. "Burglary Detection Framework for House Crime Control." In *2019 19th* International Conference on Computational Science and Its Applications (ICCSA), pp. 152-157. IEEE, 2019.

2. In Texas, 28,000 Students Test an Electronic Eye". Retrieved from https://www.nytimes.com/2004/11/17/technology/in-texas-28000-students-test-an-electronic-eye.html

3. Akpınar, S., & Kaptan, H. (2010). Computer aided school administration system using RFID technolo-gy. Procedia-Social and Behavioral Sciences, 2(2), 4392-4397.

4. Welch, Bill. "Exploiting the weaknesses of SS7." Net-work Security 2017.1 (2017): 17-19.

5. Lorenz, G., Moore, T., Manes, G., Hale, J., & Shenoi, S. (2001, June). Securing ss7 telecommunications net-works. In Workshop on Information Assurance and Security (Vol. 2, p. 1115).

6. Jakobsen, J., & Orlandi, C. (2016, October). On the CCA (in) security of MTProto. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 113-116). ACM.

7. Jakobsen, J. B., & Orlandi, C. (2015). A practical crypt-analysis of the Telegram messaging protocol (Doctoral dissertation, PhD thesis, Master Thesis, Aarhus University (Available on request)).

8. "FAQ for the Technically Inclined". Telegram. Retrieved from https://core.telegram.org/techfaq

9. Number of mobile phone messaging app users world-wide from 2016 to 2021 (2017). Retrieved from https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/

10. Vidyasagar, K., G. Balaji, and K. Narendra Reddy. "RFID-GSM imparted School children Security Sys-tem." Communications on Applied Electronics (CAE),ISSN (2015): 2394-4714.

11. Shah, Shraddha, and Bharti Singh. "RFID based school bus tracking and security system." 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2016.

12. Kamalraj, R., Mr P. Jayaram, and Mr ES Madhan. "Child Safety and Security System in School Zone using Smart Watch and RFID." International Journal of Pure and Applied Mathematics 118.18 (2018): 2523-2529.

13. Kitsos, Paris, and Yan Zhang. RFID security. Vol. 233. Springer Science+ Business Media, LLC, 2008.

14. Batina, Lejla, et al. "Public-key cryptography for RFID tags and applications." RFID Security. Springer, Boston, MA, 2008. 317-348.

15. Israsena, P., and S. Wongnamkum. "Hardware imple-mentation of a TEA-based lightweight encryption for RFID security." RFID Security. Springer, Boston, MA, 2008. 417-433.

SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Zhukabayeva T.K[1]., Abdildayeva A.A.[1],Mardenov E.M.[1], Khu Ven–Tsen[2]
tamara_kokenovna@mail.ru, abass_81@mail.ru, uvideooperator@mail.ru
Institute of Information and Computing Technologies [1]
South Kazakhstan State University[2]
Nur-Sultan, Kazakhstan

Abstract: *Wireless sensor networks (WSN) consist of a large number of sensor nodes with wireless communication capabilities that have the property of self-organization and use sensors to monitor various processes. With the rapid development of microelectronics, computer technology and wireless technology, with the growth of WSN, information security in these networks is a new and urgent task. However, the openness and tight deployment environment of information carriers has led to large hidden threats to WSN security and seriously limited the use of wireless sensor networks. Routing and topology management are important parts of a wireless sensor network. Therefore, the creation of an effective model for assessing the security of routing WSN and a model for quantifying the safety of topology, improving the security of routing control, topology and effective risk management have become an urgent research topic. Assessing the security of routing and WSN topology is of great importance. On the one hand, effective criteria for evaluating network attacks and detection methods can enhance the performance of the WSN network, thereby improving the system's ability to respond to various attacks in complex environments. On the other hand, when it comes to malicious attacks by the enemy, routing attack assessment technology and topology security assessment can provide appropriate countermeasures for a network counterattack.*

Keywords*: wireless sensor networks, information security, agent-based modeling, denial of service cyberattack.*

WSN is an advanced network technology, it differs significantly from traditional wireless networks. This is due to the unique characteristics of the node sensors in the WSN. Thus, the existing security mechanisms of traditional wireless networks are not applied directly to the WSN. Due to various resource and processing power limitations, the use of wireless sensor networks is accompanied by the need to solve additional problematic issues of ensuring information security. In particular, one of the most common attacks that affect resource consumption is routing attacks. Routing attacks are carried out at the Network layer of the OSI model. Such attacks are aimed at preventing the routing protocol from working correctly and ceasing to perform its functions [1-3]. In addition, most routing attacks affect the resources used by the wireless network, such as electricity, memory, bandwidth, and processing power. As a result of attacks Table 1, attackers can disrupt routing mechanisms, collect a large amount of traffic on one network node, introduce serious network congestion, direct data packets along an non-optimal path, selectively delete certain data packets, destroy all data packets on a certain node, and disrupt data storage mechanisms.

Types of attacks	Attack description
Hello flood attack	The hostile node transmits information with a sufficiently powerful signal, thus demonstrating that it is the nearest neighbor

Wormhole attack	A hostile host intercepts information and transfers it to another hostile host located in another part of the network. This transmission is carried out of the channel band
Detour attack	An attacker may try to direct traffic bypassing the main path, less optimal
Sinkhole attack	The hostile node convinces neighboring nodes by sending routing messages that it is the best node to continue transmitting the packet to the base station
Black hole attack	The hostile node destroys all the data that is sent to it by other nodes. Selective Forwarding. The hostile node removes only part of the packets, the rest of the packets broadcast correctly
Sybil Attack	n this type of attack, a malicious node creates the illusion of traffic congestion, requiring multiple identifiers. This not only creates an illusion, but also makes it possible to enter false information into the network using a number of fabricated non-existent vehicles; It can even launch further DoS attacks, disrupting the normal operation of data distribution protocols
Looping	Usually carried out using attacks gathering point and bypass. The attack is aimed at routing the network and depleting the node energy.
Rush- Attack	The enemy host sends a route path request message and quickly repeats these messages throughout the network
Attacks that use bypass schemes for broken nodes.	Attacks that exploit vulnerabilities in routing algorithms, in which there are techniques to avoid the use of nodes with low performance or power supplies in order to have a better chance of packet delivery
Attacks aimed at depleting network resources.	When the nodes are not constantly serviced and rely only on their limited resources, an attacker may try to deplete them in order to undermine the network
Jamming attack	The malicious node transmits signals, thereby disrupting communication, reducing the signal-to-noise ratio
Dos attack	machine or network, making it inaccessible to its intended users by flooding it with traffic

Table 1 - The main types of attacks on the WSN

Despite the fact that there are many methods for assessing WSN performance, none of these methods is aimed at optimizing the sensor deployment strategy to provide greater resistance to cyber attacks.

For WSN, there are many routing protocols that can be divided into flat routing, hierarchical routing, and location-based routing [4]. This study simulates location-based routing, which uses the physical location of a sensor node in a network to determine routing. The nearest neighbor is randomly simulated, which allows the sending node to randomly select

the node closer to the receiver and forward the packet to it. This strategy minimizes the accuracy of information needed by neighbors, thereby reducing the number of operations required to send a packet [5].

Protecting against network layer DoS attacks is a complex and ongoing area of research. There are several algorithms for detecting black holes and other intrusions into the network [6,7], but all of them require significant energy and complexity. In addition, many of these methods become less effective when several nodes in the network are compromised or when the node uses intelligent selective forwarding. Excessive routing of messages over non-intersecting paths reduces the risk that the node blocks messages to the receiver, but consumes energy and bandwidth. In addition, it may be difficult or impossible to achieve redundancy in a sparse network [8]. A single sensor node can be compromised in various ways, such as physical attacks and attacks of false nodes [3] These attacks can allow an attacker to gain a foothold in the network. Based on this, we assume that an attacker can spread the exploit from a compromised sensor node to a healthy one. Thus, the number of nodes acting as black holes increases and attacks spread.

Routing is performed by a series of autonomous decisions made by the corresponding node at each transition of the route. We use a protocol that selects one of n connected neighbors with a probability of 1 / n and forwards the message to this node [9,10];

Each node is connected to each of its neighboring nodes by directional communication. A node is a neighbor if it is in the indicated range of radio communication, and a connection is formed from the node with any neighbors that are closer to the nearest receiver at a distance in a straight line [11,12]. The exception is that if the node has a receiver within its radio range, then it only forms a link to the receiver. An example shows that the receiver is in the center of the region; therefore, the general form of each simulation was the distribution of nodes around the receiver with links pointing to the center, as shown in Fig. 2.

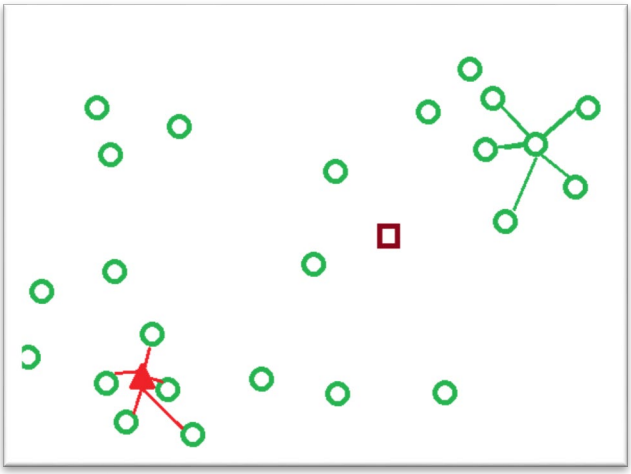


Figure 2- An example of a WSN model.

The proposed simulation model of the WSN has been implemented in NetLogo. Where we illustrated the use of this model with an example in which an attacker launches a DoS attack on a network and compare network performance based on a deployment strategy. Modeling is performed with N = 250, 62 5 and 1000, and σ = 20, 25 and 30. These values were chosen based on the results of preliminary experiments. Each of these combinations starts with five different random initial values, a total of 120 runs, including runs with a uniform distribution. These results are averaged to obtain a more complete picture of the behavior space.

When the attack reaches the final stage, the rarest network actually has the best coverage [3,13]. A sparse network makes an attack more difficult to compromise and therefore more resistant to attack than dense networks. Table 1 shows a comparison of the percentages of a network that has been hacked over time. The percentage of compromised nodes in the network is significantly higher in a denser network. As a result, the impact on coverage is greater. Limiting the number of nodes in the network, for a certain environment, WSN limit the damage that can be achieved by types of DoS attacks.

Step	N = 250	N = 625	N = 1000
30	8%	7%	7%
60	13%	16%	16%
90	15%	21	22%

Table 1 - Nodes compromised by network size

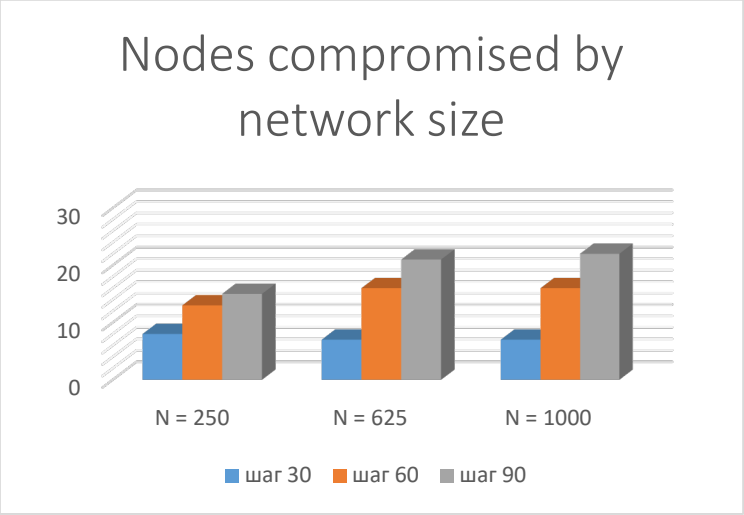


Figure 3 - Nodes compromised by network size

Conclusion

Security concerns in WSN arise due to the limited capabilities of the sensor nodes used in many crucial applications. Deploying sensor nodes in an automated environment makes networks vulnerable. Sensor networks are fundamentally different from traditional wired networks as well as wireless networks. Security is an important feature for deploying WSN. The paper shows the attacks and their classification in the WSN, and also provides a general overview of various security threats. Thus, we are directly dependent on security issues. The obvious solution is to eliminate technological disadvantages.

Reference

1. Wagner, N., C. ¸S. ¸Sahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, and W. W. Streilein. 2016. “Towards automated cyber decision support: A case study on network segmentation for security”. In Computational Intelligence (SSCI), 2016 IEEE Symposium Series on, pp. 1–10. IEEE.

2. Oliveira, L. B., A. Ferreira, M. A. Vilaça, H. C. Wong, M. Bern.. “SecLEACH—On the security of clustered sensor networks”. Signal Processing vol. 87, 2007, pp. 2882– 2895.

3. Brian Yarbrough, Neal Wagner. ASSESSING SECURITY RISK FOR WIRELESS SENSOR NETWORKS UNDER CYBER ATTACK

4. Al-Karaki, J. N., and A. E. Kamal. “Routing techniques in wireless sensor networks: a survey”. IEEE Wireless Communications vol. 11 (6), pp. 6–28.

5. Karlof, C., and D. Wagner. 2003. “Secure routing in wireless sensor networks: Attacks and countermeasures”. Ad Hoc Networks vol. 1 (2), 2004, pp. 293–315.

6. Шахов В.В, Юргенсон А.Н., Соколова О.Д., Моделирование воздействия атаки Black Hole на беспроводные сети № 1 за 2017 год. Стр. 34-39]

7. Butun, I., S. D. Morgera, and R. Sankar. 2014. “A survey of intrusion detection systems in wireless sensor networks”. IEEE Communications Surveys & Tutorials vol. 16 (1), pp. 266–282.

8. Raymond, D. R., and S. F. Midkiff. 2008. “Denial-of-service in wireless sensor networks: Attacks and defenses”. IEEE Pervasive Computing vol. 7 (1).

9. Borshchev, A., and A. Filippov. 2004. “From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools”. In Proceedings of the 22nd International Conference of the System Dynamics Society, Volume 22. XJ Technologies.

10. Nelson, R., and L. Kleinrock. 1984. “The spatial capacity of a slotted ALOHA multihop packet radio network with capture”. IEEE Transactions on Communications vol. 32 (6), pp. 684–694.

11. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Ad hoc networks, vol. 1, no. 2, pp. 293–315, 2003.

12. Антонов А.Ю. Обзор и анализ проблематики обеспечения информационной безопасности в беспроводных сенсорных сетях. Научно-практический семинар "Новые информационные технологии в автоматизированных системах" 2017

13. 曾　玲，王　伟. 水下传感器网络的安全保密体系研究, 2019

ЭЛЕКТРОНДЫҚ САУДАНЫҢ ИНТЕГРАЦИЯЛАНҒАН АҚПАРАТТЫҚ ЖҮЙЕСІ

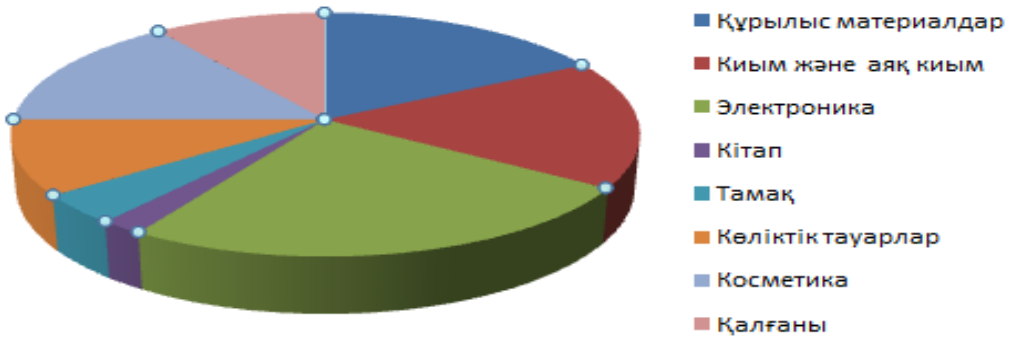
Абуов Б.Б.
e-mail: abuovbb@narxoz.kz
АҚ «Нархоз» Университеті, Қазақстан

Аңдатпа. *Мақалада электрондық сауданың дамуының факторлары жазылған. Ақпараттық технологияларды саудада қолданудың негізгі мәселелері қарастырылды. Қазақстандағы интернет дүкенінде сатылатын тауар туралы, оның пайыздық деңгейі айтылған. Ақпараттық жүйені құрудың негізгі кезеңдері сипатталған, интернет-дүкеннің әдеттегімен салыстырмалы талдау берілген. Клиент пен интернет-дүкен администраторы құрған ақпарат ағындары туралы көсетіледі. Олардың атқаратың функциялары берілген.*

Заманауи ақпараттық технологиялар (IT) негізінде электрондық коммерция қарқынды дамып келеді және жаһандық экономикадағы инновацияның маңызды факторы ретінде қарастырылады. Сауданың ауқымдану процестері нарықтың ірі операторларына айналымды ұлғайту және жалпы ресурстарды бөлу арқылы шығындарды азайту мақсатында көп брендті дүкендер мен гипермаркеттер құруда

жетекші болып табылады. Жаңа тенденциялар ЕС-де көрініс табады. Бұл тақырып бүгінде өзекті болып саналады, өйткені бүгінгі күні миллиондаған адамдар үйден шықпай, әртүрлі тауарларды электронды дүкендерде сатып алады. Әлемде, атап айтқанда Қазақстанда, интернет пайдаланушыларының саны өсіп келеді, нәтижесінде «электронды» сатып алушылар, әлеуетті «электронды» сатып алушылар саны артып келеді. Компаниялардың шоғырлануына, интернет-дүкендердің пайда болуына және гипермаркеттер қарқынын арттыруға және көптеген интернет-дүкендерге негізделген сауда стратегиясын саралауға мүмкіндік береді. Электронды сауда жүйесінің тиімділігі тікелей байланысты болатын ірі бизнес-процестерді автоматтандыру ірі кәсіпорындар үшін ең қиын мәселелердің бірі болып қала береді.

Ірі масштабты электрондық сауда жүйелерін, ақпараттық технологиялармен тиімді қолдау, ақпараттық желілердің (АЖ) архитектурасы мен мүмкіндігіне байланысты. Олар желілік сауда нүктелерін құруға бағытталған емес. Жаңа интернет-дүкендердің ашылуы, әдетте, IT-инфрақұрылымның қайталануымен жүреді, бұл қолдау шығындарының өсуіне әкеледі. Сауда ассортименті мен жеткізілім тізбегін қалыптастыруды автоматтандыру үшін логистикалық процестерді оңтайландыру және жүйелеу мүмкіндіктері жеткіліксіз пайдаланылады. Сондықтан қазір жылдан жылға ол жүйені одан әрі дамыту тез қозғалып келе жатыр. Өйткені электронды дүкендер өндірушінің шығындарын едәуір азайтады, тұрақты дүкенді ұстауға, сату нарықтарын кеңейтуге, сондай-ақ сатып алушының кез-келген өнімді кез-келген уақытта, кез-келген елде, қалада, күннің кез келген уақытында, жылдың кез келген уақытында сатып алу мүмкіндігін кеңейтеді. Статистикаға қарасақ интернетті ақпарат іздейтіндер үшін ғана емес, сонымен қатар интернеттен сатып алатындар саны да өсуде. Қазақстан Республикасы Экономика министрлігі Статистика комитетінің мәліметтері бойынша, Қазақстанның интернет-саудасындағы ең танымал тауар санаттары - электроника мен киім. Бұл екі сегмент онлайн сатып алудың жартысынан көбін құрайды. Тауарлардың басқа да санаттары үшін интернет-коммерцияға сұраныс артып келеді. Бүгінде олар Интернетте кез-келген нәрсені, соның ішінде киім, тұрмыстық заттар, ойыншықтар мен балалар тауарлары, тамақ, ондай тұрмақ көлікке дейін сатып алады(1-сурет).

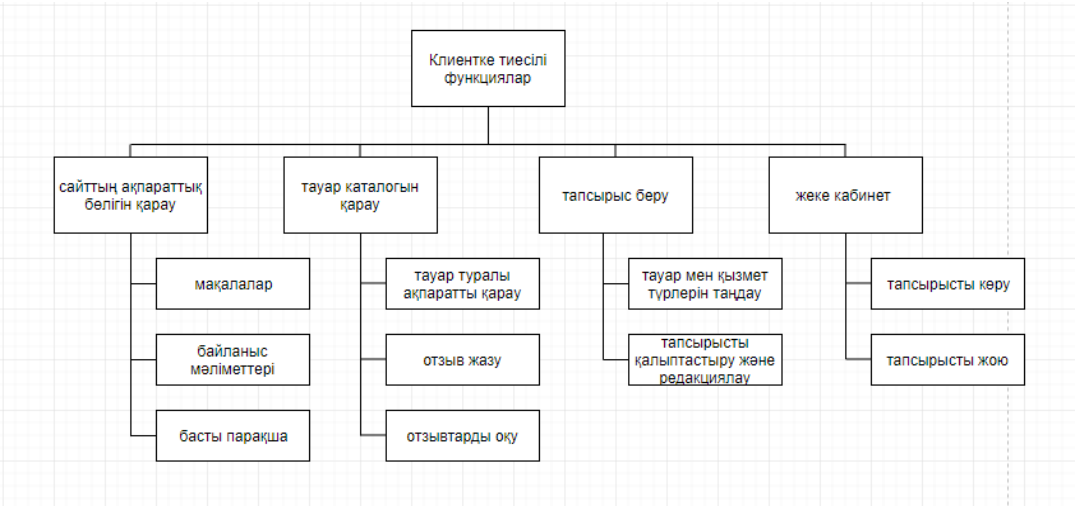


1-сурет – Интернетте сатылатын тауарлардың пайырдық көрсеткіші

Интернеттік сауда компаниясы үшін ақпараттық жүйені дамыту кезінде шешілетін маңызды міндет - басты вируалды дүкенімен мен дүкендер желісінің бағдарламалары

арасында ақпарат алмасу. Ақпаратты беру жүйенің осы бөліктері арасында дәл жүреді. Сауда орталықтары тауарларды сату туралы ақпаратты кассалық аппараттан алады. Тауарлардың ассортименті, олардың бағасы, сондай-ақ тауарларды сатудың әртүрлі шарттары туралы мәліметтер негізгі кеңседен сауда нүктелеріне жіберіледі, дәл сол мәліметтер интернет-дүкенде де көрсетіледі және өзгерген ақпаратты әрқашан нақты уақыт режимінде көрсетеді. Осылайша, барлық сауда нүктелері интернет-дүкенге автоматты түрде қосылады және шығындар, сондай-ақ ақпаратты беру уақыты азаяды.

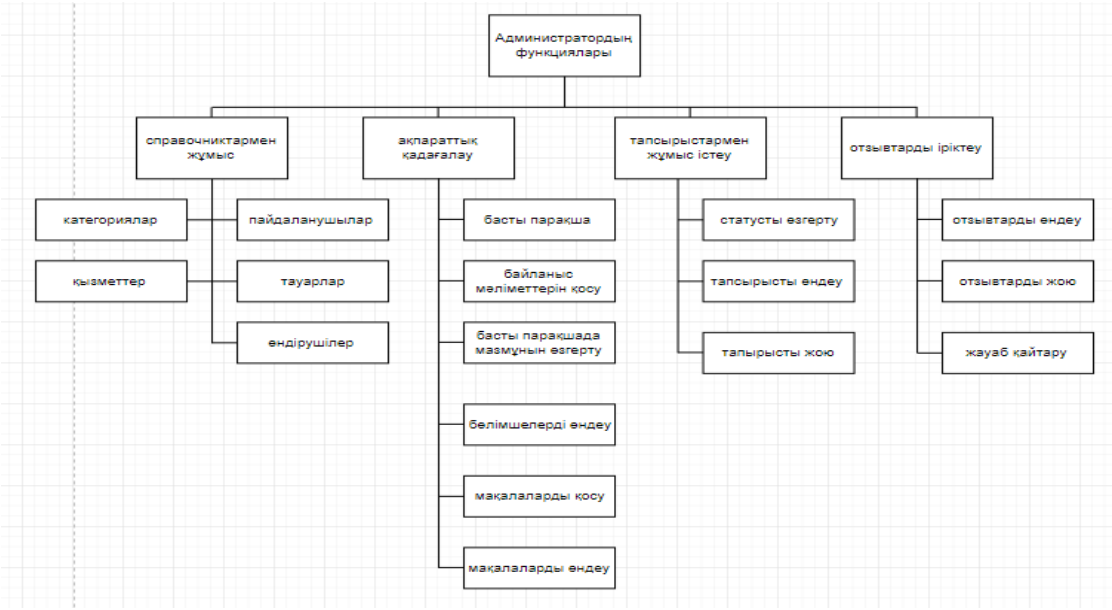
Әдетте көптеген шағын интернет магазиндері өздерінің түсіп жатқан ақпараттарын автоматтандыру үшін, ірі магазиндерден қарағанда, шет бағдарламаларды пайдаланады. Оның шешудің тиімді жолдарының бірі, ол магазиннің интерфейсін құрастыру сатысында бүкіл керекті функцияларын енгізу қажет. Ең бастыларының бірі пайланушыға магазинді пайдалану тәсілдерін максималды түрде жеңілдету. Бәріне белгілідей егер клиент мәз болған жағдайда оның осы интернет-магазинді қайтіп пайдалану болжамы арта түседі. Сол үшін интернет дүкен архитектурасы клиенттік бөлігінде интернет-дүкеннің беттерінде әлеуетті клиенттің ең ыңғайлы және қол жетімді жұмысы жасалынады. Логикасын құру, қол жетімді және анық диалогтық терезелер, ыңғайлы төлемдер мен жеткізу жүйелерінен тұрады. Өзіңіз білетіндей клиент дүкенге барған кезде өнімдерді таңдайды, басқа пайдаланушылардың пікірлерімен танысады, шолудан шығуға мүмкіндігі бар, тауарды тапсырысқа қосады, тапсырысқа қызмет атауын қосады. Тапсырысқа тауарлар қосқан кезде алдын ала тапсырыстар сақталатын себет кестесі жасалады. Себеттегі тауарлардың тізіміне сүйене отырып, тапсырыс құрамын немесе тапсырыстағы әр заттың мөлшерін өзгерту мүмкіндігі бар тұтынушы тапсырыстың жалпы құнын алады. Бұлар клиентке тиесілі ең қарапайым функциялардың бірі(2-сурет). Барлығын суреттен қарауға болады:



2-сурет – Клиенттің функциялары

Интернет дүкенді құрастыру кезінде ақпараттық жүйесін автоматтандыру алдында анализ жүргізу қажет. Бөлек функционалын құрастыру керек. Оның ішіне қойманы автоматтандыру, жұмыс процесі документтері, бухгалтерлік есеп, баға тізімдері мен тауарларды автоматты түрде түсіру, авто баға, тұтынушылардың деректерін жинау және тағыда басқа функционалдық әрекеттер атқарылатындай болуы қажет. Олар администраторға тиесілі болады Администратор бөлігі интернет-дүкенді басқаруға

арналған құралдардан тұрады және дүкеннің жалпы параметрлерін де, арнайы параметрлерді де қамтиды. Нақтырақ айтқанда, платформаның жұмысы келесідей. Парақшаның тиісті формаларын қолдана отырып, администратор Прайс-лист құжатының негізінде өндірушілердің, санаттардың, өнімдердің дирекцияларын толтырады. Сондай-ақ, администратор веб-өкілдіктің статистикалық парақтарын толтырады, оған компаниялар, байланыстар, ақпарат және т.б. сияқты мәліметтер кіреді. Сонымен қатар, администратор қызмет дирекцияларын, пайдаланушыларды, пайдаланушы рөлдерін толтырады. Администратордың функциялары анықтамалықтарды толтырудан және олармен әрі қарай жұмыс істеуден тұрады. Оның барлығы платформа администраторының жеке кабинетіне кіру керек. Администратор функцияларының ағашы 3-суретте көрсетілген.



3-сурет – Администратордың функциялары

Одан басқа тағыда, модератордың негізгі функциясы бар - бұл өнімнің каталогын жаңартып отыру. Оператордың негізгі міндеті - кіріс тапсырыстарды өңдеу, олардың мәртебесі, орындалуы және т.б.(3-сурет).

Қорыта келе, экономиканың қарқынды дамуы, жаңа техникалық мүмкіндіктердің пайда болуы экономикаға, атап айтқанда, сауда қызметінде жаңа технологияларды енгізуге байланысты мәселелерді зерттеуді талап етеді. Ғаламдық желіні (Интернет) құру нәтижесінде пайда болған бизнесті жүргізуге арналған жаңа «сандық» кеңістіктің пайда болуы кәсіпорындардың тауарларды, қызметтерді сату мүмкіндіктерін және олардың мердігерлермен, банктермен, қаржылық қызметтермен және клиенттермен өзара әрекеттесу мүмкіндіктерін кеңейе түсті. Пайдаланушылар интернеттегі тауарлар мен сатып алулар туралы ақпаратты көбірек іздеп қана қоймайды, сонымен қатар интернетте сатып алуға көбірек дайын. Сонымен бірге, тұтынушылар біртіндеп екеуін де, соның ішінде ұялы телефонды да жасауға дағдыланады.

Әдебиеттер

1. Допира Р.И., Попова Н.В., Базикова К.М. Технология разработки интернет-магазина // Научный журнал. — 2016. — № 1 (2). — С. 9-11.
2. Рейнольдс М. Электронная коммерция. — М.: Лори, 2010. -560 с.

ҮЛКЕН ДЕРЕКТЕРДІ (BIG DATA) ЗЕРТТЕУДІҢ МАҢЫЗДЫЛЫҒЫ

Бисаринов Б.Ж., Бисаринова А.Т.
e-mail: bbaituma@gmail.com, aigulbis@mail.ru
аль-Фараби атындағы Қазақ Ұлттық университет,
«Халықаралық ақпараттық технологиялар университеті» АҚ,
Қазақстан

Андатпа. *Үлкен деректер талдауы бүгінгі күні барлық салаларда басты назарда. Кәсіпорын «Үлкен деректер» талдамасын пайдаланбаса, өз бизнестерінде үлкен деректерге қарсы бәсекелестерге қарсы тұра алмайды. Үлкен деректер талдауы бизнестің алдын-ала деректер мен үрдістер туралы іскерлік түсініктерді анықтап, өз салаларында бәсекелестік артықшылығын жасауға мүмкіндік береді. Мақалада Big Data талдаулар саласында жасалынған заманауи жұмыстарын қарастыру және Big Data мен Smart Computing-нің ғылыми-зерттеу салалары қарастырылады. Бүгінгі таңда аталмыш зерттеу саласына компьютерлік ғылымдар мен ақпараттық технология қызғушылық танытуда. Аталмыш сала әлеуметтік ғылымдар және басқада пәндерде кеңінен сұраныста және ұжымдық кластерлік талдауды да кеңінен қолдану өзекті болып отыр.*

Түйін сөздер: *Үлкен деректер (Big Data), Big Data Analytics (BDA), Data Science, интернет заттары (IoT), Hadoop, SAP HANA.*

Деректер ғылымы (Data Science), деректерді сұрыптау, пайдалану, өңдеу және талдаумен байланысты ғылыми саланы қамтиды. Деректер ілімі - көптеген ғылыми әдістер қолданылатын кең мағыналы, алыстан бастау алып, тереңді қозғайтын термин. Математика, статистика және басқа көптеген сала ғылымдары осы деректер жиындарына сүйеніп жұмыс жасайды және оның нәтижелерін кеңінен қолданылады. Зерттеуші ғалым мәліметтерді жалпы деректерден алу үшін түрлі құралдарды қолданады. «Үлкен деректер (Big Data)» термині салыстырмалы түрде жаңа болып табылады. 2000-жылдардың басында осы саланың талдаушысы Даг Лейн үлкен деректердің қазіргі кездегі негізгі анықтамасын үш -Vs (көлемі, жылдамдық, әртүрлілік) ретінде белгілеген кезде ерекше серпіліс алғаны бәрәмізгеде мәлім. Сарапшылардың көпшілігі үш өлшемді деңгейді пайдаланады[1]. Деректеріңіздің дерекқорларында келесі сипаттамалар бар: *Көлемі*: Үлкен деректер - бұл деректер жинағы немесе оны өңдеуге қатысты қиындықтарға тап болатын ұйымның үлкен деректер жиынтығы. Іс жүзінде электронды коммерция, ұтқырлық, әлеуметтік медиа және Интернет заттар (ИЗ) сияқты трендтер соншалықты көп ақпарат жасайды, сол себепті әрбір ұйым осы өлшемге сай келеді. *Жылдамдық:* Ұйым жылдам деректермен жаңа деректер жасаса және нақты уақытта жауап беруі қажет болса, үлкен деректерге байланысты жылдамдыққа ие болады. Электрондық коммерция, әлеуметтік медиа немесе ИЗ-ға қатысатын көптеген ұйымдар

осы өлшемді үлкен деректерге сай қолданады. *Әртүрлілік:* Егер сіздің деректеріңіз әртүрлі форматтарда болса, үлкен деректермен байланысты әртүрлілік бар [2].

Үлкен деректердің жапы сипаттамасы

Жалпы жағдайда соңғы кездері үлкен деректер - Big Data үшін қызығушылық тудыратын тақырыптар, салалар төмендегілерді қамтиды:

Үлкен деректерге арналған техника, модельдер және алгоритмдер,үлкен деректер үшін машиналық оқыту және жасанды зияткерлік, Веб-іздеу және ақпаратты іздеу, есептеу үшін модельдер мен құралдар, үлкен деректерге арналған бұлттық және тораптық есептеулер, үлкен деректерге арналған қауіпсіздік және құпиялық, смарт құрылғылар мен жабдықтар, үлкен деректер қосымшалары: биоинформатика, мультимедиа, смартфондар және т.б.

Үлкен деректерге арналған құралдар мен жүйелер. Деректерді өндіру, графиканы өңдеу және деректер ғылымы. Интеграция және интеллектуалды есептеулер үшін платформа.Үлкен деректерді талдау және әлеуметтік медиа.

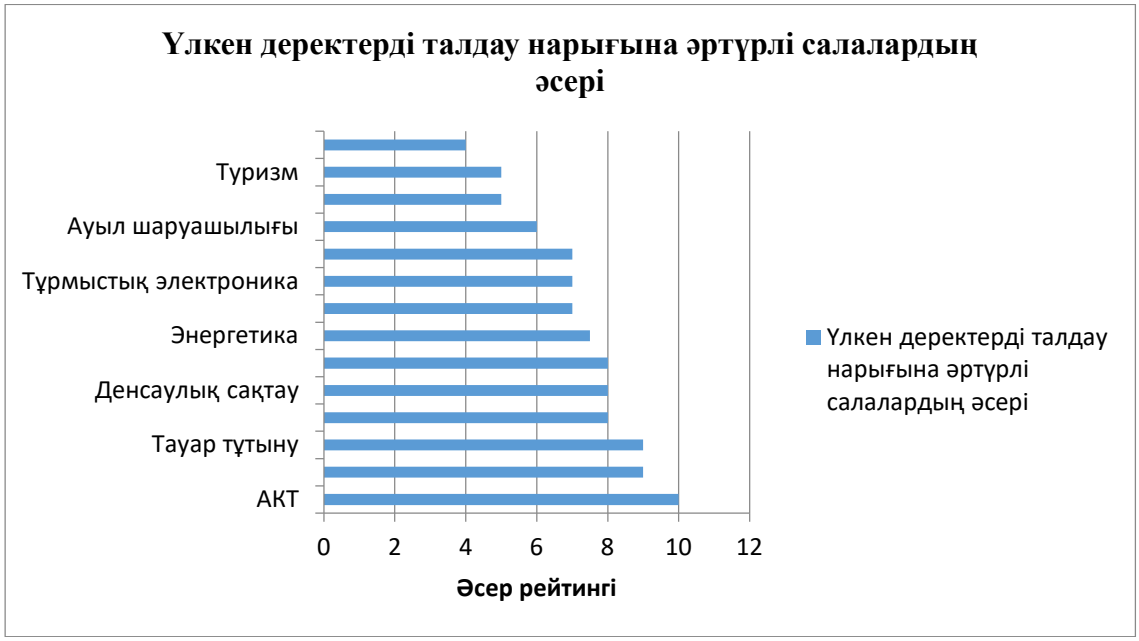
Үлкен деректерге арналған жабдық. Бағдарламалық қамтама инфрақұрылымы. Ұялы байланыс және желілер.

Big Data технологиялары

BigData жинау және өңдеу үшін пайдаланылатын технологиялар 3 топқа бөлінеді: бБағдарламалық қамтамасыз ету, жабдық, қызмет көрсету. Ең көп тараған деректерді өңдеу (бағдарламалық қамтама) тәсілдері мыналарды қамтиды: SQL, дерекқорлармен жұмыс істеуге мүмкіндік беретін құрылымдық сұраныс тілі. SQL қолдану арқылы деректерді жасауға және өзгертуге болады және деректер жиынтығын басқарылуы тиісті дерекқорды басқару жүйесі арқылы өңделеді. NoSQL - бұл термин тек SQL емес (SQL ғана емес). Ол дерекқорды басқару жүйелерінде пайдаланылатын модельдерден өзгеше дерекқорды енгізуге бағытталған бірқатар тәсілдерді қамтиды. Сонымен қатар үнемі өзгеретін деректер құрылымымен пайдалануға ыңғайлы. Мысалы, әлеуметтік желілерде ақпаратты жинау және сақтау. MapReduce - есептеуіш үлгілеу моделі. Үлкен деректер жинақтары (petabytes * және басқалары) бойынша параллель есептеулер үшін қолданылады. Бағдарлама интерфейсінде деректер өңдеуге арналған бағдарламаға берілмейді, бірақ бағдарлама деректерге ауысады. Сұраныс жеке бағдарлама болып табылады. Жұмыс принципі деректерді жүйелі түрде өңдеудің екі әдісімен және картаны қысқартудан тұрады. Карта алдын ала деректерді таңдайды. Hadoop - жоғары жүктелетін сайттардың - Facebook, eBay, Amazon және т.б. іздеу және контекстік тетіктерін іске асыру үшін пайдаланылады. Айырықша ерекшелігі, бұл жүйе кластердің кез келген түйінінің сәтсіздігінен қорғалған, себебі әрбір блок басқа түйінде деректердің кемінде бір данасы болып табылады. SAP HANA - жоғары сапалы деректерді сақтау және өңдеу NewSQL платформасы. Жоғары жылдамдықты сұрауды өңдеуді қамтамасыз етеді. Тағы бір айырмашылығы - SAP HANA жүйелік ландшафты жеңілдетеді, бұл аналитикалық жүйелерді қолдау құнын төмендетеді.

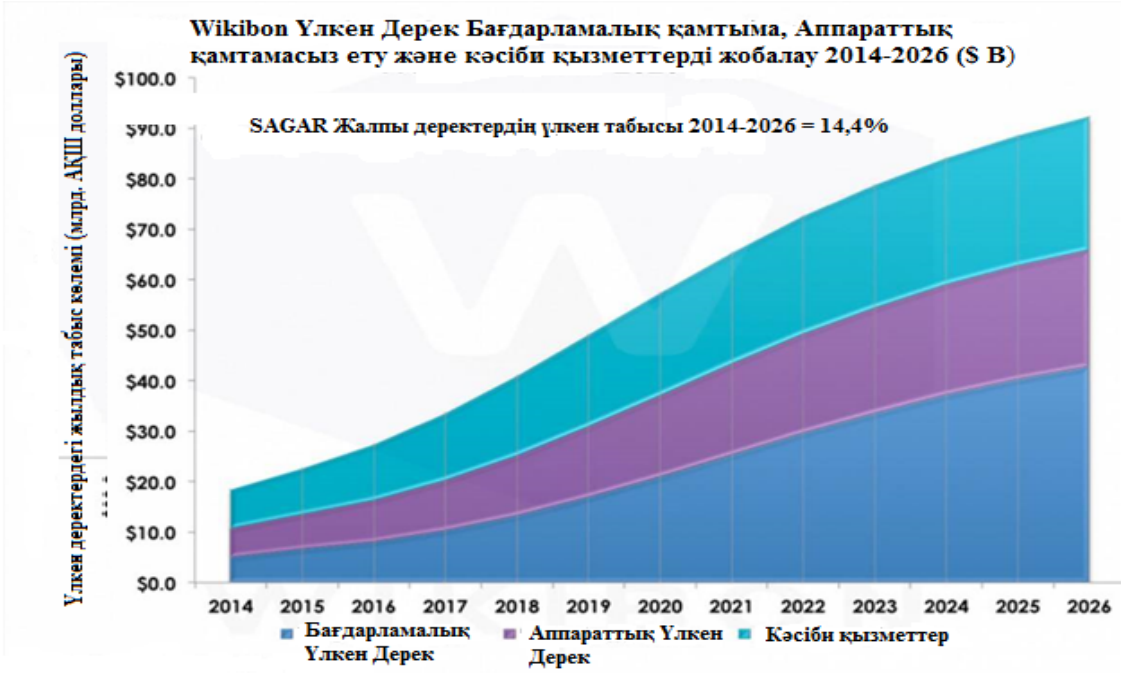
Үлкен деректерді талдау үлкен, күрделі және алдын-ала өңдеу жасалмаған деректер жиынтығын, бағалы мәліметтерді анықтауға, трендтерді дәл анықтауға, өндірістік көрсеткіштерді болжауға және шығындарды оңтайландыруға мүмкіндік береді. Өндірістік сегментте және басқа да өнеркәсіп секторларында сарапшылар BDA-ға сұраныстың артуын атап өтті, яғни үлкен деректерді талдауға салынған инвестицияның өсуі кәсіпорынның өнімділігін арттыру және ресурстарды оңтайландыру қажеттілігіне

байланысты болып отыр. Бөлшек сауда, денсаулық сақтау, банкинг және қаржы сегменттерінде соңғы бірнеше жылда BDA қолданылуда. Жақын арада жеке қызметтерді дамыту кеңінен қолданылатын болады. Қоршаған ортаны қорғау саласындағы үлкен деректер сараптамасына сұраныс жоғары болады, әсіресе Азия-Тынық мұхиты аймағындағы дамушы елдерде.



1-ші сурет. Әртүрлі салалардың үлкен деректерді талдау нарығына әсері.

Frost & Sullivan өкілдерінің айтуынша, BDA-ның қолданылуы клиенттердің қажеттіліктерін терең түсінуге мүмкіндік береді, бұл әсіресе ақылды банкинг үшін өте маңызды. Қаржылық сегментте үлкен деректерді талдау қызметтерін жекелендіру, ақпараттың бұрмалануын алдын алу, алаяқтықты анықтау және т.б. үшін пайдаланылады. Қаржыны қадағалау үшін ақшаны аударуға байланысты алаяқтық әрекеттердің алдын алуға болады.



2-ші сурет. Үлкен деректер нарығының өсуінің болжамдары.

Үлкен деректер сараптамасы жеке компаниялар мен үкіметтік ұйымдармен экологиялық тәуекелдерді бағалауға, ресурстарды пайдалануды оңтайландыруға және қоршаған ортаны қорғау ережелеріне сәйкестікті қамтамасыз етуді қарастырады. Global Forest Watch 2.0 - Дүниежүзілік Ресурстық Институтының Google Inc. компаниясымен бірлесіп іске асырған ормандарды қорғау жобаларының бірі болып табылады. Жобаның басталуынан және BDA шешімдерін енгізуден бастап, 2004 жылмен салыстырғанда, 2013 жылы Amazon-ның орансыздандыру көрсеткіші 80% -ға азайды [3].

Үлкен деректердің кереметі және нақты қауіптері

Үлкен әлеуметтік деректер деп аталатын сала бойынша көптеген зерттеулер жасалынуда. Салада төрт әлеуметтік маңызды бағыттар бар (әлеуметтік есептеу), үлкен деректер ғылымы (Big Data Science), деректерді талдауға және есептеудің әлеуметтік ғылымдарына (CSS) төрт маңызды қосалқы салалары бар. Күнделікті өмірде ағылшын тілінде BDS - Big Data Science немесе SBD, әлеуметтік үлкен деректердің ғылымы (Social Big Data) қысқарған түрдегі терминдері қолданылады. Дегенмен, «үлкен деректер» (BD) тұжырымдамасы BDS / SBD тұжырымдамасынан кеңірек. Әлеуметтік деректерді өңдеуге байланысты әртүрлі ресурстардың пайдаланушылары өздерінің деректерін пайдаланудың қайда және қалай сақталатындығына, кімге және қалай қол жеткізуге болатынына, қанша уақыт сақталатынына байланысты орынды алаңдаушылық бар. Белгілі бір технологияларды қолдану туралы мәселе олардың қолданылу мақсаттарына және тұтынушыларға қатысты. Мұнда сіз ядролық дамудың ұқсастығын жасай аласыз: атомды бейбіт мақсаттарда - ядролық энергетика үшін пайдалана аласыз және сіз атом бомбасын жасай аласыз. Сол сияқты үлкен деректерге арналған өңдеу және аналитика технологиялары қалыпты жағдайлар мен көлік апаттарының алдын алуға, жабдықтардың бұзылуын азайтуға, клиенттердің артықшылықтарын анықтауға, медициналық қызметтерге қажеттілікті анықтауға және т.б. қолданылуы мүмкін. Және сол

технологиялар адамдарға кейбір мақсаттар үшін сүзгілеуге мүмкіндік береді. Мысалы, жұмысқа орналасу. Сондай-ақ, нақты қауіп-қатерлерге азаматтардың мүдделеріне нұқсан келтіретін (қарыз алушының рейтингісі және т.б.) коммерциялық пайдалану үшін үлкен деректерді пайдалану жатады. Жылдам қарқынмен дамып келе жатқан және болашақта инвестицияның басты нысандарының бірі болудың кез-келген мүмкіндіктері - Интернеттегі зат бар екенін тағы еске ала отыруымыз керек.

Үлкен деректер (Big Data) технологиясын қолдану аясы

Бөлшек сауданың және қызмет көрсету секторының ірі және орта компанияларының Big Data технологиясын пайдалануына қызығушылығы байқалады. Бұл технологиялар банктер, ұялы байланыс операторлары белсенді пайдаланады. Бұдан басқа, ірі өндірістік компаниялардың жабдықты бұзу туралы деректерді талдау және шығындарды азайтуға мүмкіндік береді. Ұшуды басқару саласында деректер массивтерін талдау жабдықтың сенімділігін арттырады және сәтсіздік санын азайтады. Бірақ Big Data ауқымы әлдеқайда кең. Компания туралы әртүрлі ақпаратты кеңінен жариялау туралы. Тапсырылған мәліметтерді талдау, объектілердің физикалық сипаттамалары, жедел деректер, қаржылық деректер, материалдық ресурстар, заңды деректер. Ақпарат көздері: файлдық кестелер, дәстүрлі дерекқорларды басқару жүйесі (ДҚБЖ), бухгалтерлік жүйелер болуы мүмкін. Тексерілмеген деректерді талдау қажет: клиенттердің шолуы, тексеру нәтижелері, апаттар, қызмет көрсету туралы өтініш, бәсекелестік орта, ақпараттық қауіпсіздік, ақпараттық технология (АТ) инфрақұрылымы. Бұл жерде ақпарат көздері: кестелер, диаграммалар, әлеуметтік желілер, сараптамалық бағалау және т.б. болуы мүмкін. Мұндай деректерді талдау нәтижесі объектінің паспорты, оның ішінде орналасқан жері, ауданы, қабаттар саны, рұқсаттар, түгендеу деректері, бәсекелестік орта, тарихи қаржылық деректер, маусымдық сатылым факторы және т.б. Бірақ, белгілі болғандай, компанияның құны оның материалдық құнының қарапайым сомасына тең емес. Big Data технологиясы туралы ақпаратты жинау және талдау материалдық емес активтердің құнын бағалауға мүмкіндік береді. Оларға мыналар жатады: еңбек ресурстары, білім мен дағдылар; ақпараттық ресурстар, дерекқорлар, ұйымдық-басқару құрылымы, таланттар, қызметкерлердің потенциалы, бренд, беделі, даму, клиент базасы, контрагенттермен қарым-қатынас. Үлкен деректер мен цифрлық экономика шешілетін мәселелер. Қазақстан Республикасында «Сандық Қазақстан-2020» мемлекеттік бағдарламасын іске қосу мәселесі маңызды болып табылады, сол себепті экономикалық жүйені цифрлық түрге айналдыру ең алдымен үлкен деректерді тиімді басқарумен байланысты [4].

Қорытынды. Адамзаттың жаһандық жылынуына әсер етуі әлі күнге дейін көптеген қарама-қайшылықты пікірлер туғызып келеді, сондықтан да бұл сауалға деректердің үлкен көлемін талдауға негізделген сенімді болжау модельдері нақты жауап бере алады[5]. Жаһан бойынша шығарындыларды азайту бәрімізге көмектеседі және оның тағы бір көрінісі біз энергияны да аз жұмсайтын боламыз.

BigData бізді өндірістік жоспарлау, білім беру, ақпараттық қауіпсіздік, денсаулық сақтау және басқа салалардағы жаңа көкжиектерді ашады. Егер олардың дамуы тоқтаусыз жалғаса берсе, BigData технологиялары өндіріс факторы ретінде ақпараттың сапасын мүлдем жаңа деңгейге шығара алады. Ақпарат еңбек пен капиталға теңестіріліп қана қоймай, қазіргі заманғы экономиканың ең маңызды ресурсы бола алады.

Әдебиеттер

1. By Cynthia Harvey, Big Data Challenges, June 5, 2017. – https://www.datamation.com/big-data/big-data-challenges.html
2. С.Маликова Big Data: тенденции развития, опасности и перспективы. – https://www.eg-online.ru/article/372363/
3. Статья:Большие_данные_(Big_Data)_мировой_рынок http://www.tadviser.ru/index.php/
4. https://www.inform.kz/kz/2017-zhyldan-sandyk-kazakstan-2020-bagdarlamasy-iske-kosylmak_a2912600
5. B. Bissarinov, R. Mussabayev, A. Bissarinova.Collective method in solving the Big Data clustering problems. // The 16th International Scientific Conference Information Technologies and Management 2018 April 26-27, 2018, ISMA University, Riga, Latvia, p.75-76, ISSN 1691-2489.

САНДЫҚ СЕРТИФИКАТТАРДЫ ҚОЛДАНУ

Капалова Н.А.[1], Абишева А.Ж.[1,2]
nkapalova@mail.ru, ak_maral@mail.ru
[1]ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты,
[2]әл-Фараби атындағы Қазақ Ұлттық университеті,
Қазақстан

Аңдатпа. *Криптографиялық алгоритмдерді құпия кілттерсіз пайдалану мүмкін емес. Осыған байланысты құрамына кілттерді жинақтау, сақтау және үлестіру жүйелері кіретін қауіпсіз кілттерді басқару жүйесін құру қажет. Мақалада криптографиялық кілттерді басқаруға қатысушылардың іс-әрекеттерін үйлестіру жолдары, ашық кілтті инфрақұрылымда әрбір пайдаланушыға ашық кілт пен оның иесі арасында айқын және сенімді сәйкестікті орнатуға мүмкіндік беретін рәсім ашық кілтті сертификаттау механизмі, қасиеттері сипатталған.*

Қазіргі жаһандану жағдайында және Интернеттің өсуінің ықпалымен, жаңа технологияларға жиі жүгіну шұғыл қажеттілікке айналды. Ақпараттық технологиялар қазіргі заманғы адамдардың күнделікті өмірінің ажырамас бөлігі болды. Ақпараттық қауіпсіздікті тиісті деңгейде қолдау үшін, ресурсты интенсивті есептеуге негізделген барлық жаңа криптографиялық алгоритмдер әзірленуде. Ақпараттық ресурстардың түпнұсқалығы мен құпиялылығын қамтамасыз ету сияқты маңызды мәселелерді шешуде деректердің қолжетімділігі және криптографиялық механизмдердің жұмысымен байланысты уақытша кідірістер ақпараттық жүйелердің маңызды қасиеттерінің бірі [1].

Күрделі криптожүйеге қатысушылардың - криптожүйенің абоненттері - бір-бірімен байланысу үшін бастапқыда өздерінің криптографиялық кілттері болмауы мүмкін. Сонымен қатар, көптеген абоненттері бар жүйеде олар бір-бірін біле алмайды, немесе жүйеде қатысушылардың саны көбінесе белгісіз немесе өзгеріп отыруы мүмкін.

Осыған байланысты қатысушыларға криптографиялық кілттерді басқаруға қатысушылардың іс-әрекеттерін үйлестіру жолдарын ұсыну керек, яғни тұтастай жүйеде

кілттерді басқаруды енгізу. Ұйымдастырылған кілттерді басқару үшін кейбір кілттерді басқару моделін қолдау қажет. Криптожүйеде кілттерді басқару модельдерінің екі түрі кездеседі: орталықтандырылмаған немесе орталықтандырылған (үшжақты) кілтті басқару.

Орталықтандырылмаған кілттерді басқару жүйесі криптографиялық кілттерді басқарудың бірыңғай орталығының жоқтығын білдіреді. Бұл жағдайда өмірлік циклдің барлық негізгі қызмет көрсету процедураларын криптожүйенің абоненттері жүзеге асырады.

Кілттерді орталықтан таратуды қолданатын әдістердің *кемшілігі* – орталық кімге және қандай кілттер тағайындалғанын біледі, ол ақпараттық жүйеде жүрген барлық хабарламаларды оқуға мүмкіндік береді. Кілттерді тікелей айырбастау кезінде субъектілердің түпнұсқалығын аутентификациялау проблемасы бар, яғни «ортадағы адам» шабуылына ұшырау мүмкін, ол жағдай шабуылдаушы екі қатысушының арасында болған кезде орын алады [2]. Бұл жағдайда таратылатын ашық кілттерді ауыстыру қатері пайда болады, толығырақ қарастырайық.

Қолданушы А қолданушы В-ға ашық кілтін жібереді. Ортадағы адам Е өзінің ашық кілті мен жабық кілтін генерирлеп, жолдан қолданушы А-ның ашық кілтін алып алып, өзінің ашық кілтін қолданушы А-ның атынан қолданушы В-ға жібереді. Қолданушы В ештеңе білмей Е-ның ашық кілтімен хабарламаны шифрлеп (ол қолданушы А-ның ашық кілтімен шифрледім деп ойлайды), қолданушы А-ға жібереді. Е оны жолдан ұстап алып өзінің жабық кілтімен дешифрлейді. Нәтижесінде құпиялылық бұзылды.

Қолданушы В хабарламаны қолданушы А үшін шифрлегеніне сенімді болған, дегенмен де ол оны Е үшін шифрледі. Ең қызығы төртінші қадамда хабар алмасу процессі тоқтамайды. Е хабарламаны өзгертіп, оны қолданушы А-ның ашық кілтімен шифрлеп қолданушы А-ға жібереді. Осылайша екі жақ ортада хабарламаны ұрлап алатын үшінші адамның бар екенін білмей қалады.

Сондықтан, ашық кілттің қолданушы А-ға тиісті екенін растау үшін ашық кілтті қайсыбір ақпаратпен байланыстыру керек (кімге тиісті, қандай сериялық номер, қандай алгоритммен генерирленген). Егер қолданушы А оның ашық кілті ұрланғанын біліп қойған жағдайда, қолданушы В ол кілтті енді қабылдап алмауын қамтамасыз ететін ашық кілтті қайтарып алатын механизм керек. Бұл мәселені шешу үшін цифрлық *сертификаттар қолданылады*. Ол ISO стандарттарында анықталған. Сертификат - бұл абоненттің идентификаторынан, оның ашық кілтінен және куәлікті беру уақыты мен оның жарамдылық мерзімі сияқты қосымша ақпарат, сенімді түрде өкілетті ұйым немесе сенімді адам қолымен жасалған деректер жиынтығы. Ол оны сақтау немесе жөнелту кезінде ашық кілтті алмастыру мүмкіндігін болдырмау үшін арналған. Сертификатты алған және электрондық цифрлық қолтаңбаны растағаннан кейін, ашық кілттің абонентке шынымен тиесілі екеніне көз жеткізуге болады [3].

Ашық кілттер инфрақұрылымы (Public Key Infrastructure - PKI) ашық кілттерді таратудың үш жақты әдісі болып табылатыны белгілі, яғни осы немесе басқа ашық кілттің кімге қатысты екенін анықтайтын жүйе. ISO X.509 халықаралық стандарты PKI жалпы құрылымын және оларды пайдалану туралы хаттамаларды анықтайды[9]. Стандартқа сәйкес, орталық өкілеттіктер бар, ол «ашық кілт - жабық кілт» жұбына ие және өзінің ашық кілтін жариялайтын куәландыру орталығы (КО) деп аталады. Куәландыру орталығының ашық кілті бәріне белгілі. Ашық кілттер инфрақұрылымына қосылу үшін қолданушы А өзінің жеке - «ашық кілт - жабық кілт» жұбын жасайды. Жабық кілтті жасырын сақтайды, ал ашық кілтті сертификаттау орталығына жібереді.

Куәландыру орталығы қолданушының А екенін тексереді, содан кейін келесідей сандық нұсқауларға қол қояды: «Кілт А қолданушыға тиесілі». Бұл мәлімдеме сертификат деп аталады және осы кілттің А қолданушыға тиесілі екендігін куәландырады. Енді, егер А қолданушы В қолданушымен байланысқысы келсе, ол оған өзінің ашық кілтін және сертификатын жібере алады. В қолданушысында куәландыру орталығынан ашық кілті бар, ол оның көмегімен цифрлық қолтаңбаны тексере алады. Егер қолданушы В куәландыру орталығына сенім білдірсе, ол кілт шынымен А-ға тиесілі екеніне сенуіне болады. Бұл сипатталған қадамдарды орындағаннан кейін, қолданушы В өзінің ашық кілтін куәландыру орталығында тексертіп, содан кейін ашық кілт пен сертификатты А қолданушыға жібереді. Енді А және В қолданушылар бір-бірінің ашық кілттерін біле алады. Соңғысы қауіпсіз байланыс үшін сеанс кілтін жасайтын кілтті үйлестіру хаттамасын іске қосу үшін пайдаланылуы мүмкін. Ашық кілтті инфрақұрылымның негізгі тұжырымдамасы көптеген іргелі мәселелерден зардап шегеді, соның ішінде: қолданушы аттарының мәселесіне қатысты жанама авторизация; сертификаттау орталығына сенімділіктің дәрежесіне қарай қауіпсіздіктің тәуелділігі; сертификатты қайтарып алу.

PKI иерархиялық схемасы төрт түрдегі сертификаттардың болуын қамтамасыз етеді:

1. Соңғы пайдаланушы сертификаты.

2. Куәландырушы Орталығының Сертификаты (КО). Соңғы пайдаланушы сертификатының цифрлық қолтаңбасын тексеру үшін және жоғары деңгейлі КО жабық кілтімен қол қойылған болуы керек, сонымен қатар осы ЭСҚ жоғарғы деңгейдегі КО сертификаты қол жетімді болуы керек екені тексерілуі және т.б. болуы тиіс.

3. Өз бетімен қолтаңба қойылған сертификат. Бұл бүкіл PKI үшін түпкі және анықтама бойынша сенімді болып анықталады. Егер КО сертификаттарының тізбегін тексеру нәтижесінде олардың біреуі түпкі жабық кілтпен қол қойылса, онда сертификаттардың цифрлық қолтаңбасын тексеру процесі аяқталады.

4. Кросс-сертификат. Кросс сертификаттары екі түрлі PKI түпкі сертификаттарына өзара қол қою арқылы нақты PKI жұмысын кеңейтуге мүмкіндік береді.

Ашық кілт сертификатының келесі қасиеттері бар:

- КО сертификатының ашық кілтіне рұқсаты бар әрбір пайдаланушы сертификатта қамтылған ашық кілтті ала алады;
- КО-нан басқа ешбір жақ сертификат анықталмайтындай етіп сертификатты өзгерте алмайды (жалған сертификаттар жасауға болмайды).

Сертификаттарды бұрмалау мүмкін болмағандықтан, оларды қорғау үшін ерекше күш жұмсамай қолжетімді каталогқа орналастыруға болады.

PKI атқаратын қызметтерді бірнеше топқа бөлуге болады:

1. сертификаттарды басқару функциясы;
2. кілттерді басқару функциясы;
3. қосымша функциялар (қызметтер).

Сертификаттарды басқару функцияларына мыналар кіреді:

- қолданушыларды тіркеу;
- ашық кілттерді сертификаттандыру;
- КО сертификатының жабық кілтін сақтау;
- сертификат базасының мазмұны және оларды тарату;
- сертификатты жаңарту;

- кілттерді жаңарту;
- сертификатты қайта шақыру
- сертификатты қайта шақыру статусын анықтау.

X.509 форматына сәйкес бұл мәліметтер жиынына мыналар кіреді:

- ашық кілттің қызмет ету мерзімі: мерзім басы және соңы;
- кілттің номері мен сериясы;
- қолданушының жеке аты;
- қолданушының ашық кілті туралы ақпарат: берілген кілтке арналған алгоритм идентификаторы және ашық кілт;
- ЭСҚ тексеру процедурасын жүргізу кезінде қолданылатын ЭСҚ және ақпарат (мысалы, ЭСҚ генерирлеу алгоритмінің идентификаторы)
- сертификаттау орталығының бірегей аты.

Сонымен сертификат үш басты компоненттен тұрады:

- сертификаттың қолданушы-иесі туралы ақпарат;
- қолданушының ашық кілті;
- КО-ның жабық кілтімен есептелген екі алдыңғы компоненттің ЭСҚ-н куәландыру [4].

Ашық кілттің сертификаттары **валидация** (растау) процесінде пайдаланылады, яғни деректердің сандық қолтаңбамен расталғанын тексеру кезінде алушы: 1) жіберушіні сәйкестендіретін ақпарат сертификатта қамтылған деректерге сәйкес келетінін; 2) сертификаттар тізбегіндегі сертификаттардың ешқайсысы кері қайтарылмағанын және хабарламаға қол қою кезінде барлық сертификаттар жарамды болғанын; 3) жіберушінің сертификатты мақсатына сай пайдаланғанын; 4) ЭЦҚ құрылғаннан бері деректердің өзгермегенін тексереді.

Тексеру нәтижесінде алушы жіберуші қол қойған деректерді қабылдай алады.

Қолтаңба кілті сертификатының валидациясын тексеру

«...Сертификаттың валидациясын тексеру - оны пайдалануға болатындығын тексеру үшін қолтаңба кілті сертификатында орындалатын әрекеттер, атап айтқанда:

- сертификаттың тұтастығын (түпнұсқалығын) тексеру;
- сертификаттың жарамдылық мерзімін тексеру;
- сертификаттың ағымдағы уақытта қайта шақырылған тізіміндегі қолтаңба сертификатының жоқтығын тексеру;
- сертификаттың әрекет ету аймағын тексеру [5].

Біздің елге келетін болса, Қазақстан үкіметі ұлттық қауіпсіздік сертификатын, оның ішінде оны қолдану ережелерін енгізуге арналған бірқатар заңнамалық актілерді бекітті («Қауіпсіздік сертификатын беру және қолдану ережесін бекіту туралы» Қазақстан Республикасы Ұлттық қауіпсіздік комитеті Төрағасының 2018 жылғы 27 наурыздағы №23/н бұйрығы).

Бекітілген қауіпсіздік сертификатын беру ережесінде сертификат үш жыл мерзімге байланыс операторының өтініші бойынша берілетіндігі айтылған. «Байланыс туралы» жаңа заңға сәйкес операторлар қауіпсіздік сертификатын пайдаланып, трафикті шифрланған хаттамалар арқылы өткізуі керек. Телекоммуникация операторлары абоненттерге Интернетке қол жетімділіктің өзгеретін шарттары туралы хабарлау және абоненттер мен қосалқы операторлар арасында сертификатты тарату үшін жауап береді.

Сертификатты қолдану ережелері байланыс операторынан оны пайдаланудың ұйымдастырушылық және техникалық жағдайларының құпиялығын қамтамасыз етуді талап етеді [6].

Қауіпсіздік сертификаты азаматтарды, мемлекеттік органдар мен жеке компанияларды хакерлерден, Интернет-алаяқтардан және киберқауіптердің басқа түрлерінен қорғауға арналған.

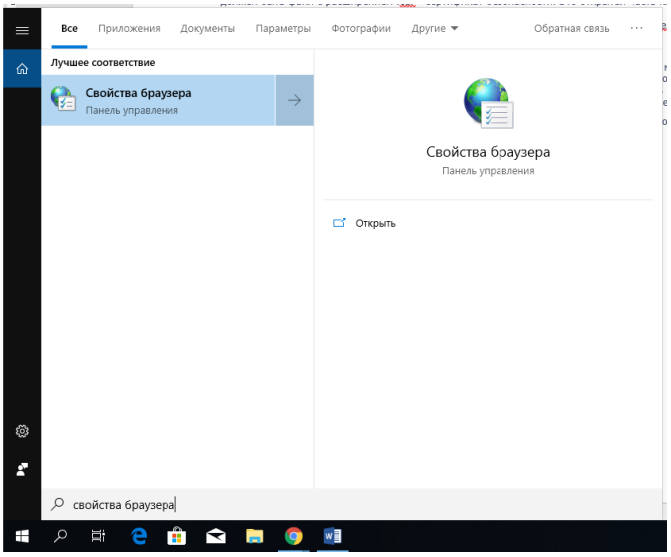
Егер электрондық қол кәдімгі флешкада сақталған болса, қауіпсіздік сертификаты - .cer кеңейтілуімен файл болуы керек. Бұл кілттің ашық бөлігі – яғни, ашық кілт (қолдың кілттік сертификаты).

Егер қорғалатын кілттік тасымалдауыш Токен қолданылатын болса, физикалық тұрғыда сертификатты көру мүмкін емес. Ол үшін ашық кілтті криптография жүйесінде (криптопровайдер) штатты функционалмен экспорттау керек.

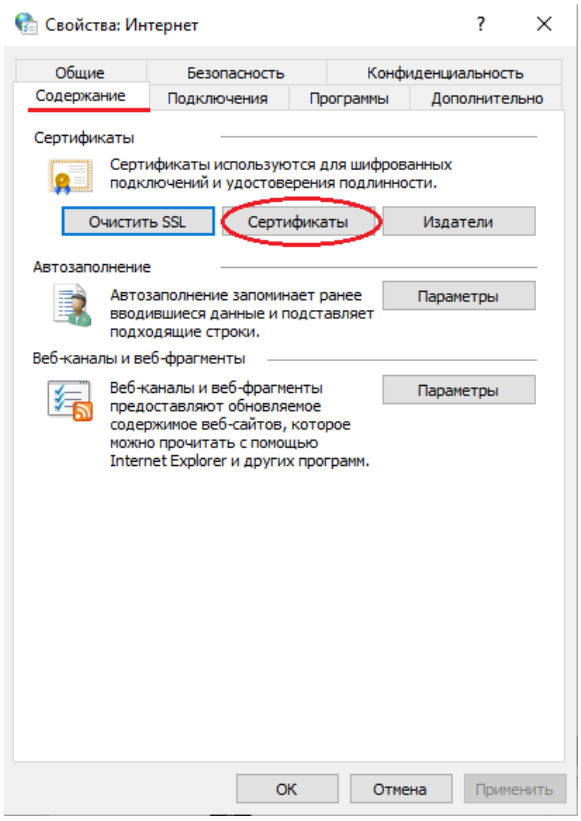
Ашық кілтті экспорттау ЭҚ қолданушының жұмыс орнында орнатылған кезде ғана жасалады. Егер ЭҚ қолданушы компьютерінде орнатылмаса, Куәландыру орталығы жіберген нұсқауларды орындап, орнату керек.

Ащық кілтті жұмыс орнында файлға қолданушы төмендегідей экспорттай алады:

Іске қосу -> Браузер қасиеті (немесе Internet Explorer браузерін іске қосыңыз -> Сервис -> Браузер қасиеті) (Сурет 1).

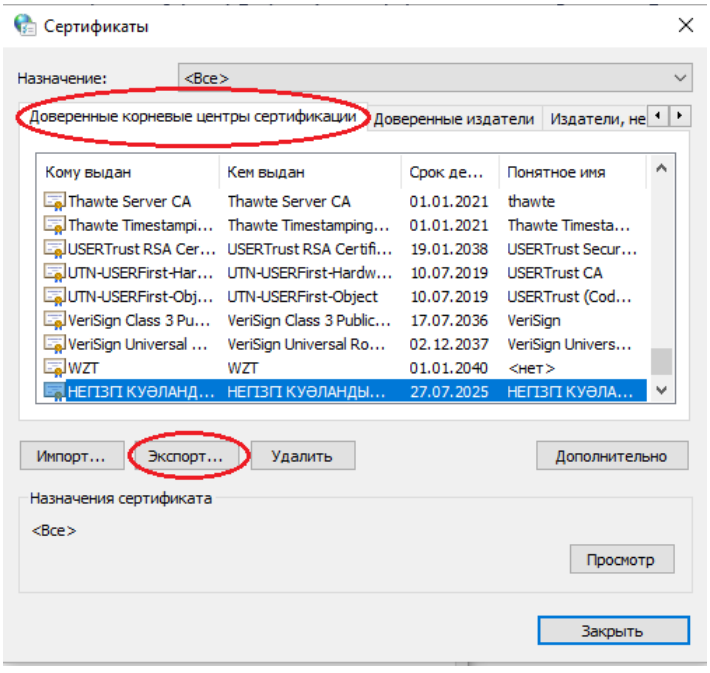


Сурет 1. Браузер қасиеті



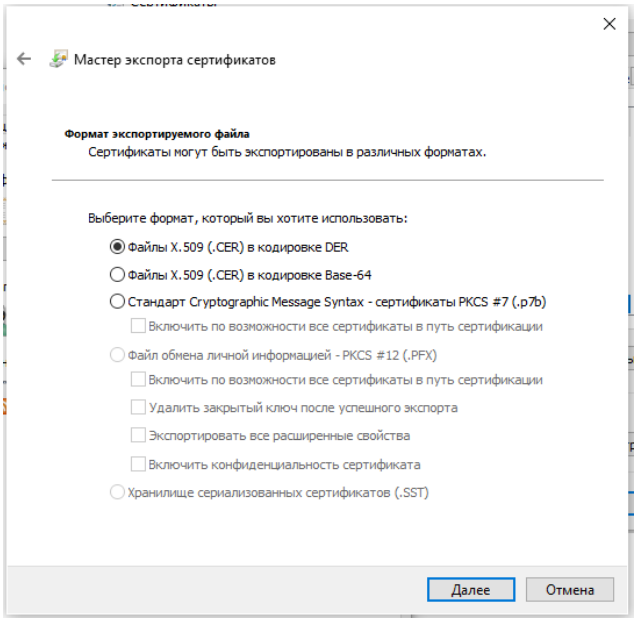
Сурет 2. Интернет қасиеті

Мазмұны вкладкасын таңдаңыз (Сурет 2), «Сертификаттар» батырмасын, «Сертификаттаудың түпкі сенімді орталықтары» вкладкасын басыңыз. Сертификаттар тізімінде керектісін таңдаңыз және белгілеңіз. «Экспорт» батырмасын басыңыз (Сурет 3).



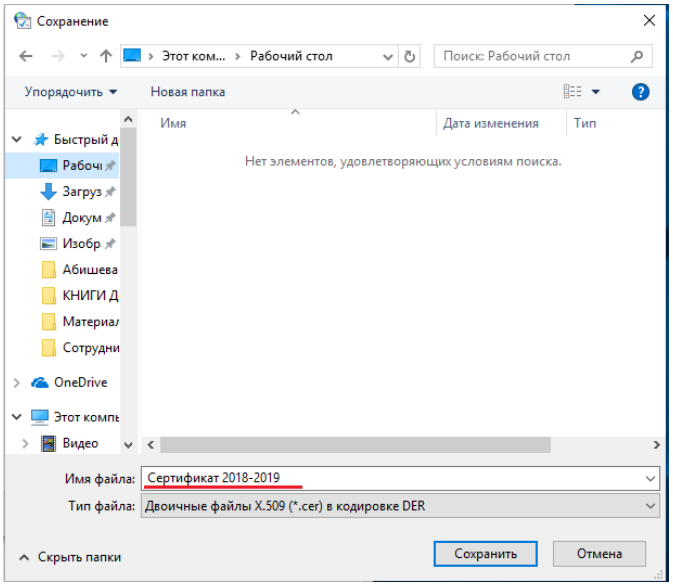
Сурет 3. Сертификаттар

«Сертификатты экспорттау мастері» іске қосылады (Сурет 4).
Мастер сұрағына жауап беріңіз:
- Жоқ. Жабық кілтті экспорттамау керек.
- Файлы X.509 (.CER) в кодировке DER



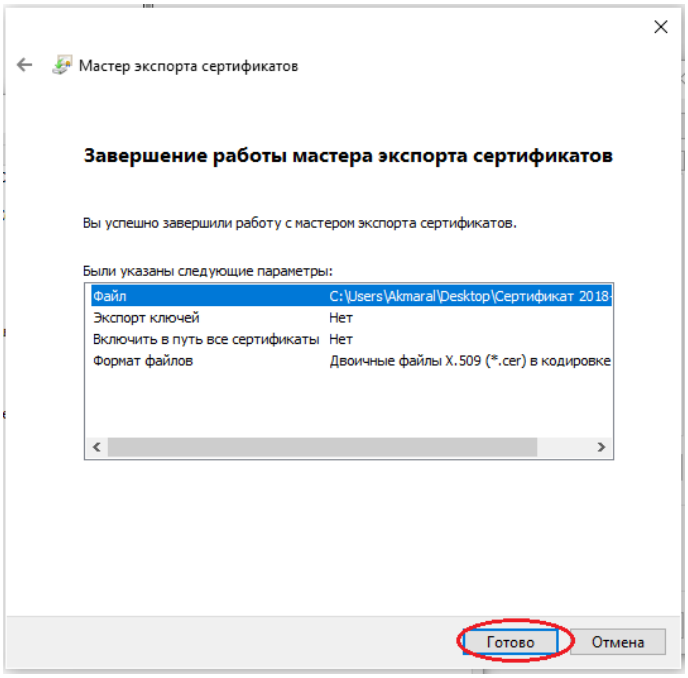
Сурет 4. Сертификатты экспорттау мастері

- Шолу. Файлды сақтайтын буманы таңдаңыз (осы терезеде қалаған файлдың атын енгізіңіз). Сақтау (Сурет 5) батырмасын басамыз.



Сурет 5. Сақтау

- Ары қарай. Дайын (Сурет 6).



Сурет 6. Сертификатты экспорттау мастері

Осы іс әрекеттердің нәтижесінде сіз көрсеткен бумада ЭҚ кілті сертификатының ашық файлы құрылады.

Негізгі кілттерді басқарудың мақсаты – қауіптерді бейтараптандыру. Ол қауіптерге мыналарды жатқызуға болады:

- Жеке кілттердің құпиялылығын бұзу;
- Ашық немесе жабық кілттердің шынайылығын және аутентификациялығын бұзу. Бұл жерде шынайылық ретінде осы кілтті қолданатын желінің конфиденциалдығын қамтамасыз ету үшін корреспонденттің түпнұсқалылығын білу немесе тексеру мүмкіндігін түсінеміз;
- Ашық немесе жабық кілттерді рұқсатсыз пайдалану, мысалы, кілтті пайдалану мерзімі аяқталған кезде.

Электрондық құжаттардың түпнұсқалығын растау жүйесі шеңберінде КО инфрақұрылымының көмегімен ЭСҚ кілттерін басқару жүзеге асуы керек. Басқару функцияларына:

- ЭЦҚ кілттерін қалыптастыру;
- Ашық кілтті тіркеу және тіркеу туралы куәлікті беру;
- Ашық кілтті куәліктің қолданылу мерзімін белгілеу;
- Ашық кілттерге қол жеткізуді ұйымдастыру;
- Сертификат мәртебесін анықтау;
- Қайтарып алудың себебін көрсететін куәліктерді қайтарып алу;
- Сертификатты тоқтата тұру / ұзарту;
- Сертификаттарды мұрағаттау;
- Сертификаты және қауіпсіздік саясатын пайдалануды басқару жатады [7].

PKI-ді қолданумен байланысты бірқатар техникалық, инфрақұрылымдық, операциялық және басқарушылық мәселелерді қарастыра отырып, шифрлау және цифрлық қолтаңба процестерінің криптографиялық беріктігінде кемшіліктер жоқ екенін атап өтуге болады, алайда бұл процестерді басқару, криптографиялық кілттерді сақтау,

объектілерді идентификациялау, сертификаттарды сақтау және т.б. жақсы іскери тәжірибеге ие болуы керек. PKI әлі даму үстінде, бірақ көптеген ұйымдар сертификаттардың көмегімен қосымшалар мен инфрақұрылымды ашық қолдана бастады. Болашаққа көз жүгіртсек, PKI-ды қолданғысы келетін кәсіпорындар мен ұйымдар жауапкершіліктің құқықтық аспектілерін, бірнеше PKI арасындағы өзара әрекеттесуді, сертификаттауды тексеру жолдарын, жабық кілттердің сақталуы және қолданушылардың оларды қабылдау сияқты мәселелерін зерттеулері қажет. Қоғамда PKI жүйесін енгізу және қолдау үшін қажет инфрақұрылымның күрделілігін ескере отырып, қысқа мерзімді перспективада PKI қолдайтын қосымшаларды нақты салалық топтар үшін одан әрі дамыту маңызды болып көрінуі мүмкін.

Әдебиеттер

1. Доронин С.Е. Протоколы коллективной электронной цифровой подписи над эллиптическими кривыми. Дис. ...канд.тех.наук. – СПб., 2011 -131с.
2. Абишева А.Ж., Капалова Н.А. Орталықтандырылған криптографиялық кілттерді басқару жүйесі. // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – 569-575.
3. Синюк А.Д., Остроумов О.А. Система классификации методов распределения ключей. //Информация и космос №3, 2006, стр.54-61
4. Защита информации и ИПО. Лекция 17. Управление криптоключами - http://yztm.ru/lekc2/l17/ (10.07.2019)
5. Полянская О. Ю. Инфраструктуры открытых ключей. Интернет-университет информационных технологий – 2007 - https://www.you-books.com/book/O-Yu-Polyanskaya/Infrastruktury-otkrytyh-klyuchej (20.02.2018)
6. Национальный сертификат безопасности Казахстана: Защита пользователей или государства? - https://online.zakon.kz/Document/?doc_id=37226731#pos=4;-137 (12.05.2019)
7. Аристархов И.В. Управление сертификатами ключей проверки электронной подписи. Дис. ... канд. тех. наук. М., 2012 - 144 с.

ОҚЫТУШЫЛАРДЫҢ ҒЫЛЫМИ БЕЛСЕНДІЛІГІН БАҚЫЛАУҒА АРНАЛҒАН АЖ КОНЦЕПЦИЯСЫ

Қорласбай М.С.
e-mail: korlasbaims@narxoz.kz
АҚ «Нархоз» Университеті 2-курс магистранты
«Ақпараттық жүйелер» мамандығы
Ғылыми жетекші – э.ғ.д.,профессор Байтенова Л.М.,
Қазақстан

Аңдатпа. *Мақалада ЖОО ғылыми саладағы мұғалімдердің еңбектерінің жариялануын бақылау мәселесі. Ғылыми еңбектерге ЖОО қолжетімділік мәселесі. Автоматтандыру процессінің ғылыми еңбектердің қолжетімділігін арттырудағы*

қолдануы. ЖОО ғылыми еңбектерді жариялаудағы белсенділікті бақылауға арналған АЖ жалпы идеясы. АЖ концепциясы. АЖ функционалы мен интерфейсіне тоқталам.

Қазақстан Республикасының ЖОО атқаратын қызметі мен мамандандырылу бағытына сай 3 түрге бөлінеді: университет, академия және институт (деңгейі бойынша теңестірілген консерватория).

Академиялар мен институттар белгіленген бір салаға мамандандырылған білім беруге бағытталған ЖОО. Мысалы, азаматтық авиация академиясы, Атырау мұнай және газ институты. Келтірілген мекемелерде жарияланған ғылыми жұмыстар осы мекемелерде жүргізіліп отырылған ғылыми жұмыстарға қолжетімді ДҚ болып табылады. Студенттер келтірілген ғылыми мақалалар негізінде өз жобаларын жүргізуде керекті теориялық және практикалық тірек ала алады. Университеттер статусына сай көптеген сала бойынша мамандар дайындауға бағытталған. Заманауи жарияланған ғылыми жұмыстар, мақалаларды ашық базалардан табу қиынға соғады.

Көрсетілген проблема қазіргі таңдағы жоғарғы білім беру мекемелері мен ғылыми зерттеу жұмыстарын жүргізетін мекемелер және кәсіпорындар арасында ақпарат алмасу жолдарының нашар құрылғандығынан тууда. ЖОО, ғылыми зерттеу жүргізу орталықтар мен кәсіпорындар мемлекеттің экономикалық, әлеуметтік және ғылыми салаларында жетістіктердің негізі болып табылады. Араларында ортақ ақпарат алмасу платформасының жоқ болуы өзара тәжірибие мен ғылыми ақпарат алмасуға бөгет қоюда.

Студенттер ғылыми зерттеу жұмыстарын бастаған сәтте ғылыми еңбектерді іздеуге кіріседі, кітапхана монографиялық жұмыстарды дерек көзі ретінде қолдануға мүмкіндік береді. Алайда қазіргі заманда жаңа мағлұматтарды қолдана жүру проекті мен ғылыми еңбектің дәрежесін көтереді. Жаңа әдістер, мағлұматтар мен теориялар өз негізінде прогрессивті әсер беруі ықтимал. Мұндай алмасу платформасын құру үшін ең алғаш Қазақстан бойынша ЖОО өзара келісімге келуі алғышарт болып табылады. Бұл қадам орындалған соң АЖ жобалауы басталады. Құрастырылған жүйе негізінде оқытушылар мен олардың ғылыми жұмыстарының жариялануы.

ЖОО ның оқытушыларына арналған АЖ ны құрастыру барысында өз алдына қоятын мақсатты айқындау жүйенің жалпы концепциясын анықтауға мүмкіндік берелі. Оқытушылар ұстаздықтан бөлек ғылыми салада еңбектерін жарыққа шығарып отыруы ғылыми дәрежелерін көтеруге бағытталады. Алайда халықаралық журналдарда еңбектерін жариялау мен конференцияларға қатысуы жайлы ақпарат тек жеке сол ғылыми тұлғаның еншісінде қалады. Өзі немесе ЖОО басқаратын ұйымға қолайлы сұрыпталған ақпараттан құралған профильдердің базасы оқытушылардың ғылыми белсенділігін бақылауға мүмкіндік туғызады.

Ақпараттың айқындылығы мен сұрыпталған формасы АЖ қолданушыға интерфейсті оңайлықпен игеруге мүмкіндік береді.

АЖ ның деректер қорына импортталатын ақпараттың айқындылығына жауап беру үшін ақпаратты деректер базасына енгізу барысында оның ақиқаттығын дәлелдеуге мүмкіндік беретін дерек көздерін енгізу негізгі талап болып табылады. Мысалы, автордың ғылыми мақаласы немесе басқа ғылыми еңбегі жайлы ақпарат (тақырыбы, сала, аннотация т.б.) деректер қорына енгізілген жағдайда кандай ортада: ғылыми журнал, конференция, ғылыми еңбектер жинағы немесе т.б. жарық коргені белгіленуі қажет. Сұрыптау жалпылама период бойынша және ғылыми журналдардың белгілеген көрсеткіштері (импакт фактор, процентиль) бойынша жүргізіледі. Бұл ғалымның

ғылыми белсенділігін айқын көрсетуге мүмкіндік беретін графиктер мен диаграммалар құрастыруға мүмкіндік береді.

АЖ ның құрылымына тоқталсақ. АЖ ға енетін субъетілер: қолданушы мен техникалық көмек көрсетуші.

Қолданушы ретінде оқытушылар мен ЖОО басқарушыларды қарастырып кету маңызды. Себебі ғалымның жеке мағлұматтарын өзгертуге немесе қосуға тек сол ғалымның мүмкіндігі ғана болады, ал ЖОО басқарушылар ұйымы тек сол оқытушылардың ғылыми саладағы белсенділігін графикалық құралдар (график, диаграмма, т.б.) арқылы ғана бақылау мүмкіндігі болады.

Техникалық көмек көрсетуші кез келген АЖ ны қалыпты жағдайда ұстап тұруға қажетті маңызды субъект болып табылады.

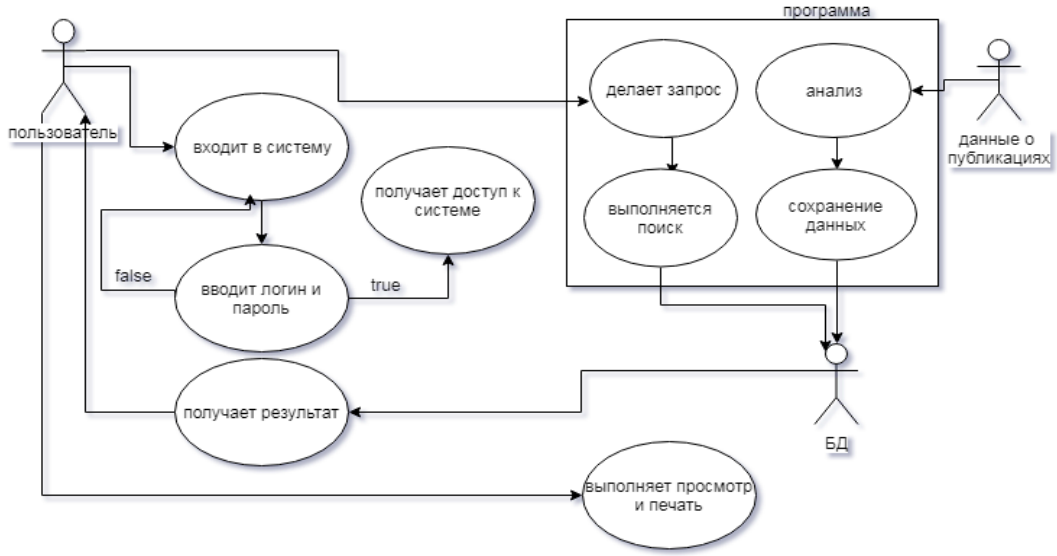
Интерфейске тоқталсақ.

Жеке мағлұматтарды қауіпсіздендіру үшін қолданушыны идентификациялау процессі талап етіледі. Бұл процесс ЖОО техникалық көмек көрсету орталығы құрастырған профильдің логин және паролын енгізу арқылы жүргізіледі.

Идентификациядан өткен соң қолданушының профильіне кіреді.

Ғылыми саладағы ғалымның еңбектері жайлы ақпаратты импорттауға формалар қолданылады. Автор, пән, тақырып, журнал атауы, журналға сілтеме, көрсеткіштер, жарияланған уақыты және таңдау тізімінде еңбек түрі таңдалынады (монография, мақала, тезис, т.б.).

Форма толтырылып сақталған соң ақпарат период және көрсткіштер бойынша сұрыпталып, оқытушы жайлы бақылауға арналған ақпарат жаңартылады.



1- сурет. АЖ жобалау концепциясы

ДҚ ға тоқталсақ.

Біріншіден бастапқыда “Автор” қорын құрастыру қажет болады. Бұл қордың негізінде ЖОО дағы оқытушылардың профильдерін жинақтауға мүмкіндік береді. Профильдердің ақпараттарын сақтауға арналған релияциялық жинақтар құрастырылады. Қауіпсіздікке бағытталған логин мен парольдар жайлы ақпараттар бөлек ДҚ құрамында болады және “Автор” мен байланыс орнатылады.

Мақалада келтірілген АЖ жобалау концепциясы ауқымды ақпарат алмасу платформасының негізі болып табылады. Оқыту процессін автоматтандыру қазіргі күні өте маңызды сұрақтардың біріне айналды, алайда сол оқытылатын ақпарат көзі болатын ғылыми зерттеу процестері мен өзара байланысының автоматтандырылуы анық проблема түрінде көрсетілмеген. Тек ұқсас проблеманы мысалға келтіред. ЖОО білім алушылардың мамандар ретінде деңгейлері төмендеуде. Көріп отырғанымыздай ЖОО, ғылыми зерттеу жүргізетін мекемелер мен кәсіпорындар арасындағы өзара мағлұмат алмасу платформасы жоқ. Сол платформаны құрастыру барысында ең алғаш вуз ішіндегі АЖ ны ғылыми жұмыстардың белсенділігін бақылауға мүмкіндік беретіндей етіп құрастырып, бірнеше университет арасында алмасу процессін ұйымдастыру қажет.

Әдебиеттер

1. Гвоздева, В. А. Основы построения автоматизированных информационных систем/ В.А.Гвоздева, И.Ю. Лаврентьева. - М.: Форум, Инфра-М, 2016. - 320 с.

2. Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем / Э.Р. Ипатова, Ю.В. Ипатов. - М.: Флинта, 2013**.** - 256 с.

ӘЛЕУМЕТТІК ЖЕЛІДЕГІ ЭКСТРЕМИСТІК МӘТІНДЕРДІ ЖІКТЕУ ДӘЛДІГІН ГРАММАТИКАЛЫҚ ҚАТЕЛЕРДІ АНЫҚТАУ ЖӘНЕ ТҮЗЕТУ АРҚЫЛЫ АРТТЫРУ

Мусиралиева Ш.Ж., Болатбек М.А.
e-mail: mussiraliyevash@gmail.com, bolatbek.milana@gmail.com
әл-Фараби атындағы Қазақ ұлттық университеті,
Қазақстан

Аннотация. *Бұл жұмыста авторлар экстремистік бағыттағы мәтіндерді анықтау мақсатында әлеуметтік желі мәтіндеріне семантикалық талдау жүргізу барысында туындайтын қиындықтардың бірі грамматикалық қателерді автоматты түрде анықтау және түзету мәселесіне тоқталады. Қателерді анықтау және түзету жүйелерінің ағылшын тіліне арналған бірнеше бағдарламалары мен деректер қоры бар. Соңғы уақытта орыс, неміс тілдері үшін де қателерді анықтау жүйелері құрылуда. Берілген жұмыста ағылшын, орыс, неміс, чех тілдеріне арналған грамматикалық қателерді түзету жүйелеріне шолу жасалады. Сондай-ақ, авторлар қазақ тілі үшін аталған сипаттағы жүйелердің болмауына байланысты берілген мәселенің өзекті екендігін көрсетеді.*

Қазіргі таңда халықаралық ақпараттық-коммуникациялық Интернет желісі экстремистік материалдарды таратуда белсенді қолданылады. Бұл жаһандық саяси процестің негізгі қатысушыларының бірі ретінде Қазақстан Республикасы үшін өте маңызды болып табылады. Экстремистік ұйымдар криминалдық қызметте Интернеттің шексіз мүмкіндіктерін белсенді пайдаланады, оның ішінде: қылмыс жасауға дайындық және оны жасау кезінде интернет-ресурстарды пайдалану; қоғамдық қауіпті қызметті басқару және үйлестіру мақсатында жасырын ақпарат алмасу; арнайы құрылған

сайттарда және басқа да интернет-ресурстарда белсенді насихаттау бойынша жоспарланған ақпараттық операцияларды жүзеге асыру; жаңа қатысушыларды аталған ресурстармен заңсыз әрекеттерге тарту және т.б. Нәтижесінде, соңғы жылдары экстремизм проблемасының өршуі байқалуда, оны Қазақстанның ұлттық қауіпсіздігіне қауіп төндіретін мәселе ретінде қарастыруға болады.

Ғаламтор алпауыттары Google, Facebook және Twitter лаңкестік мазмұнды табу және жою үшін жасанды интеллект технологиясын қолдануда. IBM-де әлеуметтік желілердегі барлық деректерді талдайтын Watson бағдарламасы бар. Ресейде Платонның ақпараттық серіктес авторы әлеуметтік желілерді бақылау және қауіптерді болжау жүйесін құрастырды. Германия үкіметі террористік шабуылдардан кейін Интернетте террористермен күресу үшін ZITiS деп аталатын жаңа киберқауіпсіздік бөлімшесін құру туралы жариялады. Қазақстанда мұндай жүйе жоқ. Сол себепті экстремизм көріністерін анықтауға, алдын алуға және жолын кесуге бағытталған тиімді шаралар кешенін іске асыруды қажет ететін бағдарламаларды құру өзекті болып табылады.

Бұл жұмыста авторлар әлеуметтік желілердегі экстремистік бағыттағы материалдарды анықтау мақсатында семантикалық үлгілерді құру барысында туындаған қиындықтардың бірін сипаттайды. Аталған мәселені шешу үшін авторлар бес кезеңнен тұратын үлгі құрастырды. Үлгінің екінші кезеңі бойынша жинақталған мәліметтер арасында қазақ тіліндегі мәтіндер ішінде орфографиялық қателері бар сөздердің көптігі анықталды. Берілген жұмыста құрастырылған корпус ішіндегі орфографиялық қателіктерді түзету әдістеріне шолу жасалады.

Грамматикалық қателіктерді түзету — мәтіндегі сөздердің қате қолданылуын және дұрыс құрастырылмаған грамматикалық құрылымдарды автоматты түрде анықтау және түзету тапсырмасы. Грамматикалық қателерді анықтау және түзету тапсырмасын көп классты классификация есебі ретінде қарастыруға болады [1].

Грамматикалық қателіктерді түзету мәселесі ең көп қарастырылған тіл ағылшын тілі болып табылады. Ал басқа тілдерге келетін болсақ, қателіктерді анықтау және түзетуге қатысты жасалған жұмыстар саны өте шектеулі болып келеді. Атап айтатын болсақ, [2] неміс, [3] орыс, [4] чех тілі үшін грамматикалық қателіктерді түзету жүйесін құрып, аталған тілдер үшін корпус құрастырған. Сондай-ақ, [5] қытай, [6] жапон, [7] араб тілдері үшін оқытуға арналған аннотациялық корпустарды құруға қатысты зерттеу жұмыстарын жүргізген [8].

Экстремистік бағыттағы мәтіндерді классификациялау үшін ең алдымен машиналық оқыту әдістерін жаттықтыруға арналған корпус қажет. Қазақ тілі үшін экстремистік бағыттағы мәтіндердің ашық корпусы жоқ. Аталған мәселені шешу мақсатында зерттеу жұмысының алғашқы кезеңінде авторлар әлеуметтік желідегі қазақ тіліндегі экстремистік мәтіндерді қамтитын корпус құрастырды. Корпуста тікелей экстремистік бағыттағы мәтіндер және "бейтарап" мәтін ретінде жіктелетін экстремистік іс-әрекеттер жайлы жаңалықтар, экстремистік әрекеттерге қарсы сипаттағы мәтіндер және жалпылама лексиканы қамтитын мәтіндер қамтылған. Құрастырылған корпустағы негізгі кілттік сөздер TF-IDF әдісі бойынша анықталды [9]. Аталған кілттік сөздер бойынша "Вконтакте" әлеуметтік желісіндегі 170 топқа талдау жасалды. Олардың ішіндегі 25 топ парсинг жасау бағдарламасында қолданылды. Құрастырылған парсинг жасау бағдарламасы топтағы соңғы алты ай ішіндегі жазбаларды көшіру арқылы корпусты толықтырып отырады. Басқа тілдегі жазбалар Google Translator арқылы аударылды [10].

Корпусқа талдау жүргізу барысында көптеген қолданушылардың қазақ тіліне тән әріптерді кирилл әріптерімен алмастыратыны жиі байқалды, мысалы "соғысқа" сөзінің орнына "согыска", "шайқасқа" сөзінің орнына "шайкаска" деп жазылады.

Осы тұста классификациялау дәлдігін арттыру мақсатында корпустағы орфографиялық қателіктерді түзету мәселесі туындайды. Қазақ тілі үшін енгізілген сөздің қате немесе дұрыс жазылғандығын анықтайтын жүйелер бар [11]. Алайда аталған жүйелер грамматикалық қателіктерді анықтағанымен, оларды автоматты түрде түзетуді қарастырмайды.

Ғалымдар зерттеу жұмыстарында орфографияны түзетудің әр түрлі әдістерін қарастырады. Алғашқы жүргізілген жұмыстардың көбі қателерді түзету үшін сөздікте жылдам іздеу жүргізіп, тіркестерді алмастыру мәселесіне арналған кандидаттарды тиімді іздеуге арналды, бұл агглютинативті және полисемантикалық тілдер үшін маңызды болып табылады.

Notepad ++ немесе MS Word сияқты мәтіндік редакторлардағы түзету жүйелері қолданушыға қате енгізілген сөз үшін таңдауға арналған бірнеше кандидат ұсынады. Алайда орташа ұзындықтағы сөйлемге арналған нұсқалар саны өте үлкен болып табылады, ал бұл орфографияны дұрыс тексерудің тек түзетулерді шығарып қана қоймай, сонымен қатар берілген мәнмәтіндегі ең жақсы нұсқаны да таңдай білу керектігін білдіреді (мысалы, piece / peace немесе компания / кампания). Мұндай мәселелер дұрыс жазуды мәнмәтіндік түзету саласының зерттеу пәні болып табылады [12].

Орфографияны түзету күрделілігі қолданылу саласы мен бастапқы тілге де байланысты болып табылады. Шынында да, егер морфология жүйесі барынша дұрыс бөлінген болса, онда іздеу мен кандидаттарды таңдауды қиындататын сөздік те соғұрлым үлкен болады. Бұл оқытуға арналған корпустың үлкен болуы керектігін білдіреді [13].

[8] жұмыста авторлар чех тіліне арналған жаңа AKCES-GEC корпусын ұсынады. Сонымен қатар, чех, неміс және орыс тілдері үшін тәжірибе жүргізіп, синтетикалық параллель корпусты қолдану барысында нейрондық машиналық аударма үлгісі аталған мәліметтер жинағы үшін жаңа нәтижелерге қол жеткізуге мүмкіндік беретінін көрсетеді. Авторлар әрбір тіл үшін алдын ала Transformer нейрондық машиналық аударма жүйесін синтетикалық мәліметтерге дайындайды. Құрастырылған жүйенің өнімділігі барлық үш тілде де әр тілдің жеке құрастырылған грамматикалық қателіктерді түзету үлгілерінің өнімділігінен жоғары болып табылады.

[13] жұмыста авторлар Live Journal, ВКонтакте және т.б. сияқты әлеуметтік желілер мен басқа да блогтардағы мәтіндердің орфографиясын түзетуді қарастырады. Мұндай мәтіндердегі қатемен жазылған сөздердің үлесі өте жоғары болып келеді, себебі теру барысында қате кетуі, орфографиялық қателер де кездесуі мүмкін, мұндай қателерді тиімді түрде түзету морфологиялық және синтаксистік талдау сияқты мәтінді әрі қарай өңдеудің қажетті алғышарты болып табылады. Авторлар түзетуге арналған кандидатты таңдау үшін фонетикалық ұқсастықпен қатар қашықтықты өңдеуді қолданған. Аталған кандидаттарды бағалау үшін тілдік үлгі мен қате үлгісін қатар қолданады және оларды қайта қарастыру үшін сызықты классификациялау алгоритмдерін пайдаланады. Содан кейін соңғы кезеңде қате үлгісінің бағасын, кандидат пен түзету арасындағы Левенштейннің өлшенген қашықтығын, тілдік үлгі бағасын және сөздік және сөздіктен тыс сөздердегі түзетулер саны, бас әріптерді пайдалану және т.б. функциялар қолданылады. Аталған жүйе орыс тіліндегі орфографияны тексерудің алғашқы

SpellRuEval сайысына қатысып, барлық көрсеткіштер бойынша жеңіске жеткен және F1-өлшем 75%-ды құраған.

[6] еңбекте авторлар тіл үйренуге арналған "Lang-8" журналына талдау жасау арқылы жапон тілін үйренушілерінің корпусын алу жұмысын жүргізген. Авторлар жапон тілін үйренушілер құрастырған 900 мыңға жуық сөйлем алып, ол жердегі қателерді түзету үшін символдарға негізделген машиналық талдау әдісін қолданған.

[14] жұмыста авторлар оқытуға арналған үлкен көлемдегі аннотациялық мәліметтерді пайдаланбайтын әдістерді көрсетеді. Зерттеу жұмысының нәтижесінде аталған әдістердің морфологиясы бай тілдердегі грамматикалық қателіктерді түзету үшін өте пайдалы екендігін көрсетеді. Сондай-ақ, бірнеше тілге талдау жасап, аталған тілдердің корпустарындағы қате жазылған сөздердің үлесін келтіреді.

Берілген жұмыстың авторлары жоғарыда келтірілген жұмыстағы корпустағы қате сөздер көлеміне қазақ тілді корпус ішіндегі қате сөздердің үлесін қосты. Орфографиялық дұрыс жазылмаған, қазақ тіліне тән әріптер кирилл әріптерімен алмастырылған сөздер қате ретінде танылды (Кесте 1).

Кесте 1. Орыс, ағылшын, араб және қазақ тіліндегі корпустардағы қате сөздер үлесі

Корпус	Қате үлесі (%)
Орыс тілі (RULEC-GEC)	6.3
Ағылшын тілі (FCE)	17.7
Ағылшын тілі (CoNLL-test)	10.8-13.6
Ағылшын тілі (CoNLL-train)	6.6
Ағылшын тілі (JFLEG)	18.5-25.5
Араб тілі	28.7
Қазақ тілі	**13.7**

Жоғарыдағы кестеден қазақ тілді корпустағы сөздердің 13.7%-ның қате жазылғандығын және қате жазылғанын, соның ішінде діни-экстремистік сипаттағы сөздердің үлесі 2%-ды құрайтындығын көруге болады. Қазіргі таңда аталған қателіктерді автоматты түрде анықтау және түзету әдістеріне шолу жасалуда, келешекте қазақ тіліндегі қате сөздерді тиімді түрде анықтайтын әдіс құрастыру жоспарлануда.

Бұл жұмыста әлеуметтік желі мәтіндеріндегі экстремистік бағыттағы сөздерді анықтау мақсатында семантикалық үлгілерді құру кезіндегі қиындықтардың бірі болып табылатын грамматикалық қателерді түзету мәселесі көтерілді. Ағылшын, жапон, орыс, неміс, чех тілдеріндегі қателерді түзетуге қатысты жұмыстарға шолу жасалды. Құрастырылған қазақ тілді корпустағы қате сөздердің үлесі анықталды. Келешекте кіріс мәтінге морфологиялық және семантикалық талдаудың тиімді орындалуына септігін тигізетін қазақ тіліндегі қателерді автоматты түрде анықтау және түзету үлгісін құру жоспарлануда.

Әдебиеттер

1. Zhongye J., Peilu W., Hai Zh. Grammatical Error Correction as Multiclass Classification with Single Model // Proceedings of the Seventeenth Conference on Computational Natural Language Learning: Shared Task, 2013. – Pages 74–81.

2. Boyd A. Using wikipedia edits in low resource grammatical error correction // Proceedings of the 2018 EMNLP Workshop W-NUT: The 4th Workshop on Noisy User-generated Text, 2018. – Pages 79– 84.

3. Rozovskaya A., Roth D. Grammar error correction in morphologically rich languages: The case of russian. Transactions of the Association for Computational Linguistics, 2019. – Pages 1–17.

4. Šebesta K., Bedˇrichová Z., Šormová K., Štindlová B., Hrdlicka M., Hrdlicková T., Hana J., Petkevic V., Jelínek T., Škodová S., Janeš P., Lundáková K., Skoumalová H., Sládek S., Pierscieniak P., Toufarová D., Straka M., Rosen A., Náplava J., Poláckova M. CzeSL grammatical error correction dataset (CzeSL-GEC) – http://hdl.handle.net/11234/1-2143 (Қаралған күні: 05.01.2020)

5. Yu L., Lee L., Chang L. Overview of grammatical error diagnosis for learning chinese as a foreign language // Proceedings of the 1st Workshop on Natural Language Processing Techniques for Educational Applications, 2014. – Pages 42–47.

6. Mizumoto T., Komachi M., Nagata m., Matsumoto Y. Mining revision log of language learning sns for automated japanese error correction of second language learners // Proceedings of 5th International Joint Conference on Natural Language Processing, 2011. – Pages 147–155.

7. Zaghouani w., Mohit B., Habash N., Obeid O., Tomeh N., Rozovskaya A., Farra N., Alkuhlani S., Oflazer K. Large scale arabic error annotation: Guidelines and framework, 2015.

8. Náplava J., Straka M. Grammatical Error Correction in Low-Resource Scenarios // Proceedings of the 2019 EMNLP Workshop W-NUT: The 5th Workshop on Noisy User-generated Text, 2019. – Pages 346–356.

9. Bolatbek M., Mussiraliyeva Sh., Tukeyev U. Creating the dataset of keywords for detecting an extremist orientation in web-resources in the Kazakh language // Journal of Mathematics, Mechanics and Computer Science, №1 (97), 2018. – Pages 134-142.

10. Shalabayev K., Alipbay K., Bolatbek M., Mussiraliyeva Sh. Definition and classification of extremist texts in vkontakte social network // Vestnik KazNRTU, No. 5 (135), 2019. – Pages 80-86.

11. Sanasoft. Онлайн проверка орфографии http://www.sanasoft.kz/c/ru/node/48 (Қаралған күні: 05.01.2020).

12. Golding A., Roth D. A winnow-based approach to context-sensitive spelling correction // Machine learning, 1999. —Vol. 34.—N. 1–3.—P. 107–130.

13. Sorokin A., Shavrina T. Automatic spelling correction for Russian social media texts // Computational Linguistics and Intellectual Technologies: Proceedings of the International Conference "Dialogue 2016", 2016.

14. Rozovskaya A., Roth D. Grammar Error Correction in Morphologically Rich Languages: The Case of Russian // Transactions of the Association for Computational Linguistics, 2019. —Vol. 7, —P. 1–17.

ISO 9001-2015 ХАЛЫҚАРАЛЫҚ СТАНДАРТЫНДАҒЫ БІРТҰТАС ЖҮЙЕ РЕТІНДЕ ЖАҢАЛЫҚТАР БАҒДАРЛАМАЛАРЫНЫҢ САПА МЕНЕДЖМЕНТІНІҢ МОДЕЛІ

Орақ Б.Б.

e-mail: orakbb@narxoz.kz
Нархоз университеті АҚ, Қазақстан

Аңдатпа. *Халықаралық стандартқа сәйкес сапа менеджментінің моделі шығарылатын өнімнің сапасын, эфир уақытының жоғары сатылымын және жалпы кәсіпорын жұмысының тұрақтылығын қамтамасыз етуге мүмкіндік береді. ISO 9001–2015 халықаралық стандартының негізгі тұжырымдамалары мен қағидалары, сапа менеджментінің қазіргі заманғы жүйелеріне қойылатын талаптар анықталған. Стандартта сипатталған процестердің барлық түрлері қарастырылады. Жүйелік тәсілге сәйкес сапа менеджментінің моделі құрылды. Атап айтқанда, иерархия қағидасы қолданылады.*

Жаңалық бағдарламаларын құру процесін тиімді ұйымдастыру проблемасы көптеген телерадио компанияларының басшыларымен кездеседі. Телеарнаның рейтингі тұтастай алғанда жаңалықтар бағдарламаларына байланысты. Жаңалықтар жұмысы қаншалықты ұйымдастырылған болса, эфир уақытын сату да тиімді болады. Электрондық бұқаралық ақпарат құралдарының (бұқаралық ақпарат құралдарының) жаңалықтар бағдарламаларының сапасы, кез-келген өнім сияқты, іске асырылуы кәсіпорындардың қызметіне негізделген бірнеше процестерге байланысты. ISO 9001-2000 халықаралық стандартының талаптарына сәйкес келетін сапа менеджменті жүйесін пайдалану өнімнің сапасын, оларды жақсарту мен кәсіпорынның тұрақтылығын қамтамасыз ету саласындағы мәселелерді шешуге қажетті құрал болып табылады. Сонымен қатар сапа менеджментіне жүйелі көзқарас кәсіпорын жұмысын тиімді ұйымдастыруға мүмкіндік береді. Мұндай тәсіл күрделі объектіні тұтасымен де, жекелеген бөліктерден де қарастыру керек дегенді білдіреді. Пән ішкі құрылымы мен ұйымдастырылуын ескере отырып, әр түрлі жағынан және көзқарастардан зерттеледі.

ИСО 9001–2015 халықаралық стандарты

ISO 9001-2015 халықаралық стандарты «ұйымды және оның процестерін басқаруда процедуралық тәсілді қолдануға шақырады, сонымен қатар оны жетілдіру мүмкіндіктерін тез анықтап, іске асырудың тәсілі ретінде қарастырады». Бұл стандарт компанияның сыртқы және ішкі ортасын қамтиды. Стандарт процестердің 4 түрін анықтайды [1]:

1) негізгі (өндірістік) процесс;
2) басқару процестері;
3) ресурстармен қамтамасыз ету процестері (оның ішінде жұмыс күші)
4) реттеу процестері (бақылау, жетілдіру және т.б.).

1. Жаңалықтар бағдарламаларын құрудың негізгі процесі диаграмма түрінде ұсынылуы мүмкін (1-сурет).

Егер ақпараттық жағдай болса, бағдарлама жетекшісі журналист пен оператордан тұратын экипажды түсірілім орнына бағыттайды. Түсіргеннен кейін түсірілген бейне материалдары бар кассета цифрландырылады, журналист-репортер сюжеттің мәтінін жазады, оны бағдарлама режиссері немесе оның адамы тексереді. Мәтінді редактор немесе дыбыс инженері оқиды. Редактор сюжеттің жақсы оқылған мәтінін және цифрланған материалды қолдана отырып, сюжеттің орнатылуын жасайды. Дайын бейне шығарушы директорға жіберіледі. Мәтіндік нұсқа жаңалық шығаратын редакторға жіберіледі. Шығарушы директор жаңалықтар шығарылымының және мәтіндік материалдардың дайын мәтінін қолдана отырып, жаңалықтарды жазып алады. Соңғы

нұсқаны орталық аппарат бөлмесіне кезекші авиациялық инженер жібереді, содан кейін жаңалықтар шығарылады.

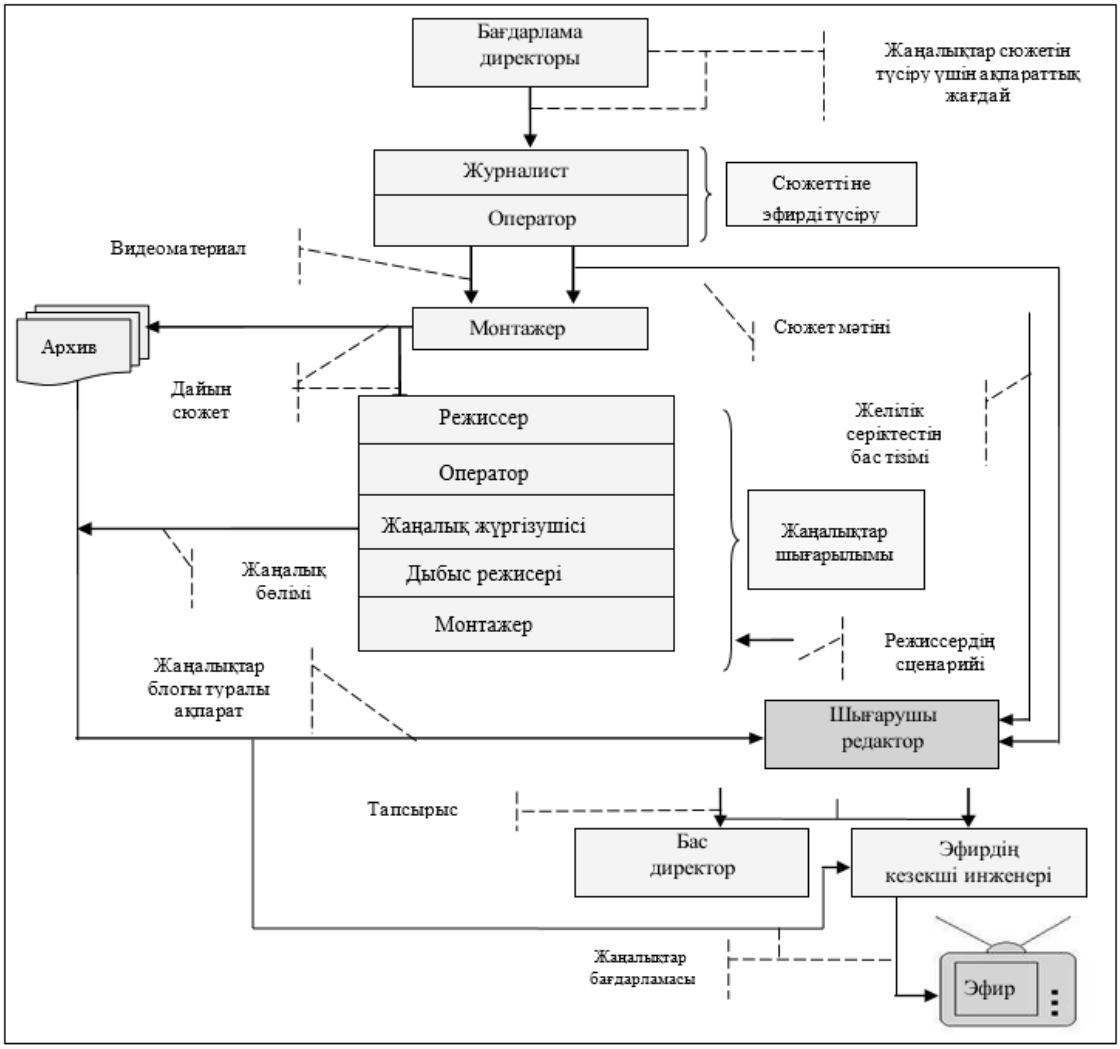
2. Әкімшілік басқару процестері нақты иерархияны, басқару мәдениетін және т.б. қамтитын бірқатар нақты ережелерге бағынуы керек. Қазіргі заманғы теледидарды басқаруда сіз теледидарлық БАҚ менеджерлерінің түрлерін нақты 3 топқа бөлуге болады [2]:

- ✓ Electronic олар жұмыс істейтін электронды тасымалдағыштың белгілі бір түрі;
- ✓ The ұйымның ішінде орналасқан деңгей;
- ✓ Their олардың блокта атқаратын функциялары.

Телерадио компаниясының басты тұлғасы - бас менеджер. Бұл шенеунік толығымен станция қызметіне жауап береді - станцияның әлеуметтік жағдайы, оның түрлі әлеуметтік процестерге қатысуы және т.б. Бас менеджер сонымен қатар басымдықты бағдарламаларды әзірлеу үшін бағдарлама директорымен жұмыс істейді. Компанияның акционерлерінің кеңесі бас менеджерден жоғары тұрған жалғыз басқару органы болып табылады.

Бизнес-менеджер теледидар станциясының сәтті жұмыс істеуі үшін жауап береді. Ол компанияның бас қаржыгері, сонымен қатар бүкіл баға саясатын анықтайтын компанияның инвестициялары мен бюджеті жөніндегі бас кеңесші.

Теледидардағы жаңалықтар режиссері күнделікті жаңалықтардың шығуына, нарықтағы жаңалықтар таратылымдарының рейтингін қамтамасыз етуге және ұстап тұруға, хабар тарату жетекшілерін жалдауға және редакцияда қарым-қатынас пен мораль стилін құруға тікелей жауапты.



1 - сурет. Жаңалықтар бағдарламаларын жасау кезінде ақпаратты берудің блок-схемасы

Сатылымдар бойынша менеджер бөлімге басшылық жасайды, осы арнадағы жарнама бағасының деңгейін анықтайды және жақсы нәтижеге жету үшін бағдарламаларды тиісті жарнама берушілерге жібереді. Сату бойынша менеджер арнаға қол жетімді эфир уақытының мөлшерін бақылап, ең жоғары жарнама рейтингін алуы керек.

Маркетинг менеджері ең алдымен нарықты зерттейді, бағдарламалардың дизайнын бақылайды, PR-компанияларды әзірлейді және жүргізеді. Маркетинг менеджері зерттеу нәтижелерін шешіп, әрі қарайғы қызметтің негізгі, бағдарланған бағыттарын көрсетеді.

Жарнамалық менеджер компания имиджіне жауап береді. Ол ғылыми-маркетинг бөлімдерімен, шығармашылық қызметтермен, жаңалықтар редакторларымен және сатылымдарымен жұмыс істейді, ұзақ мерзімді стратегиялық жоспарларды жүзеге асыру үшін бас менеджермен өзара әрекеттеседі.

Бас инженер хабар таратушы компанияның техникалық жағын қамтамасыз етеді. Станцияның техникалық құрамының жұмысын қадағалайды, студия мен портативті

жабдықтың күйін қадағалайды, станцияның хабар тарату сапасын жақсартатын жаңа технологиялар туралы біледі, техникалық бөлімге бюджетті дайындайды [2].

3.Электрондық БАҚ ресурстарына еңбек, материалдық-техникалық, қаржылық және ақпараттық жатады.

Еңбек ресурстарына ұйымның барлық құрамы, оның ұйымдық құрылымының иерархиясының барлық деңгейлері жатады.

Телекомпания сапалы ақпараттық бағдарламаларды тұрақты түрде құру үшін тиісті материалдық-техникалық ресурстарға ие болуы керек. Оларды келесідей жіктеуге болады:

–аппараттық;

–бағдарламалық қамтамасыз ету.

Аппараттық құрал дегеніміз - бұл телерадиокомпанияның техникалық жабдықтарына (теледидар және радио студиялары, бейнені редакциялау орталықтары, орталық аппараттық бөлме, жазу студиясы, аппараттық-студия бөлімі және т.б.) жатады. Бағдарламалық жасақтама жаңалық пен теледидар өндірісін автоматтандыру мәселесін шешетін мамандандырылған компьютерлік бағдарламаларға жатады. Мұндай бағдарламаларға «OCTOPUS Newsroom 5» бағдарламалық пакеті, «News Factory» бағдарламалық пакеті, «TeleVerst 2.0 2.0» автоматтандырылған жүйесі, «Digiton ATM» тарату пакеті және т.б. кіреді.

Кәсіпорынның қаржылық ресурстарына оған қол жетімді қаражат кіреді. Қаржылық ресурстар өндірісті дамытуға (өндіріс және сауда процесі), өндірістік емес объектілерді ұстауға және дамытуға, тұтынуға бөлінеді, сондай-ақ резервте қалуы мүмкін. Өндіріс пен сауда процесін дамыту үшін пайдаланылатын қаржы ресурстары оның ақшалай түрінде капиталды білдіреді. Осылайша, капитал қаржылық ресурстардың бөлігі болып табылады [3].

Компанияның ақпараттық ресурстарын сыртқы және ішкі деп бөлуге болады. Ішкі ақпараттық ресурстарға, ең алдымен, жаңалықтар бағдарламалары мен ақпараттық сюжеттердің мұрағаты кіреді (бейне архив және жаңалықтар сюжеттері мен пресс-релиздер мұрағаты). Жаңалықтар бағдарламасының бір бөлігі де солардың негізінде құрылуы мүмкін. Сыртқы ресурстар - Интернет, құқықтық құжаттар, әртүрлі агенттіктерден, бөлімдерден алынған ақпарат және т.б.

4. Хабар таратуды реттеу (бақылау, жетілдіру) процестері бірнеше деңгейде жүзеге асырылады:

–техникалық;

–бағдарламалық қамтамасыз ету;

–басқарушылық.

Техникалық деңгейде бас инженер, режиссер, операторлар, дыбыс инженерлері бейненің (теледидардағы) және дыбыстың сапасын бақылайды. Егер бұл бейне материал болса, онда режиссерлер редакциялаудың сауаттылығын бақылауы керек. Бұл шенеуніктер ақпараттың тұтынушыға техникалық жағынан дұрыс жеткізілуіне жауап береді.

Бағдарлама деңгейінде жаңалықтар бағдарламаларының мазмұнына бағдарлама жетекшісі, редакторлар, хабар таратушылар және журналистер жауап береді. Ақпарат өзектілік, тиімділік, объективтілік, сенімділік, шынайылық, нақтылық, сенсация және т.б. сияқты сапа өлшемдеріне жауап беруі керек.

Басқару деңгейінде бөлім менеджерлері барлық қызметтердің, оның ішінде техникалық және бағдарламалық бөлімдердің жұмысын бақылауы керек. Бұл деңгейде бақылау сонымен қатар «БАҚ туралы» федералды заңдарға сәйкес,

«Жарнама туралы» және т.б. Менеджерлер жұмыстың барысы мен соңғы нәтижені бақылауы керек.

Жүйелік көзқарастың принциптері

Жүйелі тәсіл кәсіпорынның сапа менеджменті негізделген бірнеше принциптерді қамтиды: [4]:

- ✓ Goal түпкі мақсат қағидаты;
- ✓ Unity бірлік принципі;
- ✓ Connect байланыс принципі;
- ✓ Mod модульдік құрылыс принципі;
- ✓ Ier иерархия қағидаты;
- ✓ Function функционалдылық принципі;
- ✓ Development даму принципі;
- ✓ Ent орталықсыздандыру қағидаты;
- ✓ Unc белгісіздік принципі.

Жаңалық бағдарламаларының сапасын басқаруда осы принциптерді қолдану өнімнің осы түріне жоғары рейтингке қол жеткізуге және тұтастай алғанда кәсіпорынның жұмысын жақсартуға мүмкіндік береді. Жүйелік тәсілдің барлық қағидаттары өте жоғары жалпылылыққа ие, яғни олар қолданбалы проблемалардың нақты мазмұнынан қатты алынып тасталған қатынастарды көрсетеді. Кез-келген нақты жүйеге, проблемаға, жағдайға, жүйелік көзқарастың принциптері көрсетілуі мүмкін және көрсетілуі керек [4].

Мақсаттардың иерархиялық құрылымы

2-суретте жүйедегі мақсаттардың иерархиялық құрылымын көрсетеді. Бұл модель мақсаттардың жиынтығы ретінде электрондық медиа жаңалықтар бағдарламаларын басқарудың сапасын көрсетеді.

G^0 жаһандық мақсатты, бірінші иерархиялық деңгейдегі жергілікті мақсаттардың жиынтығын атау – G^{I}, екіншісі – G^{II} жүйеде мақсаттардың иерархиялық құрылымы келесідей жазылады: $G^0 \rightarrow G^{\text{I}} \rightarrow G^{\text{II}}$.

Жаңалықтар бағдарламаларына арналған сапа менеджменті мақсаттарының иерархиялық құрылымы тізбегі күрделі жүйеде басқару элементтерінің маңызды қасиетін көрсетеді, яғни олар өздері қосылыстары, құрылымы және иерархиясы бар белгілі бір жүйені (ішкі жүйені) құрайды. Мұндай басқару жүйесі, ең бастысы, артықшылығы болып табылады және оның бағытталған жүйеге айналуын қамтамасыз етеді.

Басқару топтарын құратын көздер:

а) техникалық құралдар (басқару және басқа компьютерлер, микропроцессорлар, бағдарламалық құрылғылар, реттегіштер, бақылау, тұрақтандыру, компенсаторлық жүйелер және т.б.);

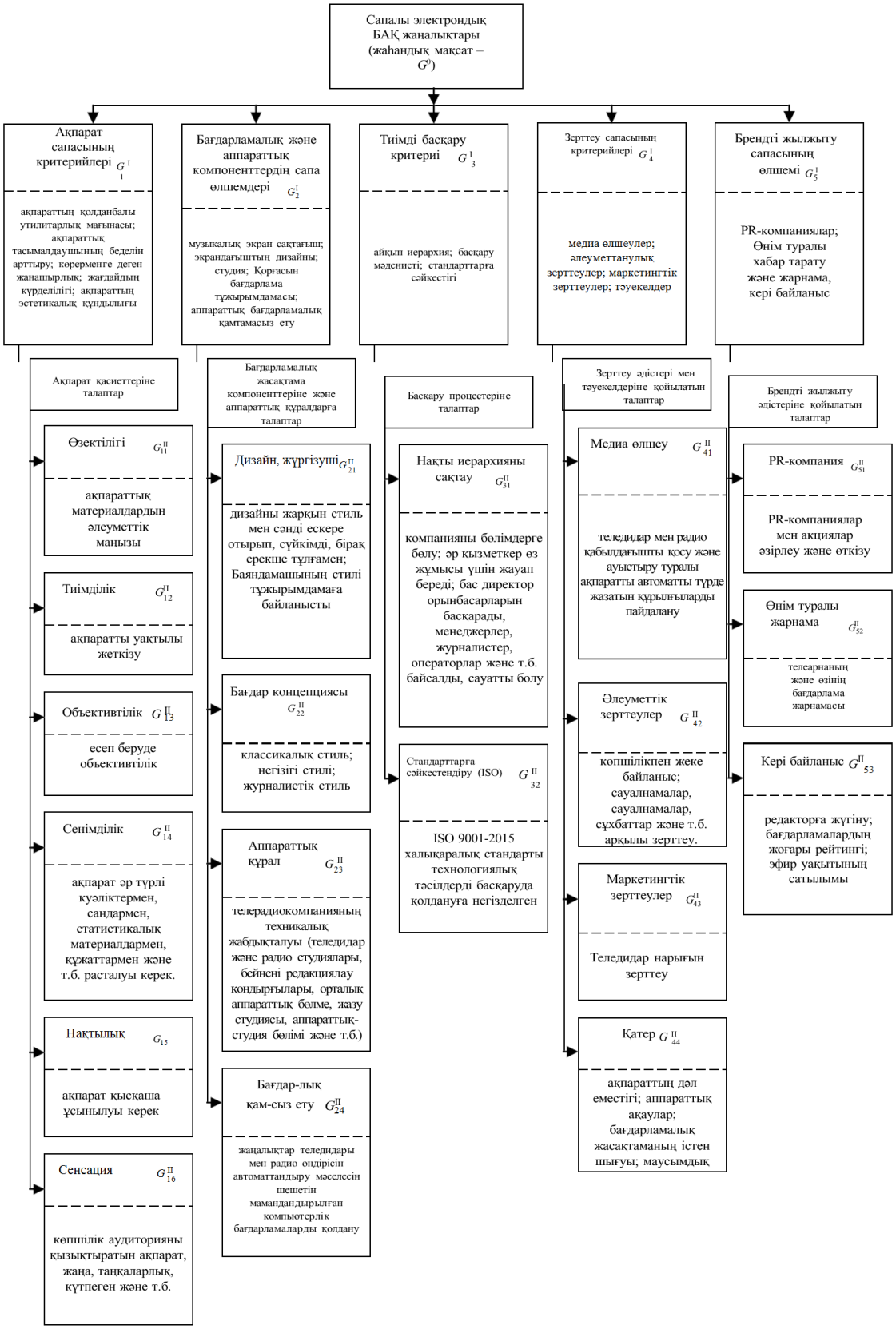
б) адамның әрекеттері мен шешімдері (бас директор, бағдарлама жетекшісі, техникалық директор, журналист, оператор, редактор, бағдарламалық жасақтама инженері, жауапты адам және т.б.).

Бұл екі көздің де жүйелік процестерге әсерімен және маңызды айырмашылықтарымен анықталатын бірқатар ортақ қасиеттері бар. Екі көздің де артықшылықтары мен кемшіліктері бар, сондықтан оларды бірге пайдалану пайдалы.

Мұндай объектілерді әдетте автоматтандырылған басқару жүйелері (АБЖ) деп атайды. Негізгі ұстанымдар барлық бақылау әрекеттерін қалыптастыру үшін техникалық құралдарға нұсқау беру және олардан гөрі адамнан гөрі жақсырақ, тезірек орындалатын барлық осы операцияларды орындау болып табылады.

Иерархиялық жүйелер әдетте бірінші иерархиялық деңгей модулдерін талдаудан бастап «жоғарыдан» зерттеледі және жасалады. Егер иерархия болмаса, зерттеуші жүйенің бөліктерін қандай тәртіппен қарастыратынын өзі шешуі керек.

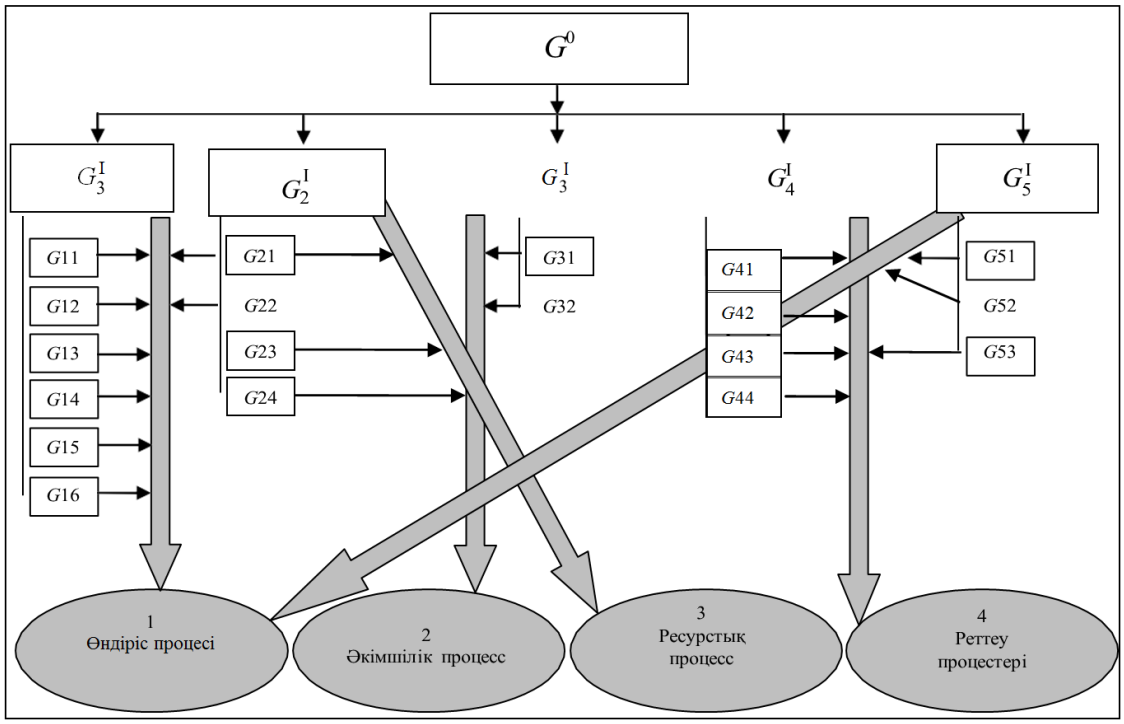
Бұл жағдайда иерархия қағидаты жүйеде элементтер, модульдер, мақсаттар арасындағы қатынастардың иерархиялық (доминантты) табиғатын табу немесе құру тиімділігіне бағытталған. Электрондық медиа жаңалықтар бағдарламаларын стандарттау өндіріс процесін жетілдіруге, жұмысты тиімді ұйымдастыруға және нәтижелерді арттыруға көмектеседі (атап айтқанда эфир уақытының сатылымын көбейтеді).



Сурет 2. Жаңалықтар бағдарламаларына арналған сапа менеджменті мақсаттарының иерархиялық құрылымы

ISO 9001–2015 халықаралық стандартындағы жаңалықтар бағдарламаларының сапа менеджментінің моделі

Жаңалық бағдарламаларының сапасын басқарудың (2-сурет) ұсынылған моделі тиімді жұмыс істеуі үшін біз оны ISO 9001–2015 халықаралық стандартының негізгі процестеріне келтіреміз (3-сурет).



Сурет 3. ИСО 9001-2015 стандартындағы жаңалықтар бағдарламаларының сапа менеджментінің моделі

Фокусталған жүйеде барлығы жаһандық мақсатқа бағынуы керек, біздің жағдайда сапалы жаңалықтар бағдарламалары. Егер түпкілікті мақсат толық анықталмаса, бұл жүйенің құрылымы мен басқаруындағы түсініксіздікке, нәтижесінде жүйеде дұрыс емес әрекеттерге әкелуі мүмкін. Мұндай әрекеттер түпкі мақсатқа сенбеу немесе оған жету мүмкіндігінің нәтижесі болуы мүмкін. Жүйелік тәсіл кәсіпорындағы көптеген мәселелерді шешуге көмектеседі, өйткені ISO 9000-2015 отбасының халықаралық стандарттары компанияның сыртқы және ішкі ортасын қамтитын сапа менеджментінің тиімді жүйесін енгізуге және қолдануға бағытталған. Кіріктірілген тәсіл кәсіпорын алдына қойылған міндеттерді тиімді шешеді.

Әдебиеттер

1. https://www.iso.org/ru/iso-9001-quality-management.html / ISO 9000 – современный менеджмент качества.

2. Ворошилов В. В. Менеджмент средств массовой информации. – СПб.: Изд-во Михайлова В. А., 2016. – 48 с.

3. Литовских А. М. Финансовый менеджмент: конспект лекций. – Таганрог: Изд-во ТРТУ, 2015. – 76 с.

4. Системный анализ в информационных технологиях / Ю. Ю. Громов, Н. А. Земской, А. В. Лагутин и др.– Тамбов: Изд-во ТГТУ, 2018. – 176 с.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ SOC-ТЫҢ АЛАТЫН ОРНЫ

Самрат С.М., Сулейменов О.Т.
e-mail: sanzhar.samrat@gmail.com, suleimenov97@gmail.com
ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты, Қазақстан

Аңдатпа: *мақалада ақпараттық қауіпсіздікті қамтамасыз ететін SOC командалық орталықтың құрылымы, жұмыс істеу принциптері, қолданатын технологиялары қарастырылған.*

Бүгінгі күні қауіпсіздікті қамтамасыз ететін жүйелер деректерді, олардың тұтастығын, қол жетімділігін толық қорғауды қамтамасыз етуге бағытталған. Өкінішке орай, мұндай жүйелерді іс жүзінде құрастыру мүмкін емес. Сондықтан шабуылдарды анықтау және оларға қарсы сауатты әрекет ету міндеті алдыңғы жоспарға шығады.

Security Operation Center (SOC) жүйесі қазіргі ақпараттық технологиялар заманында кеңінен танымал. Ақпараттық жүйелерге шабуылдар үнемі жетілдіріліп отырады, сондықтан оларға қарсы тұру үшін тиімді құралдар қажет. Ақпараттық қауіпсіз саласында SOC құру ұзақ мерзімде нақты нәтижелерге қол жеткізуге өзінің үлкен көмегін тигізеді.

Қазіргі таңда ақпараттық қауіпсіздікпен, деректердің тұтастығын, қолжетімділігін және құпиялығын қорғаумен, ақпараттық ағымдағы табиғи және жасанды қауіп-қатерлерді зерттеумен айналысатын ірі компаниялар бар. Cisco секілді қауіпсіздікпен айналысатын ірі компаниялар жылдық есептеріне көз жүгіртсек ақпаратты қорғауға арналған заманауи кешенді құралдардың дамуына қарамастан ақпараттық қауіпсіздік инциденттерінің саны азаймауда [1].

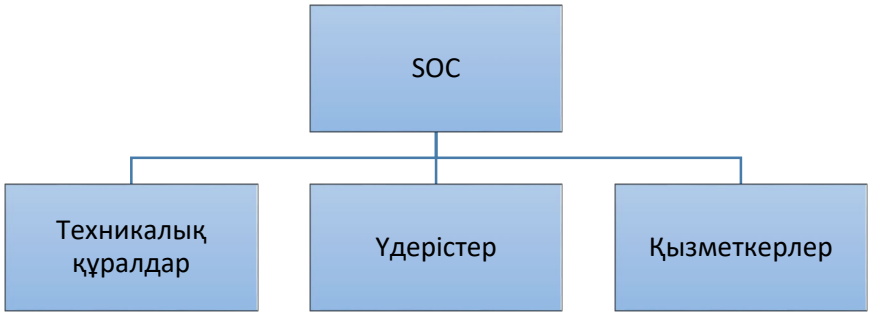
Ақпараттық қауіпсіздік инциденті (Information Security Incident) дегеніміз – жүйедегі ақпараттық қауіпсіздікті бұзатын, бұзуы мүмкін, күтпеген немесе жағымсыз кез-келген оқиғалар. Қазіргі таңдағы кездесетін инциденттердің 90% зиянды бағдарламалармен немесе олардың талап-етуші вирустар секілді түрлерінен келетін шабуылдар әсерінен тұрады. Cisco компаниясының 2018 жылдағы жылдық есебін қарасақ, сұрастырылған 2909 респонденттері инциденттердің келесі түрлерінен зиян шеккен [2]:

1-сурет. Cisco 2018 жылдық есебі

Ақпараттық қоғамда ақпараттық қауіпсіздік технологияларының дамуы инциденттермен, бірлестіктегі жүйеге өз зиянын келтіретін қауіп-қатерлермен күресетін, әр-түрлі инциденттермен жұмыс жасайтын орталықтардың пайда болуына әкелді. Ақпараттық қауіпсіз саласындағы замануи SOC ұйымдастырушылық және техникалық деңгейлердегі қауіпсіздік мәселелерімен айналысатын орталықтандырылған бөлімше. Ғимарат немесе кез-келген объектідегі SOC – бұл деректерді өңдеу технологиясын пайдалана отырып, қызметкерлер жүйені бақылайтын орталық орын.

Бүгінде Security Operation Center құру мәселелеріне ақпараттық-коммуникативті технологияларды, деректер базасын қолданатын сақтандыру компаниялары мен банктерден бастап ірі өнеркәсіптік кәсіпорындарға дейінгі көптеген салалар өкілдері қызығушылық танытуда. Мұндай қызығушылық, ең алдымен, үнемі жетілдірілетін шабуылдардан және оларға қарсы тұратын заманауи құралдардың қажеттілігінен туындады. SOC кез келген ірі ұйымның ақпараттық қауіпсіздік бөлімшесінің негізгі компоненттерінің бірі болып табылады. Бірінші кезекте ол мониторинг жүргізуге, инциденттерді, жағымсыз оқиғаларды анықтауға және оларға қарсы тұруға, олардың салдарының нәтежиесінде пайда болатын залалдар мен қаржылық шығындарды қысқартуға бағытталған [3].

Сонымен қатар Security Operation Center – бұл тек техникалық құралдар ғана емес, ақпараттық қауіпсіздік инциденттерін анықтау, талдау, әрекет ету, пайда болу туралы хабарлау және болдырмау міндеттерін атқаратын орталық болып табылады. SOC-тың бір маңызды компоненті — бұл үдерістер, себебі мониторинг пен инциденттерге жауап беретін бөлімше қызметкерлері арасындағы, сондай-ақ әр түрлі бөлімшелер арасындағы өзара байланыстар осы үдерістерден тұрады. Бұл үдерістердің қаншалықты сапалы жасалғаны SOC жұмысының тиімділігіне өз әсерін тигізеді. Сонымен кез келген SOC келесідей компоненттерден тұрады:



2-сурет. SOC компоненттері

Өз кезегінде SOC барлық уақытта эволюцияланатын және қоршаған орта жағдайларына сай тұрақты өзгеріп отыратын, бейімделетін күрделі ағзаға ұқсайды. Мұндай күрделі ағзаны құру үшін оның иесі тарапынан салмақты көзқарас және көптеген күш қажет. SOC құру — бірнеше жылға созылуы мүмкін ұзақ үрдіс, бұл ретте тек қорғау құралдарын жүйеге енгізу жарты жылға созылуы мүмкін.

SOC-тағы негізгі үрдістерді анықтау барысында SOC орындай алатын 40-тан астам негізгі функцияларды бөліп алуға болады: инциденттер туралы деректерді жинаудан бастап құқық қорғау органдарымен өзара іс-әрекеттерге дейін, зиянды кодты талдаудан бастап қызметкерлерге қауіпсіздік ережелерін таныстыруға дейін [4]. Тәжірибе жүзіне келгенде бір уақытта бұл міндеттердің барлығын бірдей қамтамасыз ететін орталықты ұйымдастыру мүмкін емес, мінсіз жүйе жоқ та шығар. Құрылған жүйенің алдында тұрған негізгі міндеттерге көңіл бөліп, олардың орындалуын қамтамасыз ететін процестерді сипаттау қажет. SOC-тің міндеттерін негізгі және көмекші деп бөліп қарастырсақ болады. Негізгі міндеттері:

- ақпараттық қауіпсіздік инциденттерін дер кезінде анықтау және оларға сәйкесінше қарсы әрекет ету;
- ақпараттық қауіпсіздік инциденттерінің алдын алу;
- кез-келген инцидент туралы есеп жасау, жүйені жетілдіруге байланысты кеңестер беру;
- бұрын болған инциденттерге талдау жасай отырып, болашақта оған қарсы тиімді әрекет етуге жағдай жасау;
- бұрын болған инциденттер негізінде компания саясатын өзгерту, ақпараттық қауіпсіздік жүйесін модернизациялау;
- инциденттер жайлы деректерді жинау, сақтау, олардың қауіпсіздігін қамтамасыз ету;
- қылмыстық және азаматтық құқық бұзушылық істерін ашуға бағытталған деректерді жинау;
- IT-жүйдегі деректердің тұтастығын қамтамасыз ету;
- келтірілетін зардаптарды минимизациялау;
- жүйеге мониторинг жасау;
- компания репутациясын және оның құнды ресурстарын сақтау;
- компания қызметкерлерін бастапқы ақпараттық қауіпсіздікпен таныстыру, инцидент болған кезде қандай стандарттар арқылы жұмыс жасау керек екенін үйрету.

Инциденттерді зерттеу және оған қарсы жауап қайтару – бұл күрделі комплексті процесс. Ол көптеген қызметкерлердің қатысуын талап етеді. Ең алдымен SOC командасына олар қорғайтын жүйенің инфрақұрылымы туралы өзекті ақпараттар болуы

тиіс және басқа бөлімшелердегі әріптестермен тиімді өзара әрекеттестіктік іс-әрекеттер қажет: жүйе иелері, менеджерлер, ақпараттық технологиялар және ақпараттық қауіпсіздік қызметкерлері, IT-саласының техникалық эксперттері, заңгерлер және т. б. Онсыз SOC жұмысын елестету қиын, сондықтан орталықты құру осы жұмыстардан басталуы қажет.

Жүйе инфраструктурасы және оның қызметтерімен толық танысып алғаннан кейін инциденттерді анықтау және олармен жүргізілетін жұмыстарды автоматтандыруға арналған негізгі процестер айқындалады.

SOC орталығы SIEM технологияларымен тығыз байланысты. Теориялық жағынан SIEM жоқ болса да SOC орталығын құру мүмкін, бірақ іс жүзінде ірі орталықтардың барлығында инциденттермен жұмыс жасау барысында SIEM технологиялары пайдаланылды.

SIEM (Security information and event management) технологиясы – желілік құрылғылар мен қосымшалардағы қауіпсіздік жүйесін әрдайым талдау жасап отыруға арналған үлкен көлемдегі техникалық құралдар кешені.

SIEM технологиясы жүйеге үздіксіз мониторинг жасап отырады. Оның негізгі функцияналдылығына келесілер жатады:

- агрегация жасау: деректер әртүрлі көздерден жиналады: желілік құрылғылар мен сервистер, қауіпсіздік жүйелерінің датчиктері, серверлер, деректер базалары, қосымшалар; зиянды оқиғаларды іздеу мақсатында деректерді топтастыру қамтамасыз етіледі.

- корреляция жасау: жалпы атрибуттарды іздеу, оқиғаларды маңызды кластерлерге байланыстыру. Технология келген бастапқы деректерді маңызды ақпаратқа айналдыру үшін әр түрлі көздерден деректерді интеграциялау үшін әр түрлі техникалық тәсілдерді қолдануды қамтамасыз етеді. Корреляция Security Event Management ішкі жиынының типтік функциясы болып табылады.

- хабарландыру: корреляциялық оқиғаларды автоматтандырылған талдау және ағымдағы проблемалар туралы хабарлау (дабыл) генерациясы. Хабарландыру қосымшаның интерфейстік панеліне шығарылуы мүмкін, сондай-ақ басқа да бөгде арналарға: e-mail, GSM-шлюзіне жіберілуі мүмкін.

- ақпараттық панелдер: оқиғаларды бақылауға көмектесетін әр-түрлі деректерді, диаграммаларды көрсететін интерфейстер.

- әр-түрлі деректерді сақтау: уақыт бойынша деректерді корреляциялау үшін және түрлендіруді қамтамасыз ету үшін өзіндік тәртіпте ұзақ мерзімді деректер қоймасын қолдану. Деректерді ұзақ уақыт сақтау компьютерлік-техникалық сараптамаларды жүргізу үшін керек, өйткені желілік оқыс оқиғаны тексеру қауіпсіздікті бұзу кезінде жүргізілуі екіталай.

- сараптамалық талдау жасау: әр түрлі тораптарда көптеген журналдар бойынша мәліметтер іздеу мүмкіндігі; бағдарламалық-техникалық сараптама шеңберінде орындалуы мүмкін;

Бұл технологияның техникалық артықшылығына DLP, IDP, антивирустар, маршрутизаторлардан келетін ақпараттарға әр-түрлі деңгейде талдау жасай алуын жатқызамыз. Өзінің критерилері бойынша әр түрлі ауытқулар болған жағдайда жүйе оны инцидент ретінде қабылдайтын болады. SIEM жұмысының негізіне математика мен статистика жатыр. Оның негізгі жұмысы ақпарат жинау және оған талдай жасай алу. Киберқылмысты анықтау барысында осы жүйе өте тиімді, себебі ол мәліметтердің барлығын жинап, сақтап отырады.

SIEM технологиясы банктік жүйелерде, сонымен қатар ірі көлемдегі қаржылық айналымдар жүретін компанияларда кеңінен пайдаланады.

Бірақта атап өткендей, SOC – ең алдымен командалық орталық, ал техникалық құралдар белгілі бір міндеттерді шешу үшін ғана қолданылады. Сол себепті орталық құру барысында ең алдымен қызметкерлердің санына емес, сапасына назар аударған жөн. Ақпараттық қауіпсіздікті қамтамасыз ететін орталықтағы қызметкерлердің білімдік деңгейін әр уақытта көтеріп отыру маңызды.

Әдебиеттер

1. Joseph Muniz, Gary McIntyre, Nadhem AlFardan. Security Operations Center: Building, Operating, and Maintaining your SOC. Published Nov 2, 2015 by Cisco Press.
2. Cisco. Cisco 2018 Annual Cybersecurity Report.
3. Лаборатория касперского. Сервисы «Лаборотории касперского» для SOC.
4. Алексей Лукацкий. Как функционирует Cisco Security Operations Center?
5. https://www.securitylab.ru
6. https://www.kaspersky.ru

ЭЛЕКТРОНДЫ ҚҰЖАТ АЙНАЛЫМДАҒЫ АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМАТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Сейтқали Ғ.Т.
e-mail: g.seitkali@gmail.com
әл-Фараби атындағы Қазақ Ұлттық Университеті,
Қазақстан

Аңдатпа. *Мақалада электронды құжат айналым туралы және оны құру жайында қысқаша ақпарат берілген. Электронды құжат айналым жүйесінің ақпараттық қауіпсіздігін қамтамасыз ету мәселелері қарастырылған. Электронды құжат айналым жүйелерінде құжаттардың сақталуын қамтамасыз етудегі проблемалар жайлы айтылған.*

Электронды құжат айналымының бірыңғай жүйесін жасау «электрондық үкімет» құрудың негізгі элементі екенін кәсіби мамандар жақсы түсінеді. Өйткені бұл жүйе құжат айналымы, яғни электронды құжат алмасу ғана емес, сонымен қатар ол құжаттардың, басшылық тапсырмаларының орындалу барысын жедел түрде тексеруге, кемшіліктердің алдын алуға, туындаған проблемаларды дерек базасын пайдалана отырып дер кезінде айқындауға және талдауға, басшылық үшін шешімдердің әртүрлі нұсқаларын әзірлеуге, ахуалды жақсартып отыруға мүмкіндік беретін бірден-бір жол. Бұл жүйе ақпараттарды, статистикалық мәліметтерді есепке алу мен іздестірудің жеңілдетілетіні және жылдамдатылатыны, құжаттарды жіктеу мен сақтаудың қарапайымданатыны іс жүзінде дәлелденіп отыр. Сонымен бірге, бұл жүйе қызметкерді жұмыста тұйықталудан сақтайды, істің мазмұндық жағына баса назар аударуға, жаңа ұсыныстар жасауға, шығармашылық жағынан өсуге ықпал етеді. Бағдарлама қызметкердің «қағазын қолына алып» кабинет-кабинетке жүгірмей, ол қағаздарға қол

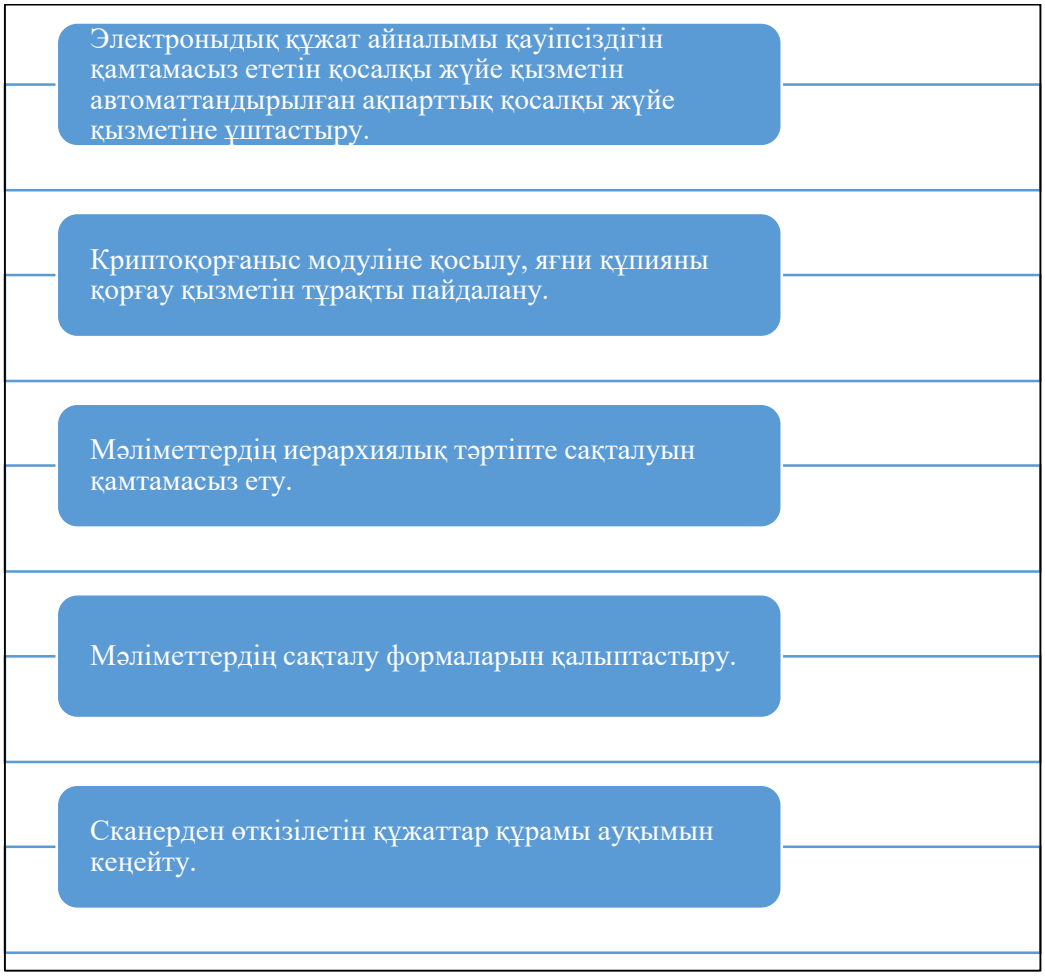
қойдырып, мөр бастыру үшін басшылардың қабылдау бөлмесі алдында кезекке де тұрмай, құжаттар жобасы туралы алыстан-ақ келісе беруіне, электрондық құжатты қағазға шығармай-ақ, оларды көбейтпей-ақ көптеген мекен-жайларға жолдай беруіне мүмкіндік береді.

Электронды құжат айналымы жүйесін іске қосу үшін 1-ші суретте көрсетілгендер қажет:

1-сурет. Электронды құжат айналым жүйесін құруға қажетті құрылғылар мен құралдар

«Қазақстанның мемлекеттік органдарының бірыңғай электронды құжат айналымы жүйесі 9 жыл ішінде 53,68 тонна қағазды үнемдеуге мүмкіндік берді. Қазіргі бұл жүйе 93 орталық және 1711 аймақтық мемлекеттік органдарында пайдаланылады. Бұрын министрліктен басқа облыстың аудандық әкімшілігіне немесе аймақтық органына дәстүрлі поштамен хатты жеткізу үшін 5-7 күн керек болатын. Электронды құжат айналымы жүйесінде бұған бар болғаны 15 минут қажет», - дейді ақпараттық технологияны дамыту департаментінің директоры Қ.Елеусізова [1].

Электрондық құжат айналымы іске қосылғаннан кейін электрондық мұрағат базасы да қалыптаса бастайды. Электрондық мұрағат қосалқы жүйесінің толық масштабты жобасын ендіру 2-ші суретте көрсетілген мәселелердің өз шешімін табуын ықпал етеді:



2-сурет. Электрондық мұрағат жүйесінің толық масштабты жобасының ықпалы

Электрондық құжат айналымының мақсаттары:

– құжаттардың электрондық түріндегі даярлануы, келісілуі, тіркелуі, берілуі есебінен еңбек сіңірілуін және уақытты азайту;

– кіріс, шығыс, ішкі, ұйымдастырушылық-өкім беру құжаттарының толық есепке алынуы мен олардың бірыңғай жүйеде сақталуы есебінен құжат айналымының айқындығын жоғарылату;

– қажетті құжатты іздеуге шығындалатын уақытты қысқарту;

– кәсіпорындағы «қағаз» құжат айналымымен байланысты шығындарды жою;

– ақпараттық қауіпсіздіктің талаптарын сақтау кезіндегі ақпараттың сапасын, толықтығын және шындылығын жақсарту;

– Шешімдерді қабылдау үшін қажетті ақпараттың жоқтығы мен қол жетімсіздігінің тәуекелін азайту; құжаттардың жойылу тәуекелін азайту;

– Құжаттардың қате нұсқаларын қолданумен байланысты тәуекелді азайту.

Электрондық құжатты құрастыру барысында 3-ші суретте көрсетілген деректемелерді негізге алу қажет:

3-сурет. Электрондық құжатты құрастыру деректемелері

Электронды құжат айналым жүйесін (ЭҚАЖ) ұйымдастыру тәртібі.

Электрондық құжат айналымын ұйымдастыру үшін ЭҚАЖ пайдаланылады, келесі функциялардың орындалуын қамтамасыз етеді:

– пайдаланушылардың қол жеткізуін авторландыру және қол жеткізу құқықтарын шектеу;

– электрондық хабарды қалыптастыру;

– электрондық құжаттың электрондық цифрлық қолтаңбасын қалыптастыру және тексеру;

– электрондық құжаттармен ұжымдық жұмыс;

– электрондық құжаттардың орындалуын бақылау;

– электрондық құжатты іздестіру;

– мемлекеттік орган шегінде және мемлекеттік органдардың арасында электрондық құжаттарды жіберу және алуын растау;

– электрондық құжаттарды сақтау;

– мемлекеттік органның электрондық құжаттар мұрағатына электрондық құжаттарды тапсыру;

Электронды құжат екі бөлімнен құралады: мазмұнды және деректемелік [2].

Құжаттың мазмұнды бөлігі мынадай форматтардағы бір немесе бірнеше файлдардан тұрады:

– графикалық;

– мәтіндік;

– кестелік;

– таныстырулар;

– мұрағатталған.

ЭҚАЖ-ге қатысушылар бірыңғай нормативтік-анықтамалық ақпаратты

пайдаланады. Ұйымдық-басқарушылық құжаттамаға қатысты нормативтік-анықтамалық ақпараттың реттелуі мен өзгеруін мұрағаттар мен құжаттаманы басқарудың уәкілетті органы жүзеге асырады.

ЭҚАЖ-дегі электрондық құжатты бастапқы өңдеу мыналарды қамтиды:

– электрондық құжаттың барлық деректемелерін тексеру;

– электрондық құжаттың барлық электрондық цифрлы қолтаңбаларының (одан әрі ЭЦҚ) дұрыстығын тексеру;

– ЭЦҚ-ны тіркеу куәлігінің және ЭЦҚ ашық кілтінің жарамдылығын тексеру;

– электрондық құжатта куәландырылған электрондық цифрлық қолтаңбаны пайдалана отырып, барлық тұлғалар мәртебесінің өкілеттіктерін тексеру.

Электронды құжаттар және олардың сақталуын қамтамасыз ету проблемалары.

Электронды құжаттарды есепке алудан бұрын есепке алу мәселесіне де тоқталуымыз жөн. Құжаттардың пайдаланылуын есепке алу мұрағат қоймасынан істер беру кітабы арқылы және берілген мұрағаттық анықтамалары, мұрағаттық үзінділерді, мұрағаттық көшірмелерді тіркеу журналы арқылы жүргізіледі.

Құжаттарды есепке алу әрбір мұрағат қоймасы бойынша бөлек жүзеге асырылады. Барлық сақтаулы құжаттар, соның ішінде істер тізімдемесіне енгізілмеген, бұл салаға жатпайтын құжаттар да, аса құнды құжаттардың сақтық көшірмелері мен пайдалану қорынан алынған көшірмелер де есепке алынуы керек. Есепке алу құжаттарына, сонымен қатар деректерді есепке алу базасына қол жеткізу тәртібі ұйым басшысы бұйрығымен (өкімімен) реттеледі. Есепке алу құжаттары белгіленген үлгі бойынша ресімделеді және олар сақтау бірлігіндегі мұрағаттық құжаттардың келіп түсуін, шығуын, санын, құрамын, жай–күйін жазуға арналады. Құжаттарды есепке алудың негізгі бірліктері мұрағаттық қор мен сақтау бірліктері болып табылады. Электрондық негіздегі құжаттарды есепке алу бірлігі ретінде бірыңғай бағдарламалық–ақпаратты нысананы құрайтын бір файл немесе бірнеше файл жазбалары барсақтау бірліктері және оған ілеспе құжаттама алынады [3].

Автоматтандырылған ақпараттық жүйелерде (ААЖ) қауіпсіздік мәселелері және оны шешу жолдары.

ААЖ қауіпсіздігін шешудің жолы ақпаратты қорғау кезінде тұтастықты сақтау болып табылады. Іс жүзінде қауіпсіздікті қамтамасыз ету саясатында сенімді және үздіксіз жұмыс жасайтын ақпараттық жүйені құру керек. Қауіпсіздікті қамтамасыз ету саясатының басты кезеңдері келесілер:

– ақпараттық және ұйымдастыру құрылымы мен ақпаратқа төнетін қауіпсіздікті қарастыру;

– қорғаныс құралдарын таңдау және орнату;

– қорғаныс құралдарымен жұмыс жасайтын қызметкерлер дайындау;

– ақпарат қауіпсізідігі мәселесіне қызмет көрсетуді ұйымдастыру;

– ААЖ ақпараттық қауіпсіздігін кезең бойынша қадағалау жүйесін құру [4].

ААЖ құрылымы мен ақпаратты өңдеу технологиясын зерттеудің нәтижесінде ААЖ ақпараттық қауіпсіздігінің концепциясы туындайды. Осының негізінде ААЖ ақпараттық қауіпсіздігін іске асыру жұмыстары жүргізіледі. Концепцияда келесі кезеңдер көрініс табады:

– ұйымның желісін ұйымдастыру;

– ақпаратты қорғауға төнетін қауіптерді зерттеу және іске асыру мүмкіндіктері мен іске асыру кезінде шамамен кететін шығынды есептеу;

– АЖ ақпаратты өңдеуді ұйымдастыру (қандай жұмыс орнында және қандай программалық қамтама көмегімен);

– қызметкерлердің сол немесе басқа ақпаратқа қол жеткізуін регламентациялау;

– қауіпсіздікті қамтамасыз етуде қызметкердің жауапкершілігі.

Қорытындылай келгенде, ААЖ ақпарат қауіпсіздігінің концепциясы негізінде келесі шарттарды қанағаттандыратын қауіпсіздіктің схемасы құрылады:

– корпоративті желіге рұқсатсыз енуден және байланыс арналары арқылы өтетін ақпараттың жойылуынан қорғау;

– желі сегменттері арасындағы ақпараттар ағынын шектеу;

– желінің күрделі ресурстарын қорғау;

– жұмыс жасау орындары мен ресурстарды рұсқатсыз қол жетуден қорғау;

– ақпараттық ресурстарды криптографиялық қорғау.

Заманауи автоматтандырылған ақпараттық жүйелердегі (ААЖ) қорғау объектісі мәліметтерді таратылған түрде өңдеуге арналған аумақтық бөлінген күрделі құрылымды гетерогенді желі болып табылады. Көп жағдайда бұл желіні корпоративті желі деп атайды. Мұндай желінің ерекшелігі әр түрлі өндірушілердің құрылғыларымен мен кез келген желілік құралдардың, сонымен қатар ақпаратты өңдеуді бірлесіп атқаруға арналмаған бір текті емес программалық қамтамалардың жұмыс жасай беретіндігінде.

Әдебиеттер

1. Мақала: «Электрондық құжат айналымы» жүйесінің арқасында 50 мыңнан астам тонна қағаз үнемделді. - https://strategy2050.kz/news/13767/ (09.12.2019).

2. Бобылева М.П. Управленческий документооборот: от бумажного к электронному. Вопросы теории и практики - 470 стр.

3. Корнеев И.К. Информационные технологии в работе с документами. – 297 стр.

4. Методы и средства работы с документами ISBN: 5-8360-0262-2; 2000 г. – 376 стр.

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ - АҚПАРАТТЫҚ ҚАУІПСІЗДІК АСПЕКТІСІНДЕ

Шайкулова А.А., Калижанова А.У.

Ғ. Дәукеев атындағы Алматы энергетика және байланыс университеті, Қазақстан

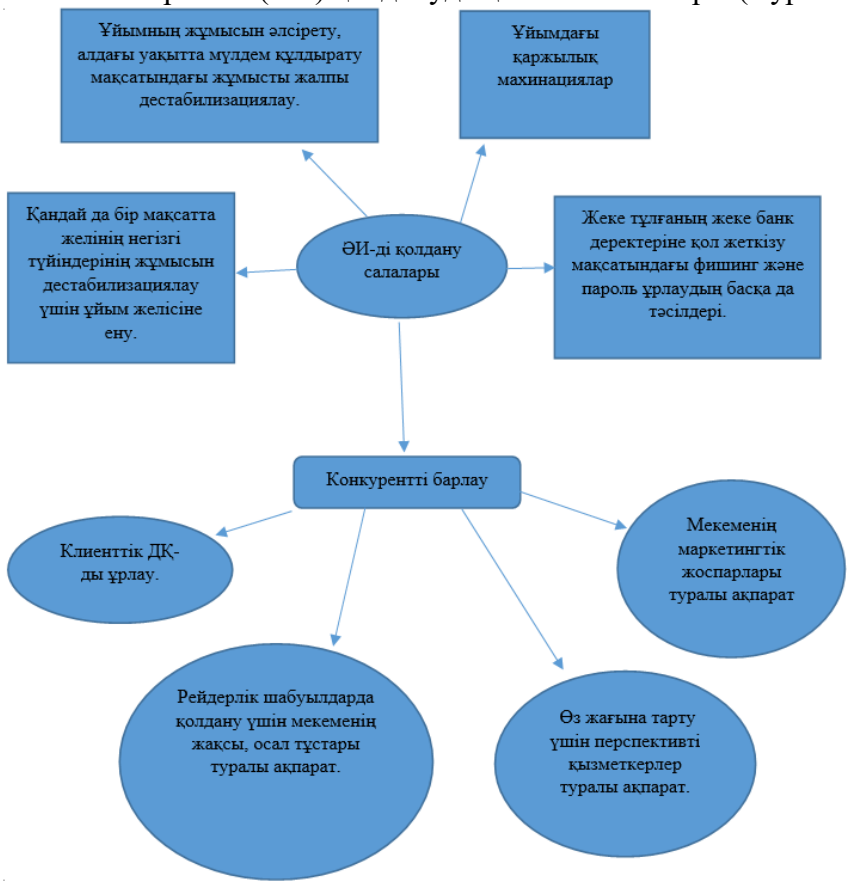
Аңдатпа. *Ақапараттық қауіпсіздік саласында адам факторы бүгінгі таңда үлкен рөл атқарып отыр. Қазір барлық мемлекеттік және коммерциялық ұйымдарда ақпарат қауіпсіздігін программалық және аппараттық жолмен қамтамасыз ету арқылы қауіпсіздік мәселесі шешімін тапты деп есептейді. Бұл Интернет пайда болғанға дейін тиімді тәсіл болғанымен, Интернет қоғамға дендеп енгеннен кейін жоғарыда айтылған тәсілдер ақпарат қауіпсіздігін толыққанды қамтамасыз етеді деп айту қиын. Әлеуметтік инженерия әдісін тиімді қолданып жатқан хакерлер үшін*

желіаралық экрандарды, идентификациялау құрылғыларын, шифрлау құралдарын, желілік және басқа да шабуылдарды анықтау жүйелерін айналып өту, сол арқылы қажетті ақпаратқа қол жеткізу үйреншікті іске айналып бара жатқан тәрізді. Олай болса ақпаратты қорғау саласында әлеуметтік инженерия әдістерін зерттеу, оларға қарсы тұру шараларын әзірлеу және қызметте пайдалану бүгнгі күннің өткір мәселесі болмақ.

***Түйіндік сөздер**: әлеуметтік инженерия, әлеуметтік инженериядан қорғау, ақпарат қауіпсіздігі, адами факторлар.*

Ақпараттық қауіпсіздік аспектісіндегі әлеуметтік инженерия деген не? Википедияда бұған мынадай анықтама беріледі: Әлеуметтану мен психологияны пайдалана отырып, нақты қажетті нәтижеге барынша тиімді әкелетін жағдайлар мен кеңістікті құру тәсілдерінің, әдістерінің және технологияларының жиынтығы. Ақпарат қауіпсіздігі аспектісінде анықтама берер болсақ, Әлеуметтік инженерия - бағдарламалық қамтамасыз етуді бұзумен байланысты емес, ақпаратқа рұқсатсыз қол жеткізу үшін қаскүнемдер пайдаланатын термин; мақсаты - жүйеге қол жеткізу үшін қолданылатын құпия сөздерді немесе жүйенің қауіпсіздігін бұзуға көмектесетін өзге де ақпаратты алу үшін адамдарды алдау. Әлеуметтік инженерияның әдістері көп, олар түрлі мақсатта қолданылады. Ақпарат қауіпсіздігіне көңіл бөлген кезде адам факторлары ескерілу керек және бұл аса маңызды.

Әлеуметтік инженерияны (ӘИ) қолданудың негізгі салалары (Сурет 1):



Сурет 1 - Әлеуметтік инженерияны қолданудың негізгі салалары

Көптеген зерттеушілер әлеуметтік инженерияны XXI ғ. хакерлерінің негізгі құралы санайды. Себебі, техникалық қорғау құралдары, программалық қорғау құралдары күннен күнге дамуда, ал адамдардың әлсіз жақтары, ойламдары, стереотиптері өзгермейді. Ең сенімді, керемет деген қорғау жабдығын қолданғанның өзінде, адами фактордың да бар екенін естен шығармау керек. А.Энштейн айтады: «Әлем бар және адамның ақымақтығы бар. Және де біріншісіне байланысты мен онша сенімді емеспін». Қаскүнемдер арасында әлеуметтік инженерияның танымалдығы өсуде, себебі кәсіпорын қызметкерлерінің өздері – адамдар, қорғау жүйесіндегі ең әлсіз буын болып табылады. Бұл фактіде көптеген түсініктемелер бар, біріншіден - жұмыскерлердің бір бөлігінің білімі жеткіліксіз, және оларға осындай шабуылдан аулақ болу үшін тәжірибе жетіспейді, сондай-ақ кәсіпорындардың көп бөлігі физикалық периметрді сыртқы қауіптерден қорғау туралы ғана ойлайды. Қызметкердің көмегімен, осы сыртқы қорғауды айналып өтіп, қаскүнем ең үлкен кедергіні айналып өтеді. Әлеуметтік инженерия тұтастай алғанда кәсіпорынның контексінде маңызды аспект болып табылады, өйткені қорғау жүйесі қаскүнем үшін еңсерілетін кедергіні қиындатады және бұл жағдайда қаскүнемге қандай қызметкерді алдағаны маңызды емес, себебі нәтиже - қорғау кедергісін айналып өтіп, барлық ішкі ресурстарға қол жеткізу маңызды. Әлеуметтік инженерияның шабуылдары құпия ақпаратпен жұмыс істеуде ең үлкен құзыретті қызметкерлерге жиі бағытталған. Шабуыл әдісі ретінде әлеуметтік инженерияның таралуының маңызды себептерінің бірі – бұл шабуылдың өте арзан түрі, шабуылдаушы Ақпараттық технологиялар саласындағы маман болмауы да мүмкін. Сондай-ақ, әлеуметтік инженерия әдістерін пайдалану кезінде нәтижеге басқа әдістермен салыстырғанда жылдамырақ қол жеткізетіндігі де маңызды фактор болып табылады. Әлеуметтік инженерияның әдістері көп, олардың ішінде жиі кездесетіндері мыналар:

Кардинг. Бұл алаяқтық түрі банк карталарымен, деректермен және т.б. түрлі іс-әрекеттерді қамтиды. Банкоматтарда деректерді, пин-кодтар мен парольдерді оқитын түрлі құрылғылар пайдаланылды. Қазір, әрине, терминалдарды қорғау мүлдем басқа деңгейде, бірақ кардинг толығымен жойылды деп айтуға болмайды.

Претекстинг (сценарий). Алдын ала анықталған әрекеттер жиыны, нәтижесінде құрбан қандай да бір ақпаратты береді немесе белгілі бір әрекетті орындайды.

Бұл әдіс клиент туралы ақпаратты ашу (туған күні, әлеуметтік сақтандыру нөмірі, шоттағы соңғы сомасы және т. б.) үшін қолданылады, ол үшін

–телефондық әңгімені жазып алу;

–пайдалы есептерді, банк есептерін алу (тікелей компания өкілдерінен) көзделеді.

Фишинг. Қолданушылардың құпия деректеріне рұқсатсыз қол жеткізу мүмкіндігін алу мақсатындағы интернеттегі алаяқтық түрлерінің бірі.

Мысалы, 2013 жылы электрондық почта арқылы жіберілген 509 хаттан 1-ші фишингтік хат болған.

1 фишингтік шабуылдың өзіндік құны 2000$-ға дейін жетеді, ал пайда 10000$-ға дейін жетеді.

Фишерлер жалған электрондық хаттарды қолданады.

Мысалы: банктің атынан жіберіп, парольді растауды сұрауы немесе ірі көлемде ақша аудару туралы білдіріс жіберуі мүмкін.

Құрбан фишердің алдауына оңай түседі, өз еркімен және деректерін бере салады. Олар жақсы психологтар, әрекеттері – нақты.

Фармин. Фишингке қарағанда қауіптірек алаяқтық болып табылады. Мақсаты DNS-адресті өзгерту, нәтижесінде қолданушы түсетін сайт түпнұсқа емес, фишинг бет болып шығады. Фарминг қолданушыларды фальш сайттарға автоматты түрде қайта бағыттайды. Қолданушы өзі қалап, банк сайтына кіреді. Бірақ бұның жасанды сайт екенін білмейді.

Фармингтің негізгі екі формасы бар:

1) Потенциалды құрбандардың компьютеріне хакерлер зиянкес ПҚ орнатады.

Компьютерге кірген вирус автоматты түрде қолданушыны кіргісі келген сайттан автоматты түрде жасанды сайтқа (онлайн банк немесе дүкен) қайта бағыттап жібереді.

2) Өте аяр, бүлдіргіш. DNS серверді жұқтыру, нәтижесінде оның әрбір қолуданушысы алаяқтық сайтқа бағытталатын болады.

Рейдерлік шабуылдар. Рейдерлер – кәсіпорынды басып алушылар. Рейдерлік шабуыл – кәсіпорында басып алу шабуылы.

Трояндық ат. Қолданушының көрсеқызарлығына, қорқынышына немесе басқа да эмоцияларына негізделеді. Қаскүнем электрондық почта арқылы мыналарды қамтитын (салым) хат жіберуі мүмкін:

– Антивирусты «жаңарту»;
– Ақшалай ұтысқа кілт;
– Қызметкерге компромат;
– Апгрейд қандай да бір программа үшін;
– Эротикалық мазмұндағы скрин–сейвер;
– Адамды жаңылыстыратын жаңалық және т.с.с..

Нәтижесінде сол хаттағы салымдық файлды жүктеген кезде ондағы зиянкес программа компьютерді жұқтырады. Бұл құрбанның компьютерінде белгілі бір командаларды орындауға немесе қандай да бір қажет ПҚ орнатуға мүмкіндік береді.

Кво үшін Кви. Бұл техникада қолданушыға қаскүнем электрондық почта немесе корпоративтік телефон арқылы хабарласады. Қаскүнем тех.қолдау қызметкері ретінде танысып, компьютерлік жүйеде тех. ақаудың бар–жоғы жөнінде сұрайды. Егер ақау бар болса, оны жоюды ұсынады:

– белгілі бір команданы енгізу;
– қандай да бір ПҚ–ны орнату және т.с.с..

Осыдан соң вирустық ПҚ–ны жүктеу мүмкіндігі ашылады.

«Жолдағы алма». Бұл әдіс троян атын бейімдеуді білдіреді және физикалық тасымалдағыштарды (CD, флешкалар) қолданады.

Қаскүнем жүктеу флешкаларын немесе дискілерді (ішінде қызық, уникальді контенттері болады. Сыртында құрбанның қызығушылығын тудыратын компания логотипі және қандай да бір жазба болуы мүмкін) компания маңында, автотұрақтағы машинада, лифттегі сөмкеде, туалетте, асханада және т.с.с. тастап кетеді (кімге тиесілі, сол адам алатындай қолайлы жерде). Нәтижесінде вирус таралып, шабуыл жасалады.

Шабуылдан қорғау әдістері. Өкінішке орай, шабуылдаушының қандай шабуылды таңдайтынын болжау мүмкін емес, қай уақыт кезеңінде жасалатынын, кім құрбан болатынын да анықтау қиын, бірақ төменде келтірілген қорғау әдістерін пайдалана отырып, шабуылдың сәтті жасалуына кедергі жасауға болады.

Қорғау жүйесін тестілеу. Бөтен адамның (қаскүнем) тарапынан қауіпсіздіктің кемшіліктерін анықтау әдісі. Бұл әдісті пайдалана отырып, қауіпсіздік саясатын әзірлеу кезінде бастапқыда ескерілмеген қорғаныс кемшіліктерін де анықтауға болады. Тестілеу

кезінде қызметкерлердің жеке өмірі мен ұйым қауіпсіздігінің нәзік мәселелері қозғалуы мүмкін, сондықтан мұндай іс-шараны өткізуге алдын ала рұқсат алу қажет.

Хабардарлық. Хабардар болу - бұл қызметкерлердің негізгі принциптері мен қажетті қорғау ережелерін меңгеруіне бағытталған алдын ала ескерту шарасы. Әрине, бұл аспект қызметкерлерді оқыту мен тестілеуді талап етеді. Осы шара шеңберінде келесі тармақтарға назар аударылады:

1. Ақпараттық қауіпсіздік мәселелеріне адамдардың назарын аудару;
2. Қызметкерлердің мәселенің маңыздылығын сезінуі және ұйымның қауіпсіздік саясатын қабылдауы;
3. Ақпараттық қамтамасыз етуді, қорғауды арттыру үшін қажетті әдістер мен іс-әрекеттерді зерделеу және енгізу.

Қорытынды

Әлеуметтік инженериядан қорғау әдістерінің тізімін шексіз жалғастыруға болады, бірақ бұл қаскүнемдер мен алаяқтардан барлық ресурстарды қорғайды деген сөз емес. Соған қарамастан адами факторларды анықтау, адами факторлар тарапынан орын алатын қажетсіз әрекеттерді болдырмау, оның алдын алуда әлеуметтік инженерия туралы білімді тарату, одан қорғану шараларын әзірлеу өте маңызды.

Әдебиеттер

1. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры.- СПб.: БХВ-Петербург, 2007. - 368 с.
2. Инструменты социальной инженерии (Электрон. ресурс) / Способ доступа: URL: https://itglobal.com/ru-kz/company/blog/kak-ponizit-rol-soczialnoj-inzhenerii-v-ugroze-proniknoveniya/
3. Социальная инженерия – как не стать жертвой? (Электрон. ресурс) / Способ доступа: URL: https://efsol.ru/articles/social-engineering.html

СОКРЫТЫЕ ВОДЯНЫЕ ЗНАКИ С ИСПОЛЬЗОВАНИЕМ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ

Абдикаликов К.А.
e-mail: abdikalikov@mail.ru
Актюбинский университет имени С. Баишева МОН РК,
Казахстан

Аннотация. *Рассматривается стеганографические методы, которые скрывают информацию с использованием алгоритма БПФ в потоках оцифрованных сигналов и реализуются на базе компьютерной техники и программного обеспечения в рамках отдельных вычислительных систем, корпоративных или глобальных сетей.*

Проблема информационной безопасности решается на протяжении всей истории человечества. Еще в древности выделились две основные направления защиты информационных ресурсов: криптография и стеганография. Криптография блокирует несанкционированный доступ к данным путем их шифрования. Стеганография же идет

принципиально далее - ее цель скрыть сам факт существования конфиденциальной информации. Хотя стеганография имеет очень долгую и богатую историю, однако только в последнее время в связи с бурным развитием информационных технологий, в частности с появлением компьютерных сетей, а также из-за наличия ограничений на использование криптосистемы и чрезвычайную актуальность проблемы защиты интеллектуальной собственности, стеганография становится предметом растущего интереса и активных научных исследований.

Так, большинство существующие программные обеспечения (ПО) построены на основе модификаций известного стеганографического метода - метода наименьшего значащего бита. Цифровые контейнеры, созданные таким ПО, характеризуются низкой устойчивостью и не могут обеспечить приемлемого уровня защиты информации. Нарушение имеющихся в контейнере корреляционных связей, обусловленное "вкраплениями" в него дополнительных данных, легко обнаружить визуальной атакой на младшие биты или применением к контейнеру серии статистических атак. Кроме того, информация может быть уничтожена активным противником

Более стойкими являются спектральные алгоритмы. Но те, что известные на сегодня, разрабатывались, прежде всего, исходя из потребностей защиты интеллектуальной цифровой собственности, и поэтому характеризуются малой пропускной способностью создаваемого стегоканалу, достаточной для передачи в сигнале-контейнере только минимума информации: логотипа фирмы, имени и координат владельца контейнера, определенной битовой последовательности небольшой длины и т. п.

Стеганографических алгоритмов, сочетающие в себе высокую устойчивость и пропускную способность при приемлемом вычислительной сложности своей реализации, нами не найдены. Таким образом, задача надежной скрытой передачи больших объемов информации на сегодня решается недостаточно эффективными путями. Необходимость усовершенствования существующих стеганографических методов и систем, практические потребности создания и сопровождения соответствующего программного обеспечения определяют актуальность выбранной проблемы исследования.

Проблемой разработки и усовершенствования методов стеганографии занимаются многие отечественные и зарубежные ученые: В.Г. Грибунин, В.К. Задирака, И.Н. Оков, Б.Я. Рябко, Р.Г. Бияшев, И.В. Туринцев, А.Н. Фионов, К. Качин (C. Cachin), Р. Андерсон (R. Anderson), Х. Фарид (H. Farid), К. Салливан (K. Sullivan), Д. Фридрич (J. Fridrich), Н. Провос (N. Provos), Абдикаликова Н.И. и др. С каждым годом растет число публикаций, посвященных стеганографии, а также в смежных областях науки. Широко применяются результаты и достижения классических наук и различных их направлений: теории информации, кодирования, алгебры, физики и т.д.

Впервые было предложено класс спектральных стеганографических алгоритмов на основе теории преобразования Фурье [1] с двойной защитой скрываемой информации: информация "внедрение" в шум сигнала-контейнера (первый уровень сокрытия) на уровне погрешности округления, возникающая при переходе от пространственного представления сигнала к частотному (второй уровень), в зависимости от условий функционирования стегосистемы может быть использована модификация алгоритма с длинным или с коротким ключом, а также предложен класс спектральных стеганографических алгоритмов (на базе теоремы о свертке), пропускная способность

стегоканалу для которых может быть соразмерны с пропускной способностью канала, дает метод наименьшего значимого бита.

Осуществлена оптимизация предложенных алгоритмов.

Полученные новые теоретические результаты в области стеганографических алгоритмов внедрены в учебный процесс Актюбинского государственного университета им. К.Жубанова и университете Байшева.

Практическая значимость полученных результатов: повышает в проведении оптимизации вычислительных затрат путем использования быстрых алгоритмов для вычисления дискретного преобразования Фурье.

На базе описанных алгоритмов создано соответствующее программное обеспечение, "внедрение" сообщения в одномерные и двумерные действительные контейнеры, в частности модельные сигналы и файлы формата FITS, полученные из сети Internet.

Данный алгоритм, в [2], основан на изменении фазы и амплитуды сигнала, получаемого из изображения путем дискретного преобразования Фурье (ДПФ). Формулы (ДПФ) выглядят следующим образом:

• Прямое $$F(k_1,k_2)=\beta\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}f(n_1,n_2)e^{-j2\pi n_1k_1/N_1-j2\pi n_2k_2/N_2}$$

• Обратное $$f(n_1,n_2)=\beta\sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1}F(k_1,k_2)e^{j2\pi k_1n_1/N_1+j2\pi k_2n_2/N_2}$$

где коэффициент $\beta=(N_1N_2)^{-1/2}$, определяется из условия, что после последовательного применения прямого и обратного преобразований мы получим исходный сигнал.

Отметим что, такое преобразование генерирует комплексные значения и, следовательно, может быть представлено в виде амплитуды и фазы. Так как мы работаем с картинкой, у которой не может быть комплексных значений яркости точек, то при изменении фазы и амплитуды в точке (k_1, k_2) на $+\alpha$ и $+A$ мы должны изменить фазу и амплитуду в точке (N_1-k_1, N_2-k_2) на $-\alpha$ и $+A$ соответственно.

Исследования показали, что фаза сильнее влияет на изображение, чем амплитуда, поэтому для увеличения стойкости следует использовать именно её. Для извлечения информации данные дискретного преобразования Фурье полученные из проверяемой картинки сравниваются с оригиналом.

Литература

1. Задирака В.К. Теория вычисления преобразования Фурье. -Киев: Наук. думка, 1983. - 216 с.

2. Beauchamp K.C. The Walch transform - a new tool for control engineers //Cybernetics. -1972. -V.2. - P.113-125.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ИНФРАСТРУКТУРАХ

Айтхожаева Е.Ж., Акатаев Н.Н.
e-mail: nurba82@gmail.com
Казахский Национальный Технический Университет имени К.И. Сатпаева, Казахстан

Аннотация. *Рассматривается система стандартизации ISO/IEC 27k на системы управления информационной безопасности (ИБ), стандарты которой применяются для обеспечения безопасности объектов критической информационно-коммуникационной инфраструктуры (ИКИ), выполняется их классификация по областям применения. Особое внимание уделяется стандарту СТ РК ISO/IEC 27010:2017 (на основе стандарта ISO/IEC 27010:2015), целенаправленному на применение в критических инфраструктурах. Обсуждаются существующие в РК критерии отнесения объектов к критически важным объектам ИКИ, неполнота которых диктует необходимость их корректировки и разработки алгоритмов оценки критичности бизнес-процессов.*

Введение. Проблема информационной безопасности (ИБ) любой инфраструктуры имеет первостепенное значение как при проектировании инфраструктуры, так и ее эксплуатации. Эта проблема приобретает особую остроту, когда речь идет об обеспечении безопасности объектов критической информационно-коммуникационной инфраструктуры (КВОИКИ). Киберугрозы безопасности КВОИКИ представляют собой стратегические угрозы безопасности страны, независимо от своего характера. Обеспечение безопасности КВОИКИ - это обеспечение национальной безопасности.

Критически важная информационно-коммуникационная инфраструктура (ИКИ) может относиться к одной из таких сфер, как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, атомная энергетика, оборонная промышленность, химическая промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность. И не обязательно субъект критической информационно-коммуникационной инфраструктуры должен являться государственным органом или государственным учреждением. Это может быть любое казахстанское юридическое лицо, индивидуальный предприниматель. Все определяется сферой деятельности субъекта.

Главным аспектом решения проблемы кибербезопасности информационных технологий (ИТ) является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ. Для этого разработана система стандартизации, которая существует и развивается в виде международных и национальных стандартов и регламентов, действующих в сфере ИБ, как для любых ИКИ, так и для КВОИКИ.

Система стандартизации на системы управления ИБ. Ключевыми характеристиками информационной безопасности являются конфиденциальность, целостность, доступность. Главная цель системы стандартизации в области ИБ - обеспечение гарантий указанных свойств информации через регламентацию мер по обеспечению надлежащего уровня защищенности информационно-коммуникационной

инфраструктуры, в том числе и критически важных объектов информационно-коммуникационной инфраструктуры.

Семейство международных стандартов на Системы Управления (Менеджмента) Информационной Безопасностью (СУИБ или СМИБ) ISO/IEC 27k разрабатывается ISO/IEC JTC 1/SC 27. Включает в себя более 70 стандартов, 50 из которых опубликовано, по остальным имеются проекты или они находятся в разработке (используется последовательная схема нумерации стандартов, начиная с 27000 и далее) [1].

Большинство стандартов семейства ISO/IEC 27k связано между собой. Основополагающий стандарт 27000 включает больше десяти документов. ISO/IEC 27000:2018 содержит информацию о том, какую взаимосвязь имеют стандарты: область деятельности, роль, функции и отношения друг с другом. В ISO/IEC 27000 дается укрупненная классификация стандартов, по которой они делятся на четыре класса: стандарты, описывающие общие принципы и терминологию; стандарты, устанавливающие требования; стандарты, содержащие общие рекомендации; стандарты, содержащие рекомендации для специальных областей.

Эта классификация не дает полного представления об охвате стандартами областей ИБ. Ниже приводится более подробная классификация, которая позволяет уяснить области применимости семейства ISO/IEC 27k и систематизировать осмысление стандартов:

- стандарты, содержащие определения, основные принципы и требования к СУИБ, базовую структуру управления ИБ, а также компетенции, навыки и знания, требуемые профессионалам в области управления ИБ (27000, 27001, 27014, 27021);
- стандарты, содержащие практические правила управления ИБ (27002);
- стандарты, содержащие руководства по внедрению СУИБ, обеспечению кибербезопасности (27003, 27013, 27032, 27100, 27101, 27103);
- стандарты, содержащие метрики и измерения (27004);
- стандарты, регламентирующие управление рисками ИБ, в том числе для межсекторных и межорганизационных коммуникаций (27005, 27010, 27554, 27557);
- стандарты, содержащие требования к органам аудита и сертификации систем управления информационной безопасностью (27006, 27007, 27008);
- стандарты, регламентирующие управление сетевой безопасностью (27033 – 7 частей);
- стандарты обеспечения безопасности приложений (27034 – 6 частей);
- стандарты, регламентирующие управление инцидентами ИБ, в том числе выявление и расследование инцидентов (27035 – 3 части, 27037, 27039, 27040, 27041, 27042, 27043, 27050);
- отраслевые стандарты, ориентированные на применение в определенных сферах деятельности, учитывающие специфические угрозы и уязвимости этих сфер (27009 – рекомендации по разработке отраслевых стандартов, 27016 - экономика управления информационной безопасностью, 27011 – электросвязь, 27015 - финансовый и страховой сектор, 27019 – энергетика, 27102 - киберстрахование, 27799 - здравоохранение и др.);
- стандарты обеспечения безопасности при взаимодействии с поставщиками, в том числе и с поставщиками облачных услуг (27036 – 3 части, 27017, 27018, 27070, 27071). Облачные вычисления имеют свои особенности, что привело к необходимости разработки специальных стандартов, регламентирующих управление ИБ в облаках на основе ISO/IEC 27002, защиту персональных данных, взаимодействие между поставщиками и клиентами облачных сервисов;

- стандарты, которые регламентируют требования для аутентификации, в том числе и биометрической (27099, 27551, 27553);

- стандарты, которые будут регламентировать безопасность и конфиденциальность «умных городов» и Интернет-вещей - Smart City и IoT (27030, 27570);

- стандарты, которые будут регламентировать процессы защиты и конфиденциальности Big Data (27045, 27046).

Классификация является отчасти условной, так как некоторые стандарты можно отнести к нескольким классам. Например, 7 часть стандарта ISO/IEC 27033 по управлению сетевой безопасностью (Руководство по обеспечению безопасности беспроводных сетей - Риски, методы проектирования и механизмы контроля), касается также и управления рисками и содержит требования к механизмам контроля ИБ (аудит). Следует заметить, что это не единственный стандарт, в котором содержатся требования к механизмам контроля СУИБ.

Практически все отраслевые стандарты представляют собой отраслевое дополнение к стандарту ISO/IEC 27001 с учетом специфических требований безопасности, а внедрение стандартов, и не только отраслевых, регламентируется ISO/IEC 27002.

Все стандарты периодически обновляются с разными интервалами во времени. Например, стандарт ISO/IEC 27000 был обновлен в 2018 году, а последние версии стандартов ISO/IEC 27001 и ISO/IEC 27002 датируются 2015 годом, действующая версия стандарта ISO/IEC 27008 выпущена в 2019 году.

Большинство национальных стандартов по СУИБ представляют собой гармонизированные и адаптированные международные стандарты. В национальных стандартах указано «Настоящий стандарт идентичен международному» с указанием наименования международного стандарта.

Казахстан не является исключением: на постоянной основе ведется работа по выпуску национальных стандартов по СУИБ на казахском и русском языках с сохранением нумерации международных стандартов. Например, СТ РК ISO/IEC 27001, СТ РК ISO/IEC 27004, СТ РК ISO/IEC 27008, СТ РК ISO/IEC 27010, СТ РК ISO/IEC 27033, и др.

Среди международных стандартов есть стандарт ISO/IEC 27010:2015, который ориентирован именно на КВОИКИ. Стандарт представляет собой руководство по совместному использованию информации, выходящей за границы отдельных секторов экономики и государств: по рискам информационной безопасности, механизмам контроля, проблемам и инцидентам. ISO/IEC 27010:2015 предназначен для поддержки создания доверия при обмене и предоставлении конфиденциальной информации в критичных инфраструктурах. Можно сказать, что основная суть стандарта – это дополнения и уточнения стандартов ISO/IEC 27001 и ISO/IEC 27002 с целью обеспечения доверительного обмена и совместного пользования конфиденциальной информацией, в том числе в критически важных информационно-коммуникационных инфраструктурах.

Стандарт Республики Казахстан СТ РК ISO/IEC 27010:2017 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности для связи между подразделениями и организациями» (на основе стандарта ISO/IEC 27010:2015) идентичен ISO/IEC 27010:2015. Он имеет приложения, в которых содержится: описание потенциальных выгод от обмена конфиденциальной информацией между организациями; руководство о том, как члены

сообщества обмена информацией могут оценить степень доверия, которое может быть оказано предоставленной информации; описание протокола «Светофор», широко используемого в сообществах по обмену информацией для маркировки конфиденциальной информации с целью указания аудитории ее дальнейшее распространение и примеры моделей организации сообщества по обмену информацией [2].

Стандарт разработан для применения при обмене и совместном пользовании конфиденциальной информацией любыми предприятиями, как в Казахстане, так и на международном уровне. Его можно применять в важнейших критических инфраструктурах государства или организации.

Определение критичности важных объектов информационно-коммуникационной инфраструктуры.

В статье 6 Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации» указано, что перечень критически важных объектов информационно-коммуникационной инфраструктуры, а также правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры утверждает Правительство Республики Казахстан.

В постановлении Правительства РК от 8 сентября 2016 года № 529 (изменения внесены постановлением Правительства РК от 09.04.2018 № 179) утверждаются правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры.

Указаны четыре критерия отнесения объектов ИКИ к КВОИКИ [3]:

- влияние объекта ИКИ на непрерывную эксплуатацию особо важных государственных объектов, при нарушении функционирования которого будет остановлена деятельность особо важных государственных объектов;
- влияние объекта ИКИ на непрерывную и безопасную эксплуатацию стратегических объектов, при нарушении функционирования которого будет остановлена деятельность стратегических объектов либо возникает угроза чрезвычайной ситуации техногенного характера;
- влияние объекта ИКИ на непрерывную и безопасную эксплуатацию объектов отраслей экономики, имеющих стратегическое значение, при нарушении функционирования которого будет остановлена деятельность объектов отраслей экономики, имеющих стратегическое значение, либо возникает угроза чрезвычайной ситуации техногенного характера;
- влияние объекта информационно-коммуникационной инфраструктуры на обеспечение устойчивого функционирования объекта информатизации "электронного правительства" и иных информационно-коммуникационных услуг, частичное или полное нарушение (прекращение) функционирования которых может привести к чрезвычайной ситуации социального характера.

Эти критерии не охватывают весь спектр влияния объектов КИИ на национальную безопасность. Например, по этим критериям организации из сферы здравоохранения не будут относиться к КВОИКИ. Этим самым исключается здоровье нации из национальной безопасности.

Видимо, исходя из этих критериев, в докладе МЦРОАП РК (2019 год) «О состоянии информационной безопасности» указано, что имеется всего 219 критически важных

объектов ИКИ в РК из числа 29000 организаций, имеющих собственную инфраструктуру. 130 объектов планируется добавить в текущем году.

При рассмотрении критически важных информационно-коммуникационных инфраструктур, кроме общепринятых стандартов, необходимо дополнительное нормативно-правовое регулирование.

В Приказе Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16 марта 2018 года № 44/НҚ "Об утверждении Правил создания и обеспечения функционирования единой национальной резервной платформы хранения электронных информационных ресурсов" отдельными пунктами выделены требования для КВОИКИ.

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 № 52/НҚ "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры" непосредственно касается КВОИКИ.

Официальный интернет-ресурс Комитета по информационной безопасности Министерства Цифрового Развития, Инноваций и Аэрокосмической Промышленности Республики Казахстан имеет раздел "Обеспечение информационной безопасности КВОИКИ", в котором представлено актуальное понятие КВОИКИ и обязанностей КВОИКИ со ссылками на официальные документы, приводятся порядок, методика и правила испытаний объектов информатизации «электронного правительства» и информационных систем в ГТС (Государственная техническая служба).

Выводы. Необходимо дополнить критерии отнесения объектов ИКИ к КВОИКИ. Так как к КВОИКИ применяется дополнительное нормативно-правовое регулирование, очень важно определиться, является ли защищаемый объект КВОИКИ. И, если является, необходимо определить насколько значима его критичность, т.е. необходимо провести его категорирование. Для адекватного отнесения объектов ИКИ к КВОИКИ и категорирования КВОИКИ необходим анализ критичности бизнес-процессов организации, как это делается, например, в РФ. Для этого необходимо разработать алгоритмы оценки критичности бизнес-процессов или адаптировать алгоритмы мировой практики с учетом особенностей РК.

Литература

1. Standards by ISO/IEC JTC 1/SC 27. Information security, cybersecurity and privacy protection. https://www.iso.org/ru/committee/45306/x/catalogue (2.12.2019).
2. СТ РК ISO/IEC 27010:2017 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности для связи между подразделениями и организациями» (на основе стандарта ISO/IEC 27010:2015).
3. Постановление Правительства РК от 8 сентября 2016 года № 529 Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры (с изменениями и дополнениями по состоянию на 26.12.2018 г.).

СТАНДАРТЫ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ И КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Айтхожаева Е.Ж., Сырлыбаева А.Н.
e-mail: syrlybayeva.assiya@gmail.com
Казахский Национальный Технический Университет имени К.И.Сатпаева, Казахстан

Аннотация. *Рассматриваются международные стандарты в области расследования инцидентов, которые являются основой компьютерной криминалистики. Отмечается отсутствие аналогичных стандартов в Казахстане, кроме одного. Приводятся стандарты РК, которые частично можно применить при расследовании инцидентов. Выполняется тестирование на выявление инцидентов безопасности с использованием общедоступного сетевого сниффера Wireshark и обучающего веб-ресурса ENISA. Отмечается необходимость разработки стандартов РК в области расследования инцидентов, гармонизированных с международными стандартами.*

Введение. Повсеместное применение ИТ во всех сферах человеческой деятельности, переход общества к статусу «цифрового» открыло не только новые возможности для развития и совершенствования общества, но и привело к новым угрозам, массовому росту кибератак. Инциденты, нарушающие конфиденциальность, целостность и доступность информации являются массовым явлением во всем мире. Согласно отчетов Международного союза электросвязи (ITU) по результатам ежегодных исследований в Глобальном индексе кибербезопасности Казахстан в 2017 году занимал 82 место, в 2018 году - 71 место, а в 2019 году - 40 место из 193 стран мира. Уровень кибербезопасности государств оценивается по пяти основным показателям: законодательная база, технические и организационные мероприятия, деятельность на международной арене и создание потенциала развития сферы информационной безопасности (ИБ). Можно сказать, что Казахстан вошёл в список стран с высоким уровнем готовности противостояния угрозам ИБ.

Расследование инцидентов. Киберпреступления присутствуют везде, где используются в том или ином виде информационные технологии (компьютерные системы, локальные и глобальные сети, облачные среды, мобильная связь, телекоммуникации).

Инциденты нарушения ИБ могут иметь самые разные последствия, но все они должны быть расследованы. Для того, чтобы иметь возможность расследования инцидентов, необходимо иметь логи, в которых фиксируются события. Существует целый класс программных систем сбора и корреляции событий информационной безопасности (UBA, UEBA, SIEM, SOAR). Но их использование не решает саму проблему расследования киберпреступлений (инцидентов кибербезопасности). Этой проблемой занимается форензика (компьютерная криминалистика), которая является сравнительно новой, но очень важной областью ИБ.

В процессе расследования инцидентов выделяют четыре основных этапа: сбор, исследование, анализ, представление [1, 2].

Самый важный первый этап - сбор улик и доказательств. Начинается с разработки плана сбора информации, улик и доказательств, в том числе и с носителей компьютерной информации.

На втором этапе проводится экспертное исследование собранной информации и объектов-носителей. Оно включает извлечение, а также считывание информации с носителей, декодирование и вычисление из нее той информации, которая имеет отношение к делу. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе вся найденная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

На заключительном этапе специалистам необходимо представить отчет о результатах анализа, который включает в себя описание выполненных действий, используемых методик и инструментов

Международные стандарты форензики. Для расследования инцидентов применяются разные методы цифровой криминалистики. Цель стандартов, относящихся к цифровой криминалистике, состоит в том, чтобы продвигать передовые методы и процессы для сбора и исследования цифровых доказательств, используемых при расследовании киберпреступлений.

К международным стандартам, рассматривающим вопросы компьютерной криминалистики, относятся следующие стандарты:

- ISO/IEC 17799:2005 Code of practice for information security management (описывает процедуры, мероприятия и обязанности по управлению инцидентами);
- ISO/IEC TR 18044:2004 Information security incident management (описывает информацию реагирования на инциденты для менеджеров ИБ);
- ISO/IEC 27035 Information technology - Security techniques - Security incident management (описывает руководство по управлению инцидентами для крупных и средних организаций);
- ISO/IEC 27037 Information technology - Security techniques - Guidelines for identification, collection and/or acquisition and preservation of digital evidence (описывает обработку цифровых доказательств, идентификацию, сбор, приобретение и сохранение потенциальных цифровых доказательств, имеющих доказательную ценность);
- ISO/IEC 27038 Information technology - Security techniques - Specification for digital redaction (определяет характеристики методов для цифрового редактирования цифровых документов, которые могут использоваться как для сокрытия конфиденциальной информации, так и для сокрытия следов преступлений);
- ISO/IEC 27039 Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS) (определяет требования к системам обнаружения вторжений, которые используются для выявления атак и вторжений в сеть или систему и оповещения о них);
- ISO/IEC 27041 Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method (руководство по обеспечению процессов судебной экспертизы цифровыми доказательствами с сохранением и подтверждением уверенности в их целостности и достоверности);
- ISO/IEC 27042 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (описывает анализ и интерпретацию

цифровых доказательств для решения проблем преемственности, достоверности, воспроизводимости и повторяемости);

- ISO/IEC 27043 Information technology - Security techniques - Incident investigation principles and processes (описывает процессы и принципы, применимые к различным видам расследования);

- ISO/IEC 27050 Information technology — Electronic discovery (4 части стандарта охватывают как нетехнический, так и технический персонал, связанный с расследованием преступлений, с указанием действий по идентификации, сохранению, сбору, обработки и анализу информации при расследовании).

Стандарты РК. В Казахстане имеется один государственный стандарт СТ РК ИСО/МЭК 17799-2006 на основе ISO/IEC 17799-2005. Национальные стандарты, гармонизированные и адаптированные с другими международными стандартами, направленными на расследование инцидентов, отсутствуют.

Но в РК есть стандарты, которые частично можно применить при расследовании инцидентов, такие как:

- СТ РК ИСО/МЭК 15408 (3 части) Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (содержит сведения о классах доверия к вычислительным системам, что, в принципе, можно соотнести с классами доверия при расследовании инцидентов безопасности);

- СТ РК 1699-2007 Системы контроля и управления доступом. Общие технические требования (описывает общие требования и классификацию систем контроля и управления доступом отечественного и иностранного производств, рассмотрены требования технической системы контроля и управления санкционированным доступом и перемещением людей, транспорта и других объектов в (из) контролируемой зоны);

- СТ РК ГОСТ Р 51275-2017 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (описывает общие угрозы информационной безопасности, процессы сбора логов, работу SIEM-систем);

- СТ РК ГОСТ Р 51188-2007 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Общие требования (описывает обеспечение специальной обработки программных средств в целях выявления компьютерных вирусов, а также на устранение последствий, вызванных возможными воздействиями компьютерных вирусов на операционные системы, системные и пользовательские файлы с программами и данными, начальные секторы магнитных дисков, таблицы размещения файлов);

- СТ РК ИСО/МЭК ТО 14516-2007 Технологии информационные. Методы обеспечения защиты. Использование и управление услугами доверенной третьей стороны. Общие требования (описывает требования при обмене информацией между двумя сторонами, включая элементы доверия).

Судебные экспертизы при расследовании преступлений в сфере компьютерной информации

Для того чтобы успешно проводить расследования инцидентов информационной безопасности необходимо обладать практическими навыками работы с инструментами по извлечению цифровых артефактов. Основная цель при проведении работ -

использование методов и средств для сохранения (неизменности), сбора и анализа цифровых вещественных доказательств, для того чтобы восстановить события инцидента.

Ниже представлено рассмотрение этапов расследования преступления, с использованием общедоступного сетевого сниффера Wireshark.

Моделируемая ситуация: рабочая станция диспетчерского контроля и сбора данных (SCADA), используемая для управления производственным процессом. Данные, а именно сетевые пакеты данной моделируемой ситуации, предоставляются обучаемой веб-страницей ENISA Collection of CERT [3].

Приложение, работающее на рабочей станции SCADA, дает оператору две кнопки для управления работой насоса. Одна кнопка для выключения насоса и другая - для аварийного отключения, если по какой-то причине первая кнопка не работает. Несмотря на кажущуюся простоту, эта система имеет решающее значение для работы установки. Сеть не имеет связи с другими сетями. В этом сценарии четыре системы будут связаны между собой одним аппаратным коммутатором, как показано на рисунке 1. Поскольку необходимо будет отслеживать трафик, поступающий во все вышеперечисленные системы и от них, для захвата трафика необходимо настроить Span-порт на коммутаторе, где будет отражаться трафик от четырех систем (рабочих станций и PLK).

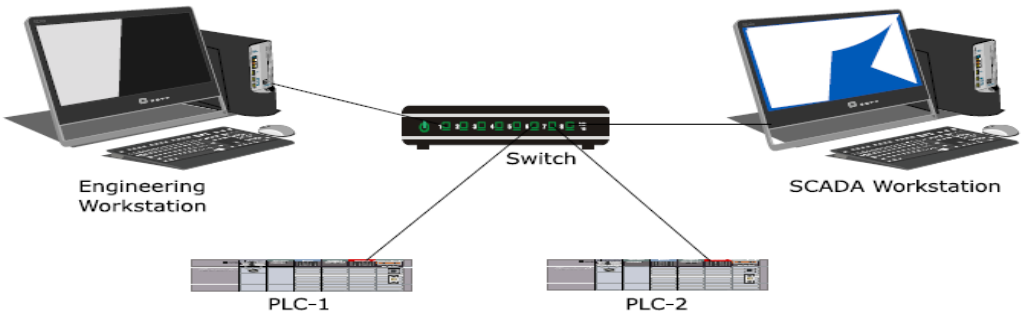


Рис. 1. Настройка сети на атомной электростанции

При анализе исследуемого пакета подозрительным показались пакеты сеансов, ориентированные на авторизацию, проходящие по протоколу VNC.

На SCADA использовалась аутентификация типа VNC, которая является процессом ответа «1» или «0» на вызов. Сервер отправляет запрос аутентификации, случайную 16-байтовую строку. Клиент отправляет ответ аутентификации, содержащий также 16-байтовую строку, состоящую из запроса, зашифрованного алгоритмом DES, ключом шифрования которого является пароль. Сервер отвечает пакетом результатов аутентификации. Первые четыре байта кодируют целое число, значение 1 означает, что аутентификация была неудачной; значение 0 означает, что аутентификация прошла успешно. В случае неудачной аутентификации сервер добавит строку, описывающую причину неудачной аутентификации, а затем закроет соединение.

Необычный тип аутентификации (TightVNC) выдает первоначальное VNC-соединение, с которого началась предполагаемая атака (рис. 2, рис. 3).

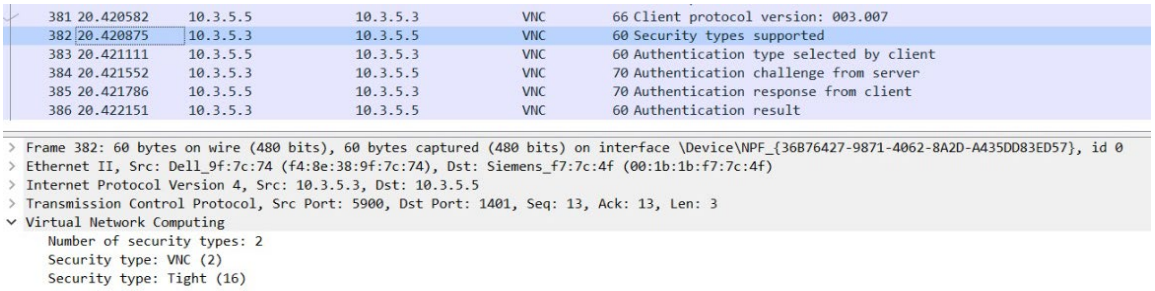


Рис. 2. Сканирование авторизации VNC

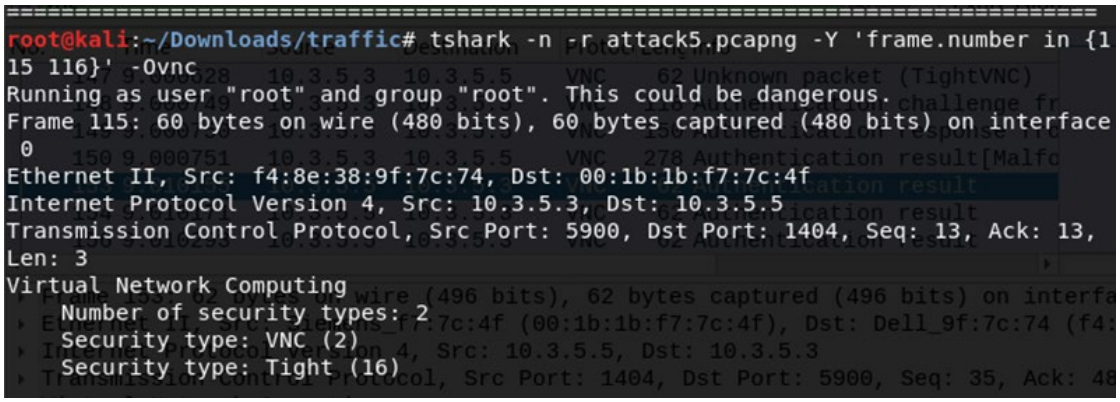


Рис. 3. Проверка типа протокола VNC

Были произведены попытки подбора пароля. В первых сеансах сервер отвечает пакетами результатов неудачной аутентификации которые содержат код 1 = Authentication result: Failed, что и следовало ожидать (рис. 4).

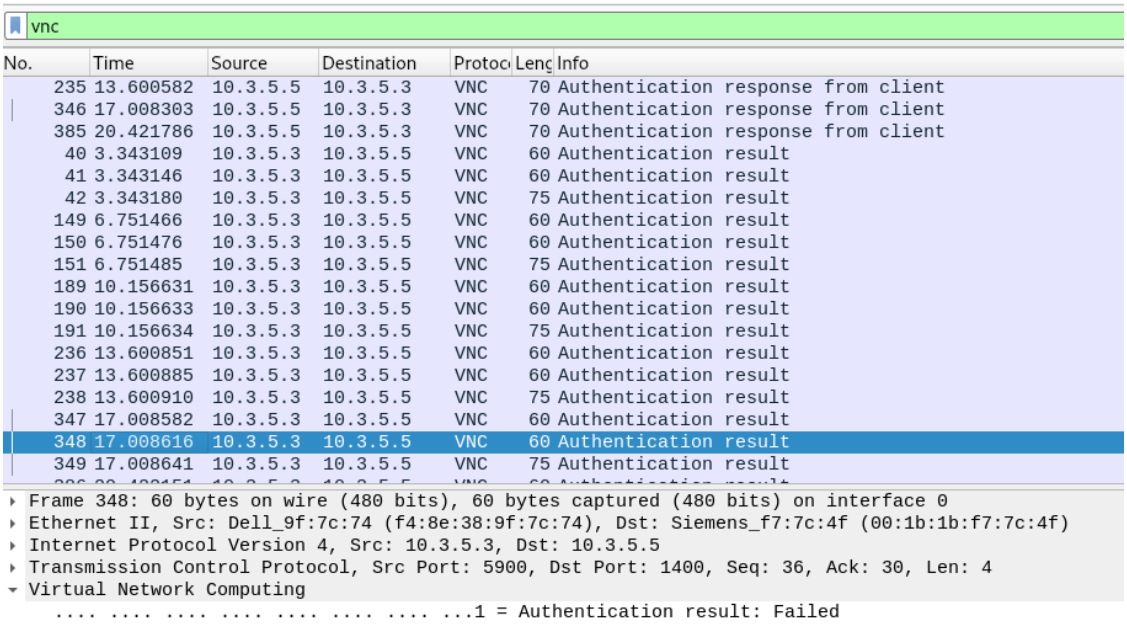


Рис. 4. Результат неудачной авторизации хакера

Ответ сервера на предпоследнюю попытку имеет код 0, но присоединена строка «Ошибка аутентификации». Последний сеанс отличается, есть только один пакет результатов аутентификации, и на этот раз он имеет значение 0 = Authentication result: OK, и никакой дополнительной строки не прикреплено (рис.5). Кроме того, клиент закрывает соединение, что видно из следующего пакета TCP. Следовательно, злоумышленник имеет пароль к системе.

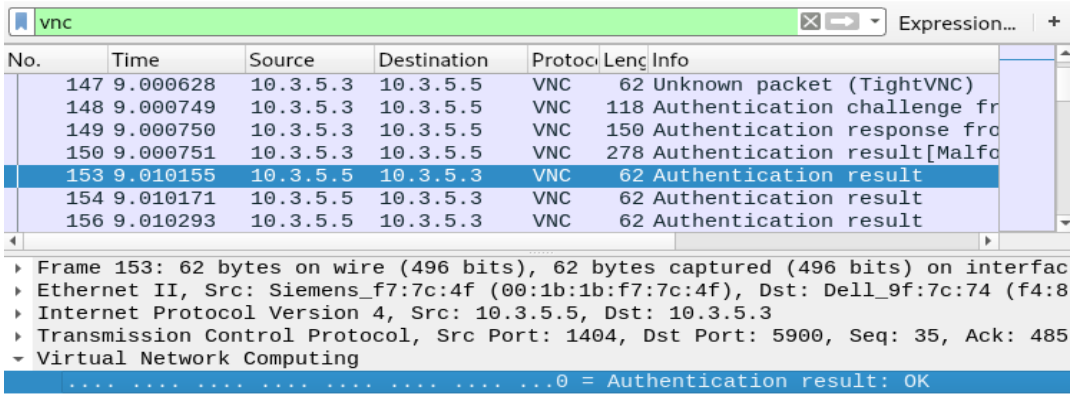


Рис. 5. Результат удачной авторизации хакера

Комбинация соединения VNC и инцидента (отключение насоса) вызывает подозрения, так как оператор SCADA обычно не использует удаленное соединение, а сидит напротив рабочей станции. Поэтому необходимо тщательного изучить сеансы соединений VNC, рассмотрев движения и нажатия кнопок мыши «событие указателя клиента». Кнопка 1 нажимается в кадре 1126 в положении x = 518 / y = 261, как видно на рисунке 6.

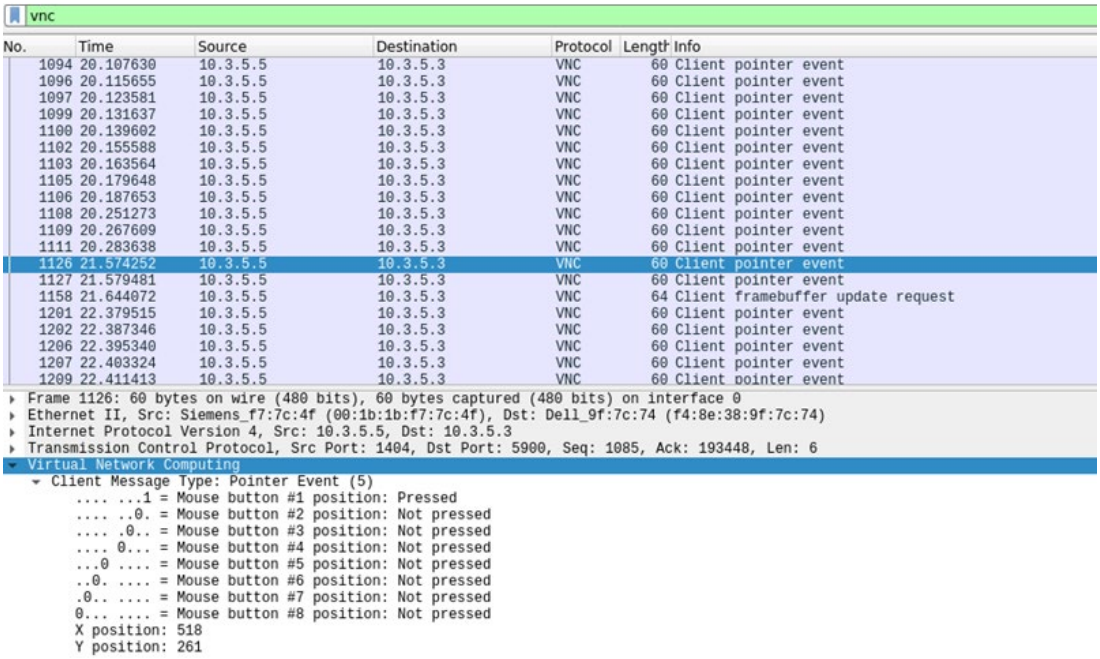


Рис. 6. Результаты нажатия мыши

Соответственно, после нажатия этой кнопки происходит сразу два события, которые при обычной авторизации проходят поэтапно. А именно аутентификация и вывод из строя насоса.

Таким образом был выявлен инцидент: проведение атаки грубой силы по подбору пароля и отключению насоса.

Выводы. Каждый из приведенных выше международных стандартов с разной степенью пояснения и в различной структуре описывает набор мер построения процесса управления инцидентами информационной безопасности. Необходима разработка стандартов РК путем гармонизации и адаптации международных стандартов в области компьютерной криминалистики. При этом следует учесть обновление международных стандартов и тенденцию к увеличению их количества в области форензики.

Приведенное тестовое расследование полностью моделирует инцидент реальной жизни, так как исследуемые пакеты, предоставленные обучающим центром ENISA, получены с реальной атомной станции. Такое, приближенное к реальным условиям, расследование готовит начинающего специалиста к оперативным действиям и выбору методики сетевой криминалистики.

Литература

1. Casey, E. Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet / E. Casey. – NYC: Academic Press, 2011. – 840 p.
2. Федотов, Н.Н. Форензика – компьютерная криминалистика /Н.Н. Федотов. – Москва: Юридический Мир, 2007. – 432 с.
3. European Union Agency for Cybersecurity. ENISA Collection of CERT. - https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#network_forensics (13.11.2019)

ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ НОВОГО АЛГОРИТМА ШИФРОВАНИЯ QAMAL

Алгазы[2] К.Т, Бабенко[1] Л.К., Бияшев[2] Р.Г., Ищукова[1] Е.А., Капалова[2] Н.А., Нысанбаева[2] С.Е.

e-mail: kunbolat@mail.ru

[1]Институт компьютерный технологий и информационной безопасности Южного федерального университета, Россия

[2]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В настоящий момент в Республике Казахстан ведутся работы по разработке нового стандарта симметричного шифрования данных. Одним из претендентов на роль стандарты выступает алгоритм шифрования Qamal, разработанный и Институте информационных и вычислительных технологий (г. Алматы, Республика Казахстан). В статье рассмотрены дифференциальные свойства основных операций, составляющих шифр Qamal. Рассмотрены подходы к построению*

многораундовых характеристик для шифра Qamal. Было показано, что для версии шифра со 128-битным блоком данных и таким же размером секретного ключа уже для трех раундов шифрования имеет сложность нахождения правильных пар текстов 2^{-120}, что делает дифференциальный криптоанализ неприменимым к шифру Qamal.

Актуальность исследования

Первым из известных государственных стандартов шифрования данных стал стандарт DES, принятый в США в начале 70-х годов. Это было то время, когда первые ЭВМ (электронные вычислительные машины) постепенно переставали быть экзотикой и начали входить в жизнь и работу небольших фирм и исследовательских лабораторий. Это привело к тому, что проблема защиты данных, хранимых и обрабатываемых на них, осознавалась все большим числом специалистов. Многие крупные корпорации, не говоря уже о государственных службах, проводили собственные исследования в данной области. В результате стали появляться различные алгоритмы шифрования. Одним из самых известных исследовательских центров такого рода в те времена являлась научная лаборатория фирмы IBM, возглавляемая доктором Хорстом Фейстелем [1]. В результате была создана система шифрования под названием Люцифер. Для этой системы шифрования Хорстом Фейстелем была предложена математическая модель, которая в настоящее время носит название «схема Фейстеля». Принцип схемы Фейстеля заключается в том, что за один раунд зашифровывается только половина или часть текста. Блок текста разделяется на части. Одна часть проходит через некоторое математическое преобразование. И результат этого преобразования складывается по модулю два со второй частью текста. После этого части текста меняются местами. Еще одним плюсом схемы оказался тот факт, что за счет использования операции «Исключающее-ИЛИ» или как ее еще называют операция сложения по модулю два становится возможным использовать одну и ту же схему как для зашифрования данных, так и для расшифрования данных, достаточно только изменить порядок следования раундовых подключей. Изначально стандарт DES принимался сроком на 5 лет, но впоследствии его срок в статусе стандарта был неоднократно продлен [2]. К концу 20 века компьютеры уже получили широкое распространение и вычислительные мощности выросли в разы. Поэтому правительство США задумалось о смене стандарта. В результате был объявлен конкурс на принятие нового стандарта шифрования данных – конкурс AES (Advanced Encryption Standard). Конкурс был объявлен в 1997 году Национальным институтом стандартов и технологий США (NIST – National Institute of Standards and Technologies) [3]. Для участия в конкурсе было заявлено 15 алгоритмов шифрования, созданных учеными разных стран. В результате пятилетнего исследования в качестве нового стандарта США был выбран алгоритм шифрования Rijndael, разработанный двумя учеными-математиками из Бельгии — Винсентом Риджменом (V. Rijmen) и Джоан Дейменом (J. Daemen). Алгоритм Rijndael построен по схеме сети на основе подстановок и перестановок (SPN) и имеет архитектуру «Квадрат» (Squre). На тот момент архитектура «Квадрат» и SP-сеть представляли собой инновационное решение. Сейчас же многие алгоритмы являются AES-подобными и повторяют структуру шифра Rijndael.

Параллельно с конкурсом AES в январе 2000 года начался весьма похожий конкурс в Европе, предполагающий выбор криптостандартов Евросоюза. Этот конкурс назывался NESSIE (New European Schemes for Signature, Integrity and Encryption — «новые европейские алгоритмы электронной подписи, обеспечения целостности и

шифрования») [3]. В результате работы над конкурсом NESSIE учеными-криптографами был написан большой труд под названием «NESSIEsecurityreport»[3], однако европейский стандарт так и не был выбран.

Под влиянием настроений США и Европы в Японии был создан проект CRYPTREC. CRYPTREC – это аббревиатура от Cryptography Research and Evaluation Committee [4]. Проект был создан с целью исследования криптоалгоритмов и последующей рекомендации конкретных алгоритмов для использования в государственных и частных организациях. В результате проекта CRYPTREC был выделен ряд алгоритмов шифрования, рекомендованных к использованию. Для 64-битных шифров были рекомендованы: CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, трехключевой вариант алгоритма Triple DES. Для 128-битных: AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000.

В России стандарт симметричного шифрования ГОСТ 28147-89 был принят в 1989 году. Однако до 1994 года он оставался засекреченным. ГОСТ 28147-89 представляет собой 64-битный блочный шифр, построенный по схеме Фейстеля. Разработчики заложили в шифр избыточную стойкость за счет большого количества раундов шифрования (32 раунда) и наложения секретного ключа с использованием операции сложения по модулю 2^{32}. 1 января 2016 года в России был принят новый стандарт шифрования данных – ГОСТ Р 34.12 – 2015 [6]. В новый стандарт шифрования входят два алгоритма шифрования: Магма и Кузнечик. Магма представляет собой бывший стандарт ГОСТ 28147-89 с одним исключением. В стандарте ГОСТ 28147-89 S-блоки замены не были зафиксированы и могли выбираться произвольным образом. В алгоритме Магма S-блоки регламентированы стандартом. Алгоритм Кузнечик представляет собой 128-битный симметричный блочный шифр, построенный по принципу SP-сети.

Государства, которые раньше составляли СССР, получили в наследство и стандарт шифрования ГОСТ28147-89. В настоящий момент наблюдается тенденция данных государств к развитию собственной государственной системы безопасности, которая в том числе включает и развитие собственных стандартов шифрования данных. Так, в Республике Беларусь был разработан стандарт СТБ 34.101.31-2007 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности» [7]. Сначала в 2007 году стандарт СТБ 34.101.31-2007 был принят в качестве предварительного стандарта в 2007 году. В 2011 году СТБ 34.101.31-2007 был введен в действие в качестве окончательного стандарта. В июле 2015 года стандарт симметричного шифрования был принят в Украине [8]. Стандарт ДСТУ 7624:2014 описывает работу алгоритма шифрования Калина, который является AES-подобным алгоритмом шифрования.

В Республике Казахстан в настоящий момент также ведется работа по созданию государственного стандарта симметричного шифрования данных в рамках проекта программы целевого финансирования «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» от Комитета науки Министерства образования и науки Республики Казахстан (№ гос. регистрации 0118РК01064).Одним из проектных алгоритмов шифрования выступает шифр Qamal, предложенный для исследования в настоящей работе. Подробное описание шифра Qamal можно найти в работе [9].

Основные этапы дифференциального анализа

Прежде чем приступить к дифференциальному анализу алгоритма шифрования KazCrypt, необходимо рассмотреть дифференциальные свойства каждого из его операций по отдельности. Подробное описание метода дифференциального анализа можно найти в работах [10 – 13]. Отметим, что всего можно выделить четыре основных этапа применения метода дифференциального анализа.

Этап 1. Анализ дифференциальных свойств всех составляющих преобразований в алгоритме шифрования.

Этап 2. Поиск наиболее вероятного значения дифференциала, то есть такой пары входная разность – выходная разность, появление которой наиболее вероятно.

Этап 3. Поиск правильных пар текстов. То есть таких текстов, для которых сумма по модулю два на входе в алгоритм шифрования совпадает со входной разностью, а сумма значений на выходе алгоритма шифрования совпадает с выходной разностью.

Этап 4. Анализ правильных пар текстов с целью определения битов секретного ключа.

Основная сложность дифференциального криптоанализа заключается в сложности нахождения правильных пар текстов, которая в свою очередь напрямую зависит от значения вероятности рассматриваемого дифференциала. Именно поэтому нахождение дифференциала, имеющего наибольшую вероятность, имеет первоочередное значение. Зная разность самого вероятного дифференциала, можно прогнозировать насколько успешным будет анализ самого шифра, либо его сокращенной версии. Имеется ввиду определение количества раундов шифра, для которых еще возможно применение дифференциального криптоанализа.

Дифференциальные свойства операции сложения по модулю 2

В дифференциальном криптоанализе преобразуемые тексты рассматриваются не по отдельности, а совместно. Вернее рассматривается их разность, которая определяется как результат сложения этих текстов по модулю два: $\Delta X = X \oplus X1$.

В этом случае значение разности ΔX будет содержать нули в тех позициях, в которых исходные сообщения были равны и единицы там, где биты различались.

Известно, что операция сложения данных с секретным ключом не влияет на изменение разности текстов. Это связано с тем, что при шифровании используется один и тот же секретный ключ шифрования. Таким образом, тексты будут складываться с одним и тем же значением К, которые в свою очередь сложившись друг с другом образуют значение равное нулю: $\Delta X = X \oplus K_i \oplus X1 \oplus K_i = X \oplus X1$.

Дифференциальные свойства операции замены битов с использованием S-блока

Так как S-блок шифра меняет 8 битов на 8 битов, то возможный диапазон входных разностей совпадает с диапазоном выходных разностей и находится в пределах от 0 до 255. Мы построили таблицу зависимости выходных разностей ΔC S-блока от значения входной разности ΔA и выявили следующие свойства:

Свойство 1. Значение $\Delta C = 0$ на выходе преобразования может быть получено только в том случае, когда $\Delta A = 0$. В этом случае вероятность появления разности на выходе равна 1.

Свойство 2. В построенной таблице анализа максимальным значением вероятности является значение 6/256 = 3/128.

Свойство 3. Существуют значения входных разностей ΔA, которые после прохождения через S-блок замены остаются неизменными. Это, например, такие значения (в 10-ной форме) как ΔA = 2, 3, 4, 6, 15, 16, 17, 18 и другие.

Свойство 4. Значение входной разности ΔA= 254 (ΔA = 0xfe) преобразуется в значение разности ΔC = 128 (ΔC = 0x80) с вероятностью p=4/256 = 1/64.

Дифференциальные свойства преобразования Mixer1

Несмотря на то, что преобразование Mixer1 является линейным преобразованием, необходимо определить как будут изменяться значения разностей при применении операции сложения по модулю 256. Известно, что при выполнении операции сложения по модулю 2^n разность остается неизменной с вероятностью p=1 только в том случае, если входная разность содержит всего один ненулевой бит в самом старшем разряде. Таким образом, если в преобразовании Mixer1 будет задействовано значение разности, равное 0x80, то какие бы преобразования мы с ним ни делали, вероятность всегда будет оставаться равной 1. Преобразование Mixer1 зависит от четырех байтов одного столбца. Поэтому важно рассмотреть, как будут меняться выходные значения. При этом с точки зрения дифференциального криптоанализа нас интересуют те варианты, которые затрагивают наименьшее количество активных байтов. Так как в операции Mixer1 сложение выполняется по модулю 256, то значение разности0x80 всегда будет оставаться неизменным. Так, сложение двух одинаковых разностей 0x80 и 0x80 по модулю 256 (0x100) будет приводить к нулю. Таким образом, мы можем рассмотреть 15 вариантов заполнения исходного столбца преобразования Mixer1, где значения байтов могут быть равны только 0x00 или 0x80. Пример одного такого преобразования приведен в таблице 1.

Таблица 1 – Результат преобразования разностей в преобразовании Mixer1. Вариант 1

Исходное состояние	Первое изменение	Второе изменение	Третье изменение	Четвертое изменение
0x80	0x80	0	0	0
0	0x80	0x80	0	0
0	0	0x80	0x80	0
0	0	0	0x80	0x80

Дифференциальные свойства преобразования Mixer2

Преобразование Mixer2 является линейным преобразованием. Оно не оказывает влияния на изменение вероятности преобразования разности. Однако для построения многораундовых характеристик важно определить, как именно будет преобразовано значение строк, содержащих в одном из байтов значение 0x80, которое будет получено после преобразования Mixer1. При этом важно помнить, что каждая строка использует свой полином m для умножения. В каждой строке содержится 4 байта. Если учесть, что каждый байт может содержать или значение разности, равное 0, или значение разности, равное 0x80, то всего получается 15 возможных заполнений для каждой строки от 0x00000080 до 0x80808080. Рассмотрим, как будут преобразованы данные разности с использованием полиномов m (для версии блока в 128 битов получается всего 60 вариантов: 15 вариантов заполнения и 4 полинома m). Нас интересуют те случаи, когда байты на выходе преобразования Mixer 2 после прохождения через блок замены S могут

быть преобразованы к значениям 0x80. То есть в таблице зависимостей ΔA и ΔC на пересечении ΔA, образованного из байта выхода преобразования Mixer2, и ΔC=0x80, должно стоять значение, отличное от 0. Мы разработали программу, с помощью которой просчитали все возможные вариант.

В результате применения данной программы было выявлено, что из 60 рассмотренных комбинаций заданному условию удовлетворяет всего одно значение. Входная разность, равная 0x80808000 преобразуется к разности 0xbbc868cf и после прохождения через S-блок замены может быть преобразована к значению разности 0x80808080. Именно эту комбинацию мы будем в дальнейшем использовать для построения многораундовых характеристик.

Построение многораундовых характеристик

Опираясь на дифференциальные свойства основных операций шифра Qamal, построим многораундовую характеристику и определим ее вероятность. Наша задача построить характеристику так, чтобы было затронуто как можно меньше активных S-блоков. От этого напрямую зависит вероятность нахождения правильной пары текстов по заданной характеристики. Наша задача определить какое количество раундов для шифра Qamal может быть проанализировано быстрее, чем методом полного перебора. Для блока данных в 128 битов используется секретный ключ длиной 128 битов, а значит сложность полного перебора составляет 2^{128}.

Рассмотрим первый раунд шифрования. Операцию сложения с раундовым подключом мы опускаем, так как она не влияет на изменение разности текстов. Нам необходимо, чтобы на входе преобразования Mixer1 появилось значение байтов 0x80. В соответствии со свойством 4 из подраздела 4.3, значение 0xfe будет преобразовано в значение 0x80 с вероятностью $4/256=1/64=2^{-6}$. При этом мы должны сформировать вход первого раунда таким образом, чтобы после преобразования Mixer1 ненулевая разность оказалась в третьей строке массива состояния. Если входная разность будет затрагивать первый и четвертый байты для первых трех столбцов состояния, то после S-блоков замены все ненулевые байты преобразуются в байты 0x80 с вероятностью $(2^{-6})^6 = 2^{-36}$. Можно видеть, что уже с первого раунда шифрования вероятность получения раундовой характеристики достаточно мала. Преобразование Mixer1 изменит массив состояния, не влияя на общую вероятность. В результате ненулевые байты окажутся только в первых трех позициях третьей строк. Все остальные значения будут нулевыми. Подробно схема преобразования для первого раунда представлена в таблице 2.

Таблица 2. Преобразование разности для первого раунда шифра Qamal

Вход первого раунда				Вход преобразования Mixer 1				Вход преобразования Mixer 2			
0xfe	0xfe	0xfe	0	0x80	0x80	0x80	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0
0xfe	0xfe	0xfe	0	0x80	0x80	0x80	0	0	0	0	0

Выше было показано, что, если на вход третьей строки в преобразовании Mixer2 поступает значение 0x80808000, то на выходе будет получено значение 0xbbc868cf. При этом каждый байт разности 0xbbc868cf может быть преобразован к байту 0x80. Вероятность того, что все четыре байта будут преобразованы в значения 0x80 составит

$(2^{-7})^4 = 2^{-28}$. Таким образом, итоговая вероятность для двух раундов шифрования составит 2^{-64}. После функции Mixer1 будут заполнены вторая и четвертая строки байтами 0x80,как это показано в таблице 3.

Таблица 3. Преобразование разности для второго раунда шифра Qamal

Вход в S-блок				Вход в преобразование Mixer1				Вход в преобразование Mixer2			
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0x80
0xbb	0xc8	0x68	0xcf	0x80	0x80	0x80	0x80	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0x80

В результате анализа дифференциальных свойств преобразования Mixer2, было выявлено, что для второй и четвертой строки входная разность 0x80808080 не может быть преобразована таким образом, чтобы в следующем раунде после S-преобразования образовать все байты разности равные 0x80. Поэтому мы рассмотрели другие варианты преобразований. На вход S-блока третьего раунда поступят вторая и четвертая строки состояния, содержащие значение разности 0x95d14821, полученные после преобразования Mixer2 (таблица 4). В соответствии с таблицей дифференциальных свойств, мы определили, что байт 0x95 может быть заменен на байт 0x80. Для остальных байтов был подобран вариант замены, которые после преобразования Mixer1 затронет три ненулевые байта столбца (из четырех). Байт 0xd1 в соответствии с таблицей анализа имеет шансы быть преобразованным в байт 0x40 и в байт 0xc0. В этом случае преобразование Mixer1 будет выполнено в соответствии с таблицей 5. Байты 0x48 и 0x21 не могут быть преобразованы также, как байт 0xd1.Поэтому для них было выявлено, что они имеют возможность преобразования в байты 0x10 и 0xf0. В этом случае преобразование Mixer1 будет выполнено в соответствии с таблицей 6.

Таблица 4. Преобразование разности для третьего раунда шифра Qamal

Вход в S-блок				Вход в преобразование Mixer1				Вход в преобразование Mixer2			
0	0	0	0	0	0	0	0	0x80	0xc0	0x30	0x30
0x95	0xd1	0x48	0x21	0x80	0x40	0x10	0x10	0	0x80	0x20	0x20
0	0	0	0	0	0	0	0	0x80	0x40	0x10	0x10
0x95	0xd1	0x48	0x21	0x80	0xc0	0x1f	0x1f	0	0	0	0

Таблица 5. Преобразование Mixer1 для байтов 0x40 и 0xc0

Входные разности	Первый шаг преобразования	Второй шаг преобразования	Третий шаг преобразования	Выходная разность
0x00	0x00	0x40	0x80	0xc0
0x40	0x00	0x00	0x40	0x80
0x00	0x40	0x00	0x00	0x40
0xc0	0x00	0x40	0x00	0x00

Таблица 6. Преобразование Mixer1 для байтов 0x10 и 0xf0

Входные разности	Первый шаг преобразования	Второй шаг преобразования	Третий шаг преобразования	Выходная разность
0x00	0x00	0x10	0x20	0x30

0x10	0x00	0x00	0x10	0x20
0x00	0x10	0x00	0x00	0x10
0xf0	0x00	0x10	0x00	0x00

Вероятности преобразования каждого байта по S-блоку замены для третьего раунда составляет 2^{-7}. Всего в третьем раунде используется 8 ненулевых блоков. Таким образом, вероятность преобразования в третьем раунде равна $(2^{-7})^8 = 2^{-56}$. Получается, что вероятность для трех раундов шифра будет равна 2^{-120}, что очень близко к значению вероятности полного перебора. Поэтому дальше рассматривать преобразование разности смысла не имеет. Нам необходимо определить значение разности на выходе третьего раунда шифрования. Для этого рассмотрим разности на входе в преобразование Mixer2 третьего раунда. Применив к нему преобразования Mixer1 и Mixer2, получим состояние разностей как показано в таблице 7.

Таблица 7 – Состояние разностей после третьего раунда шифрования

0x4c	0x6b	0x94	0xea
0xad	0xde	0x47	0x5b
0xe1	0xb2	0xd3	0xb1
0x00	0x00	0x00	0x00

Заключение

Нами рассмотрен проектный алгоритм симметричного шифрования Qamal, который рассматривается в качестве претендента на стандарт шифрования данных в Республике Казахстан. Показано, что для версии шифра со 128-битным блоком данных и секретным ключом такой же длины дифференциальный криптоанализ становится неприменимым после трех раундов шифрования. Для полной проверки надежности шифра предстоит еще его тщательное исследование с использованием других криптоаналитических атак.

Работа выполнена в рамках программы целевого финансирования BR05236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» Министерства образования и науки Республики Казахстан.

Литература

1. History of DES. - http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/des%20history.html
2. Bruce Shnier Applied Cryptography: Protocols, Algorithms, and Source Code in C. - 1996. - John Wiley & Sons. - 784 P.
3. Панасенко С.П. Конкурсы AES и NESSIE [Электронный ресурс] - https://www.osp.ru/pcworld/2004/12/169401/
4. Specifications of e-Government Recommended Ciphers // https://www.cryptrec.go.jp/en/method.html
5. GOST 28147-89: Encryption, Decryption and Message Authentication Code (MAC) Algorithms // https://tools.ietf.org/html/rfc5830
6. GOST R 34.12–2015 «Information technology. Cryptographic data security. Block ciphers» // https://tc26.ru/en/standards/standards/gost-r/gost-r-34-12-2015-information-technology-cryptographic-data-security-block-ciphers.html

7. Fault-based Attacks on the Bel-T Block Cipher Family // https://zerobyte.io/publications/2015-JP-belt.pdf
8. A New Encryption Standard of Ukraine: The Kalyna Block Cipher - https://pdfs.semanticscholar.org/7771/8fbf6c2044b6f1aa2e66a1eda99121caa4da.pdf
9. Kunbolat Algazy, Ludmila Babenko, Rustem Biyashev, Evgeniya Ishchukova, Nursulu Kapalova, Saule Nyssanbayeva Investigation of the Different Implementations for the New Cipher Qamal // SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks Article No. 8. Sochi, Russia — September 12 - 15, 2019 - doi>10.1145/3357613.3357622
10. E. Biham, A. Shamir: "DifferentialCryptanalysisoftheFull 16-roundDES", Crypto'92, Springer-Velgar, 1998, p.487
11. E. Biham, A. Shamir: "Differential Cryptanalysis of DES-like Cryptosystems", Extended Abstract, Crypto'90, Springer-Velgar, 1998, p.21
12. E.A. Ishchukova, E.A. Tolomanenko, L.K. Babenko Differential analysis of 3 round Kuznyechik // Proceedings of the 10th international conference on Security of information and networks (SIN 2017), ACM, New York, NY, USA.
13. Бабенко Л.К. Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа // Москва, «Гелиос АРВ», 2006 г. – 376 с.

О МОДЕЛИ РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Бегимбаева Е.Е.
e-mail: enlik_89@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Обнаружение конфликтов при информационном взаимодействии возможно только при наличии адекватной модели, которая описывает автоматизированную систему и элементы с потенциально конфликтным взаимодействием. В статье рассмотрен модуль разрешения конфликтных ситуаций в автоматизированной системе защищенного информационного взаимодействия. Приведены недостатки обеспечения бесконфликтного взаимодействия.*

В настоящее время происходит активный процесс информатизации всех сфер деятельности общества и государства. Она направлена, на активное внедрение компьютерной техники и новых информационных технологий в различные сферы, на эффективное формирование и использование национальных информационных ресурсов. При автоматизации информационного взаимодействия важным является обеспечение информационной безопасности. В связи с этим задачи обеспечения защиты информации в автоматизированной системе информационного взаимодействия (АСИВ) выходят на передний план. Для решения этих задач разрабатывается комплекс

программ, который состоит из модулей обеспечивающие конфиденциальность информации и защиту данных от несанкционированного доступа.

Вопросам построения систем защиты информации и комплексных систем информационной безопасности посвящено множество работ зарубежных специалистов: D. Ullman, Michael A. Harrison, П.Д. Зегжды [1], А.А. Молдовяна, М.А.Поляничко [2] и других.

В соответствии с [1] информация в автоматизированной системе информационного взаимодействия находится в безопасности, если все компоненты этой системы защищены от возможных угроз на требуемом уровне. Автоматизированные системы, обеспечивающие безопасность, информации, называются защищенными.

АСИВ включает в себя такие составляющие, как [3]:

- модуль шифрования;
- модуль цифровой подписи;
- модуль разграничения доступа;
- модуль разрешения конфликтных ситуаций (РКС) [4].

Независимо от формы представления электронной информации, в автоматизированной системе могут возникать различные конфликтные ситуации. Обеспечение бесконфликтного взаимодействия является важной задачей для обеспечения комплексной безопасности системы. В число таких задач входят исследование информационных объектов АСИВ и анализ уровня защищенности передаваемой информации в случайных и преднамеренных конфликтах [2].

Недостатками существующих методов, процедур и инструментальных средств обеспечения бесконфликтного взаимодействия программных средств защиты информации являются [2]:

- отсутствие инструментальных средств, направленных на обнаружение конфликтов, специфичных для автоматизированной системы информационного взаимодействия;
- малая детализация информации об обнаруженных конфликтах;
- большая сложность поиска и анализа конфликтов в АСИВ.

Таким образом, задача разработки модуля разрешения конфликтных ситуаций и автоматизация является актуальной.

Обнаружение конфликтов при информационном взаимодействии возможно только при наличии адекватной модели, которая описывает автоматизированную систему и элементы с потенциально конфликтным взаимодействием.

Рассмотрим построение модели разрешения конфликтных ситуаций. Пусть $func$ – функция вызываемая из модуля РКС. Во множестве (1) содержаться данные об имени функции, ее параметрах и возвращаемом значении.

$$func = \{name, p_1 \dots, p_n, rt\}, \quad (1)$$

где $name$ – имя функции, $p_1 \dots, p_n$ – параметры поступающие на вход функции, rt-тип возвращаемого значения.

Множество $func$ учитывает все необходимые данные для выявления конфликта между вызываемым и вызывающим объектом. Все возможные возвращаемые значения содержатся в отдельном множестве. Каждый параметр представляет собой множество p.

Для описания параметров, используется отдельное множество, содержащее информацию об имени и типе параметра. Каждый параметр, передаваемый на вход функции, задается множеством:

$$P = \{name, t\}, \quad (2)$$

где *name* - имя параметра, *t* - тип параметра.

Все допустимые типы данных, которые могут быть переданы на вход функции, содержаться во множестве:

$$\mathrm{T} = \{t_1 \dots, t_n\}, \quad (3)$$

где *t* - название типа.

Конфликты в АСИВ можно условно поделить на конфликты, связанные с ЭЦП, шифрованием; связанные с технической составляющей и программными средствами. Каждая конфликтная ситуация при информационном взаимодействии электронными документами является уникальной.

Литература

1. Зегжда Д.П. и др. Теория и практика обеспечения информационной безопасности. — М.: Яхтсмен, 1996.

2. Поляничко М.А. Модель обнаружения конфликтов программных средств защиты информации на основе анализа зависимостей динамических библиотек // Естественные и технические науки. – М.: Спутник+,2012. – Вып. 6 (62). – С. 524 – 526.

3. Бияшев Р.Г., Бегимбаева Е.Е., Рог О.А. Разработка автоматизированной системы защиты информации в процессе трансграничного обмена // матер. науч. конф. «Современные проблемы информатики и вычислительных технологий». – Алматы: ИИВТ МОН РК, 2019. – С. 148-154.

4. Rustem Biyashev, Saule Nyssanbayeva and Yenlik Begimbayeva Development and Analysis of Possible Conflict Situations Resolution Systems in an Automated System // Proceeding of International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019), Guilin, China, 2019. - Vol. 89 – 182-184 p.

ИССЛЕДОВАНИЕ РАЗРАБОТАННЫХ АЛГОРИТМОВ ПО КРИТЕРИЮ «ЛАВИННОГО ЭФФЕКТА»

Бияшев Р.Г., Алгазы К.Т., Хомпыш А.

e-mail: brg@ipic.kz, kunbolat@mail.ru, ardabek@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В работе приведены результаты исследования* «лавинного эффекта» *разработанных алгоритмов AL01, Qamal и BC-2. При проектировании алгоритма шифрования необходимо, чтобы шифр удовлетворял лавинному критерию. Если алгоритм не обеспечивается лавинным эффектом в необходимой степени, то криптоаналитик может сделать вывод о входных данных, основываясь на выходных. Рассматриваемые алгоритмы удовлетворяет требование* «лавинного эффекта».

Введение

Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней. Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы; криптосистемы с открытым ключом; электронная подпись; управление ключами. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

Симметричные блочные алгоритмы шифрования, в настоящее время, являются основным криптографическим средством обеспечения конфиденциальности при обработке информации в современных информационно-телекоммуникационных системах. Современные шифры базируются на принципе Керкгоффса [1,2], согласно которому секретность шифра обеспечивается секретностью ключа, а не секретностью алгоритма шифрования. В большинстве блочных алгоритмов симметричного шифрования используются следующие типы операций: табличная подстановка, при которой группа битов отображается в другую группу битов (S-box); перемещение, с помощью которого биты сообщения переупорядочиваются; операция сложения по модулю 2, обозначаемая XOR; циклический сдвиг на некоторое число битов.

К современным алгоритмам блочного шифрования предъявляют достаточно жесткие требования, связанные с областью применения, возможностью реализации на различных вычислительных платформах и другими факторами. Основные из требований:

1. Алгоритм должен обеспечивать высокий уровень стойкости, и эта стойкость не должна основываться на сохранении втайне самого алгоритма.
2. Незначительное изменение исходного сообщения должно приводить к существенному изменению зашифрованного сообщения даже при использовании одного и того же ключа.
3. Алгоритм должен успешно противостоять атакам по выбранному тексту, то есть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.
4. Алгоритм должен эффективно реализовываться на специализированной аппаратуре, предназначенной для выполнения операций шифрования и расшифрования, то есть реализация алгоритма в виде электронных устройств должна быть экономичной.
5. Не должно быть "слабых" ключей, облегчающих криптоанализ.
6. Алгоритм должен легко модифицироваться для различных уровней безопасности и удовлетворять как минимальным, так и максимальным требованиям и другие.

При разработке алгоритмов шифрования обязательно проведение их анализа на стойкость к различным видам криптоатак. Одними из наиболее распространенных в настоящее время стандартных методов являются атаки на основе линейного и дифференциального криптоанализа [3]. Суть последнего состоит в отслеживании изменения разности между значениями выходных бит в зависимости от изменения входных бит (в исходных данных) на различных раундах преобразования. Необходимое

условие обеспечения стойкости алгоритма шифрования к дифференциальному криптоанализу – наличие лавинного эффекта в базовом преобразовании.

Если шифр оперирует информацией, представленной в двоичной форме, то инвертирование даже одного бита в блоке исходных данных приведет к тому, что все биты в соответствующем блоке зашифрованных данных с вероятностью $\frac{1}{2}$ независимо друг от друга также поменяют свое значение. Такой шифр невозможно вскрыть способом, менее затратным с точки зрения количества необходимых операций, чем полный перебор по множеству возможных значений ключа. Данное условие является обязательным для шифра рассматриваемого типа, претендующего на то, чтобы считаться хорошим [4].

1. Результаты проверки «лавинного эффекта» алгоритма «AL01»

Алгоритм шифрования «AL01» относится к классу симметричных блочных алгоритмов. В данном алгоритме длины блока шифрования и базового ключа одинаковы и равны к 16 байт (или 128 битам). Количество раундов шифрования – 4. В алгоритме выполняются всего две операции: побитовое сложение *XOR* и подстановка байтов через S блок замены. Схема шифрования алгоритма AL01 приведен на рисунке 1.

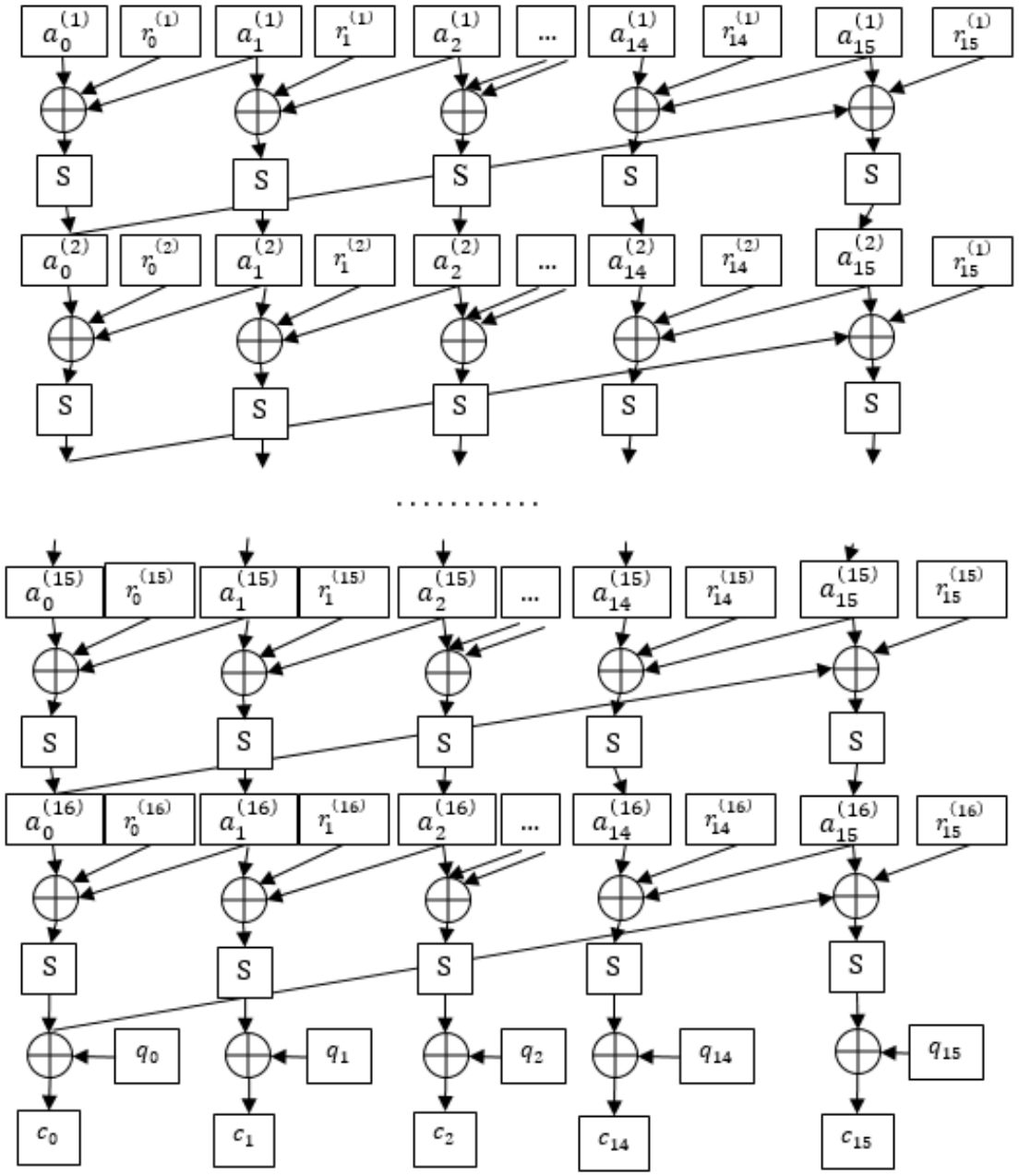


Рисунок 1 – Схема алгоритма шифрования AL01

Лавинный эффект – важное криптографическое свойство для шифрования. Оно означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к лавинному изменению значений выходных битов шифртекста. Исследование лавинного эффекта, обычно применяется к блочным шифрам и криптографическим хеш-функциям. Для характеристики степени лавинного эффекта в криптографическом преобразовании определяется и используется лавинный параметр – численное значение отклонения вероятности изменения бита в выходной последовательности при изменении бита во входной последовательности от требуемого значения вероятности, равной 0,5 [5].

Если малые изменения в открытом тексте приводят к малым изменениям в зашифрованном тексте, то это позволяет злоумышленнику сузить пространство ключей или область поиска открытого текста [2,6].

Для лавинного критерия значение лавинного параметра определяется формулой

$$\varepsilon = |2k_i - 1|, \quad (1)$$

где i – номер изменяемого бита во входном значении, k_i – вероятность изменения половины битов в выходном значении при изменении i -го бита во входном значении по сравнению с выходным значением при исходном (неизмененном) входном значении.

Далее приводятся результаты проверки лавинного эффекта алгоритма шифрования «AL01». Алгоритм шифрования состоится из 16 шагов (или рядов, как указано в описании). На каждом шаге рассматриваемый байт суммируется с соседним правым байтом и элементом ключа по операции *XOR*. Далее полученный байт проходит через S блок. Этот процесс повторяется 16 раз.

Если рассмотреть пару открытых текстов, отличающихся между собой только на 1 бит, то соответствующие их шифртексты полностью будут отличаться только после выполнений последнего 16-го шага. Покажем, как меняются разности соответствующих шифртекстов в каждом ряду в случае, когда их открытые тексты отличаются только в последнем бите:

1 ряд	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 xx
2 ряд	00 00 00 00 00 00 00 00 00 00 00 00 00 00 xx xx
3 ряд	00 00 00 00 00 00 00 00 00 00 00 00 00 xx xx xx
4 ряд	00 00 00 00 00 00 00 00 00 00 00 00 xx xx xx xx
5 ряд	00 00 00 00 00 00 00 00 00 00 00 xx xx xx xx xx
6 ряд	00 00 00 00 00 00 00 00 00 00 xx xx xx xx xx xx
7 ряд	00 00 00 00 00 00 00 00 00 xx xx xx xx xx xx xx
8 ряд	00 00 00 00 00 00 00 00 xx xx xx xx xx xx xx xx
9 ряд	00 00 00 00 00 00 00 xx xx xx xx xx xx xx xx xx
10 ряд	00 00 00 00 00 00 xx xx xx xx xx xx xx xx xx xx
11 ряд	00 00 00 00 00 xx xx xx xx xx xx xx xx xx xx xx
12 ряд	00 00 00 00 xx xx xx xx xx xx xx xx xx xx xx xx
13 ряд	00 00 00 xx xx xx xx xx xx xx xx xx xx xx xx xx
14 ряд	00 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx
15 ряд	00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
16 ряд	xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

В практических примерах алгоритм был проверен на лавинный эффект. Для проверки выбрали случайный открытый текст длиной 128 бит. Произведя инверсию битов в каждой позиции получили новый 128 новых открытых текстов и зашифровали их. Вычислили вероятности k_i между полученными шифртекстами и исходным шифртекстом.

Из формулы видно, что экстремальность ε может принимать значения от 0 до 1 включительно. Чем ближе значение ε к нулю, тем более «хорошим» является алгоритм. И наоборот, чем значение ближе ε к 1, тем более «плохим» является алгоритм.

Действительно, если ε мало, то это значит, что при изменении всего одного бита в исходных данных в выходных данных изменится примерно половина бит. При этом

номера этих бит образуют случайную последовательность. А это значит, что инвертирование даже одного бита в блоке исходных данных приведет к тому, что все биты в соответствующем блоке зашифрованных данных с вероятностью близкой к 1/2 независимо друг от друга так же поменяют свои значения. Если значение ε близко к 1, то малые изменения исходных данных приводят к малым изменениям в выходных данных, что позволит злоумышленнику сузить пространство ключей или область поиска открытого текста [2]. Результаты анализа по открытому тексту вышесказанного алгоритма показано в таблице 1.

Таблица 1 – Анализ лавинного эффекта по открытому тексту алгоритма AL01

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	I	k_i	i	k_i	i	k_i
1	0,51	17	0,48	33	0,55	49	0,54	65	0,50	81	0,59	97	0,45	113	0,52
2	0,41	18	0,43	34	0,49	50	0,46	66	0,48	82	0,45	98	0,59	114	0,61
3	0,47	19	0,48	35	0,50	51	0,56	67	0,56	83	0,50	99	0,48	115	0,48
4	0,59	20	0,48	36	0,47	52	0,52	68	0,52	84	0,46	100	0,49	116	0,52
5	0,46	21	0,51	37	0,43	53	0,47	69	0,51	85	0,52	101	0,54	117	0,53
6	0,59	22	0,50	38	0,49	54	0,47	70	0,48	86	0,54	102	0,45	118	0,53
7	0,52	23	0,59	39	0,51	55	0,54	71	0,55	87	0,45	103	0,45	119	0,55
8	0,43	24	0,55	40	0,53	56	0,55	72	0,57	88	0,44	104	0,44	120	0,48
9	0,49	25	0,52	41	0,48	57	0,54	73	0,41	89	0,53	105	0,56	121	0,51
10	0,45	26	0,55	42	0,45	58	0,50	74	0,54	90	0,51	106	0,47	122	0,48
11	0,50	27	0,53	43	0,53	59	0,51	75	0,48	91	0,55	107	0,51	123	0,51
12	0,50	28	0,52	44	0,47	60	0,51	76	0,50	92	0,55	108	0,48	124	0,44
13	0,54	29	0,47	45	0,66	61	0,51	77	0,51	93	0,50	109	0,49	125	0,51
14	0,44	30	0,49	46	0,53	62	0,47	78	0,47	94	0,40	110	0,52	126	0,52
15	0,51	31	0,51	47	0,53	63	0,56	79	0,55	95	0,61	111	0,52	127	0,41
16	0,46	32	0,47	48	0,46	64	0,49	80	0,45	96	0,45	112	0,48	128	0,48

Аналогичным образом может быть определен лавинный критерий для оценки лавинного эффекта по ключу (при изменении одного бита ключевой последовательности изменяется в среднем половина выходных битов). Результаты приведены в таблице 2.

Таблица 2 – Анализ лавинного эффекта по ключу алгоритма AL01

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,44	17	0,51	33	0,48	49	0,47	65	0,51	81	0,55	97	0,53	113	0,56
2	0,54	18	0,44	34	0,51	50	0,54	66	0,53	82	0,44	98	0,46	114	0,54
3	0,44	19	0,42	35	0,49	51	0,44	67	0,42	83	0,46	99	0,41	115	0,52
4	0,58	20	0,5	36	0,5	52	0,51	68	0,43	84	0,48	100	0,51	116	0,52
5	0,52	21	0,42	37	0,52	53	0,46	69	0,49	85	0,48	101	0,54	117	0,51
6	0,54	22	0,49	38	0,52	54	0,48	70	0,52	86	0,55	102	0,48	118	0,55
7	0,55	23	0,45	39	0,51	55	0,53	71	0,54	87	0,53	103	0,49	119	0,40
8	0,51	24	0,51	40	0,41	56	0,37	72	0,44	88	0,55	104	0,51	120	0,45
9	0,46	25	0,51	41	0,51	57	0,56	73	0,48	89	0,44	105	0,47	121	0,45
10	0,56	26	0,52	42	0,5	58	0,48	74	0,54	90	0,54	106	0,57	122	0,55
11	0,48	27	0,51	43	0,51	59	0,48	75	0,51	91	0,46	107	0,49	123	0,54
12	0,58	28	0,52	44	0,49	60	0,51	76	0,46	92	0,40	108	0,5	124	0,53
13	0,55	29	0,55	45	0,48	61	0,55	77	0,45	93	0,51	109	0,47	125	0,55

14	0,55	30	0,43	46	0,55	62	0,48	78	0,54	94	0,62	110	0,45	126	0,46
15	0,45	31	0,45	47	0,52	63	0,48	79	0,49	95	0,44	111	0,48	127	0,52
16	0,55	32	0,55	48	0,49	64	0,45	80	0,47	96	0,45	112	0,48	128	0,44

Значения Хи-квадрат последовательности из значений таблиц 1 и 2 соответственно равны 66,42 и 67,75. Если учитывать, что степень свободы равны 127, то можно сказать, что полученные результаты являеюся положительными. Среднее значение ε в обоих случаях равно 0,07. Чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании. Алгоритм AL01 удовлетворяет требованиям лавинного критерия.

2. Результаты проверки лавинного эффекта алгоритма «Qamal»

Структурная схема разработанного алгоритма зашифрования приведена на рисунке 2. Алгоритм поддерживает длины блока и ключей в 128, 192 и 256 бит. От длины блока и ключа зависит число раундов шифрования. Ключам *K* длиной в 128, 192 и 256 бит соответствуют числа раундов шифрования 8, 10 и 12. Все раунды завершаются операцией сложения по модулю 2 с раундовым ключом.

Алгоритм зашифрования включает разработанные процедуры наложения ключа с помощью операции побитового сложения (*XOR*), *S*-блока замены, процедур перемешивания Mixer1 и Mixer2.

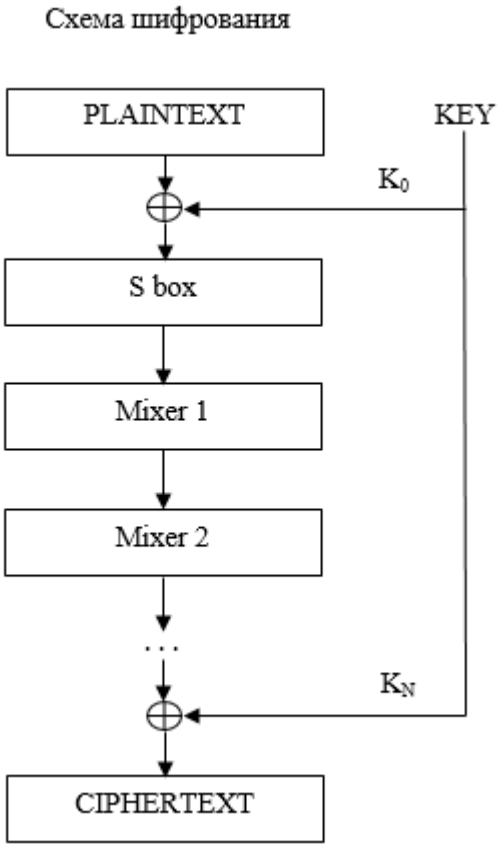


Рисунок 2 – Схема алгоритма зашифрования «Qamal»

Рассмотрим пример того, как данные преобразования, используемые в алгоритме, влияют на лавинный эффект.

В качестве входа берем два откытых текста, отличающихся друг от друга только на один бит. Для их зашифрования используется один и тот же ключ. Выясняем, как распространяется данное изменение в одном раунде.

Отк. текст 1(T_1)	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Отк. текст 2(T_2)	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Ключ	CD	BF	03	36	9E	AD	5E	F3	E9	8F	2F	2F	DF	8A	B4	B1
$T_1 \oplus K$	CD	BF	03	36	9E	AD	5E	F3	E9	8F	2F	2F	DF	8A	B4	B1
$T_2 \oplus K$	CC	BF	03	36	9E	AD	5E	F3	E9	8F	2F	2F	DF	8A	B4	B1
$S(T_1 \oplus K)$	7C	CB	18	75	57	22	0A	F5	0D	16	C1	C1	D7	92	41	FE
$S(T_2 \oplus K)$	11	CB	18	75	57	22	0A	F5	0D	16	C1	C1	D7	92	41	FE
$M_1\ S(T_1 \oplus K)$	EB	12	90	D9	21	1A	4D	E7	97	98	07	54	B7	95	24	29
$M_1\ S(T_2 \oplus K)$	93	12	90	D9	75	1A	4D	E7	C1	98	07	54	4C	95	24	29
$M_2\ M_1\ S(T_1 \oplus K)$	B8	55	8B	3E	22	C3	50	38	3B	B3	81	5B	6E	AA	A2	B1
$M_2\ M_1\ S(T_2 \oplus K)$	40	F9	93	A8	16	3D	55	C0	81	37	E4	C5	3C	7B	76	06

Первый выбранный открытый текст в двоичном представлении состоит только из нулей. Второй открытый текст также состоит из нулей, за исключением восьмого бита. Операция побитового сложения (*xor*) не влияет на распростронение изменений. Изменение одного бита в S-блоке замены распространяется только на один байт, а в операции *Mixer1* – на каждый четвертый байт. После вышеуказанных операций выполняется операция *Mixer2,* в результате которой изменение распространяется на весь шифртекст. Конкретные числовые характеристики приведены ниже.

Проверка данного алгоритма к лавинному эффекту производилась по такому же порядку как было проведено в алгоритме AL01. В работе приведены результаты анализа для одноараундового и полнораундового алгоритма в таблицах 3 и 4. Среднее значение ε для каждого из них равно 0,07 и 0,062, соответственно. Чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании.

Таблица 3 – Анализ лавинного эффекта алгоритма Qamal после первого раунда

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,48	17	0,40	33	0,40	49	0,55	65	0,47	81	0,53	97	0,51	113	0,44
2	0,46	18	0,51	34	0,45	50	0,46	66	0,44	82	0,48	98	0,49	114	0,52
3	0,50	19	0,51	35	0,47	51	0,49	67	0,46	83	0,51	99	0,44	115	0,55
4	0,53	20	0,43	36	0,48	52	0,51	68	0,45	84	0,50	100	0,55	116	0,55
5	0,62	21	0,42	37	0,49	53	0,48	69	0,45	85	0,45	101	0,55	117	0,52
6	0,48	22	0,45	38	0,53	54	0,48	70	0,48	86	0,53	102	0,41	118	0,47
7	0,48	23	0,45	39	0,44	55	0,44	71	0,50	87	0,41	103	0,47	119	0,52
8	0,47	24	0,58	40	0,46	56	0,47	72	0,56	88	0,54	104	0,48	120	0,42
9	0,46	25	0,47	41	0,57	57	0,52	73	0,46	89	0,50	105	0,49	121	0,49
10	0,48	26	0,52	42	0,50	58	0,50	74	0,57	90	0,47	106	0,52	122	0,50
11	0,55	27	0,45	43	0,46	59	0,53	75	0,44	91	0,54	107	0,57	123	0,45
12	0,44	28	0,52	44	0,55	60	0,51	76	0,49	92	0,51	108	0,48	124	0,49
13	0,48	29	0,54	45	0,49	61	0,63	77	0,49	93	0,52	109	0,57	125	0,49
14	0,44	30	0,52	46	0,52	62	0,51	78	0,48	94	0,51	110	0,44	126	0,53

15	0,55	31	0,52	47	0,48	63	0,54	79	0,48	95	0,53	111	0,51	127	0,59
16	0,52	32	0,51	48	0,56	64	0,48	80	0,47	96	0,48	112	0,45	128	0,54

Таблица 4 – Анализ лавинного эффекта алгоритма Qamal после восьмого раунда

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,48	17	0,47	33	0,50	49	0,52	65	0,46	81	0,45	97	0,52	113	0,54
2	0,52	18	0,49	34	0,54	50	0,52	66	0,50	82	0,52	98	0,54	114	0,57
3	0,43	19	0,49	35	0,48	51	0,48	67	0,51	83	0,55	99	0,46	115	0,58
4	0,48	20	0,53	36	0,52	52	0,49	68	0,51	84	0,53	100	0,41	116	0,50
5	0,44	21	0,56	37	0,44	53	0,50	69	0,42	85	0,52	101	0,54	117	0,50
6	0,48	22	0,48	38	0,49	54	0,54	70	0,46	86	0,45	102	0,46	118	0,45
7	0,48	23	0,51	39	0,50	55	0,48	71	0,50	87	0,56	103	0,51	119	0,55
8	0,50	24	0,50	40	0,56	56	0,47	72	0,41	88	0,53	104	0,52	120	0,58
9	0,49	25	0,55	41	0,48	57	0,47	73	0,52	89	0,52	105	0,56	121	0,45
10	0,48	26	0,51	42	0,48	58	0,48	74	0,50	90	0,46	106	0,55	122	0,46
11	0,52	27	0,50	43	0,48	59	0,47	75	0,45	91	0,54	107	0,51	123	0,43
12	0,45	28	0,49	44	0,55	60	0,55	76	0,41	92	0,52	108	0,45	124	0,48
13	0,52	29	0,50	45	0,49	61	0,49	77	0,41	93	0,48	109	0,48	125	0,49
14	0,52	30	0,43	46	0,45	62	0,49	78	0,54	94	0,48	110	0,50	126	0,45
15	0,50	31	0,45	47	0,48	63	0,48	79	0,55	95	0,56	111	0,52	127	0,60
16	0,50	32	0,54	48	0,54	64	0,47	80	0,52	96	0,47	112	0,53	128	0,49

Далее, для практической оценки лавинного эффекта использовался критерий по ключу. Проверка была выполнена путем введения изменений в ключ, как и в открытом тексте. Результаты анализа приведены на рисунке 3. Как видно из рисунка, значение k_i лежит в интервале (0,4; 0,6). Криптоалгоритм удовлетворяет лавинному критерию, если при изменении одного бита на входе алгоритма изменяется в среднем половина битов на выходе алгоритма. Алгоритм Qamal удовлетворяет требованию лавинного критерия.

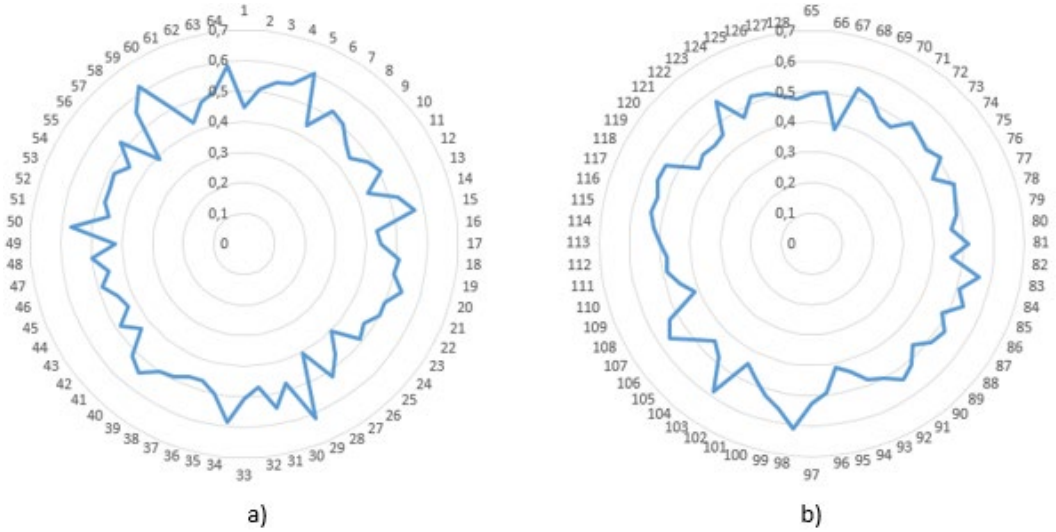


Диаграмма значений k_i: a) значений i от 1 до 64, b) значений i от 65 до 128.
Рисунок 3 - Анализ лавинного эффекта ключа для полнораундового алгоритма

3. Результаты проверки лавинного эффекта алгоритма BC-2

В алгоритме шифрования ВС-2 зашифрование производится путем последовательного выполнения трех преобразований: Conversion-S, Conversion MB и AddRoundKey [7]. Рассмотрим пример того, как данные преобразовании, используемые в алгоритме ВС-2, влияют на лавинный эффект.

В качестве входа берем два откытых текста, отличающихся друг от друга только на один бит:

1) AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA

2) AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AB

1. AddRoundKey:

1) F6 A2 3D 41 B4 1C 78 C2 9E 8B BF 7E 4E 07 AE DE A9 A0 38 6D F9 BB 4C 26 EE 89 7F CB 0C BE E3 33;

2) F6 A2 3D 41 B4 1C 78 C2 9E 8B BF 7E 4E 07 AE DE A9 A0 38 6D F9 BB 4C 26 EE 89 7F CB 0C BE E3 32.

2. Conversion-S:

1) 64 F8 75 0C EE AE 48 E4 7D FB E4 EF 6D 92 6E 61 35 C6 34 07 67 BD 37 A7 33 62 FA 9A 95 96 2E ED;

2) 64 F8 75 0C EE AE 48 E4 7D FB E4 EF 6D 92 6E 61 35 C6 34 07 67 BD 37 A7 33 62 FA 9A 95 96 2E 16.

Как видно, в операциях AddRoundKey и Conversion-S изменения одного бита распространяются только на один байт. Далее рассмотрим следующее преобразование.

3. Conversion MB:

1) A9 CB EF C3 66 CA 99 7D 71 D7 78 F9 0D 17 EC 42 DF 00 37 BA 6B 1C 59 3E 9A CE 38 11 41 3C 1A 4D;

2) FA F7 B0 08 DB 73 0C 50 9F 61 EB 25 D5 A6 EE C7 47 CC D4 15 F6 91 DB A3 C2 89 3F 39 BB 2D 9D B3.

Таким образом, полная диффузия достигается уже на первом раунде после операции Conversion MB.

Для практической оценки лавинного эффекта использовался лавинный критерий по тексту. Для проверки выбрали случайный открытый текстов длиной 256 бит. Произведя инверсию битов в каждой позиции, получили 256 новых открытых текстов и зашифровали их. Вычислили вероятности k_i между полученными шифртекстами и исходным шифртекстом. Результаты приведены в таблицах 5-7. 99,9% значений k_i (вероятность изменения половины битов в выходном значении) лежат в интервале (0,41; 0,59). Средние значения ε дляя раундов 1, 2 и 10 ,соответственно равны 0.055, 0.0473, и 0.047

Таблица 5 - Анализ лавинного эффекта алгоритма ВС-2 после первого раунда

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,49	33	0,44	65	0,51	97	0,52	129	0,54	161	0,48	193	0,45	225	0,50
2	0,50	34	0,46	66	0,53	98	0,48	130	0,48	162	0,50	194	0,46	226	0,46
3	0,49	35	0,48	67	0,53	99	0,43	131	0,50	163	0,55	195	0,54	227	0,50
4	0,50	36	0,48	68	0,49	100	0,51	132	0,52	164	0,48	196	0,48	228	0,51
5	0,46	37	0,56	69	0,45	101	0,48	133	0,53	165	0,47	197	0,54	229	0,48
6	0,52	38	0,55	70	0,46	102	0,45	134	0,54	166	0,50	198	0,44	230	0,47
7	0,51	39	0,53	71	0,48	103	0,54	135	0,50	167	0,51	199	0,46	231	0,56
8	0,49	40	0,50	72	0,55	104	0,48	136	0,48	168	0,53	200	0,48	232	0,56

9	0,48	41	0,49	73	0,54	105	0,46	137	0,51	169	0,49	201	0,45	233	0,54
10	0,44	42	0,50	74	0,48	106	0,50	138	0,54	170	0,47	202	0,55	234	0,45
11	0,49	43	0,48	75	0,49	107	0,53	139	0,45	171	0,51	203	0,45	235	0,49
12	0,51	44	0,44	76	0,51	108	0,50	140	0,49	172	0,49	204	0,48	236	0,47
13	0,49	45	0,45	77	0,50	109	0,47	141	0,49	173	0,53	205	0,51	237	0,47
14	0,55	46	0,47	78	0,57	110	0,54	142	0,48	174	0,52	206	0,53	238	0,51
15	0,49	47	0,45	79	0,43	111	0,54	143	0,44	175	0,55	207	0,43	239	0,39
16	0,47	48	0,54	80	0,50	112	0,52	144	0,51	176	0,54	208	0,52	240	0,47
17	0,51	49	0,54	81	0,50	113	0,52	145	0,50	177	0,49	209	0,50	241	0,50
18	0,41	50	0,46	82	0,46	114	0,46	146	0,46	178	0,47	210	0,48	242	0,51
19	0,45	51	0,51	83	0,48	115	0,55	147	0,46	179	0,50	211	0,51	243	0,50
20	0,44	52	0,54	84	0,47	116	0,59	148	0,51	180	0,52	212	0,46	244	0,51
21	0,43	53	0,43	85	0,52	117	0,49	149	0,50	181	0,52	213	0,50	245	0,49
22	0,49	54	0,42	86	0,50	118	0,49	150	0,44	182	0,46	214	0,49	246	0,46
23	0,56	55	0,52	87	0,52	119	0,55	151	0,52	183	0,50	215	0,51	247	0,52
24	0,52	56	0,50	88	0,51	120	0,50	152	0,50	184	0,46	216	0,51	248	0,47
25	0,52	57	0,54	89	0,48	121	0,52	153	0,52	185	0,52	217	0,51	249	0,49
26	0,54	58	0,46	90	0,48	122	0,47	154	0,44	186	0,52	218	0,48	250	0,45
27	0,49	59	0,50	91	0,46	123	0,54	155	0,51	187	0,51	219	0,45	251	0,49
28	0,51	60	0,53	92	0,50	124	0,53	156	0,50	188	0,50	220	0,54	252	0,53
29	0,52	61	0,52	93	0,45	125	0,53	157	0,48	189	0,47	221	0,50	253	0,42
30	0,49	62	0,54	94	0,50	126	0,54	158	0,48	190	0,53	222	0,49	254	0,47
31	0,48	63	0,54	95	0,43	127	0,55	159	0,48	191	0,49	223	0,47	255	0,41
32	0,48	64	0,42	96	0,50	128	0,44	160	0,50	192	0,48	224	0,52	256	0,59

Таблица 6 - Анализ лавинного эффекта алгоритма BC-2 после второго раунда

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,48	33	0,48	65	0,53	97	0,48	129	0,49	161	0,50	193	0,48	225	0,54
2	0,52	34	0,54	66	0,50	98	0,50	130	0,51	162	0,49	194	0,49	226	0,51
3	0,45	35	0,47	67	0,47	99	0,48	131	0,52	163	0,52	195	0,52	227	0,52
4	0,54	36	0,48	68	0,59	100	0,52	132	0,50	164	0,50	196	0,48	228	0,54
5	0,43	37	0,52	69	0,54	101	0,48	133	0,52	165	0,42	197	0,52	229	0,50
6	0,51	38	0,49	70	0,55	102	0,52	134	0,46	166	0,53	198	0,51	230	0,46
7	0,49	39	0,48	71	0,49	103	0,48	135	0,44	167	0,47	199	0,49	231	0,47
8	0,48	40	0,46	72	0,49	104	0,52	136	0,42	168	0,50	200	0,48	232	0,54
9	0,54	41	0,52	73	0,52	105	0,50	137	0,48	169	0,49	201	0,51	233	0,52
10	0,55	42	0,55	74	0,50	106	0,49	138	0,54	170	0,48	202	0,49	234	0,50
11	0,53	43	0,52	75	0,47	107	0,53	139	0,44	171	0,51	203	0,46	235	0,54
12	0,50	44	0,47	76	0,52	108	0,48	140	0,50	172	0,48	204	0,47	236	0,52
13	0,54	45	0,48	77	0,50	109	0,53	141	0,48	173	0,52	205	0,49	237	0,51
14	0,51	46	0,51	78	0,47	110	0,53	142	0,50	174	0,46	206	0,45	238	0,50
15	0,48	47	0,54	79	0,53	111	0,59	143	0,50	175	0,52	207	0,47	239	0,47
16	0,52	48	0,49	80	0,50	112	0,53	144	0,56	176	0,50	208	0,46	240	0,50
17	0,52	49	0,50	81	0,54	113	0,54	145	0,49	177	0,50	209	0,47	241	0,50
18	0,52	50	0,48	82	0,53	114	0,50	146	0,47	178	0,47	210	0,48	242	0,49
19	0,46	51	0,52	83	0,50	115	0,48	147	0,49	179	0,48	211	0,52	243	0,51
20	0,51	52	0,50	84	0,51	116	0,46	148	0,52	180	0,51	212	0,47	244	0,52
21	0,49	53	0,51	85	0,49	117	0,48	149	0,48	181	0,47	213	0,51	245	0,45
22	0,50	54	0,50	86	0,51	118	0,43	150	0,46	182	0,50	214	0,54	246	0,54

23	0,47	55	0,44	87	0,52	119	0,55	151	0,55	183	0,50	215	0,49	247	0,47
24	0,51	56	0,47	88	0,50	120	0,50	152	0,50	184	0,46	216	0,53	248	0,49
25	0,54	57	0,46	89	0,46	121	0,51	153	0,48	185	0,55	217	0,51	249	0,53
26	0,48	58	0,48	90	0,54	122	0,49	154	0,49	186	0,50	218	0,50	250	0,57
27	0,54	59	0,50	91	0,51	123	0,50	155	0,47	187	0,47	219	0,48	251	0,54
28	0,48	60	0,49	92	0,50	124	0,44	156	0,54	188	0,48	220	0,49	252	0,47
29	0,49	61	0,53	93	0,51	125	0,54	157	0,48	189	0,55	221	0,49	253	0,48
30	0,44	62	0,57	94	0,46	126	0,46	158	0,47	190	0,46	222	0,51	254	0,47
31	0,52	63	0,50	95	0,46	127	0,52	159	0,50	191	0,46	223	0,52	255	0,53
32	0,46	64	0,48	96	0,48	128	0,48	160	0,47	192	0,50	224	0,55	256	0,50

Таблица 7 - Анализ лавинного эффекта алгоритма BC-2 после десятого раунда

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,49	33	0,49	65	0,51	97	0,54	129	0,54	161	0,45	193	0,50	225	0,51
2	0,50	34	0,47	66	0,48	98	0,51	130	0,49	162	0,48	194	0,55	226	0,49
3	0,46	35	0,52	67	0,53	99	0,52	131	0,44	163	0,49	195	0,50	227	0,54
4	0,51	36	0,54	68	0,52	100	0,50	132	0,49	164	0,50	196	0,51	228	0,52
5	0,57	37	0,47	69	0,54	101	0,51	133	0,55	165	0,53	197	0,46	229	0,52
6	0,50	38	0,46	70	0,49	102	0,53	134	0,50	166	0,55	198	0,49	230	0,52
7	0,48	39	0,53	71	0,52	103	0,46	135	0,51	167	0,45	199	0,48	231	0,50
8	0,50	40	0,53	72	0,52	104	0,50	136	0,55	168	0,54	200	0,51	232	0,50
9	0,50	41	0,51	73	0,48	105	0,50	137	0,44	169	0,47	201	0,52	233	0,47
10	0,49	42	0,46	74	0,46	106	0,46	138	0,52	170	0,49	202	0,50	234	0,48
11	0,47	43	0,65	75	0,47	107	0,52	139	0,53	171	0,52	203	0,55	235	0,49
12	0,49	44	0,48	76	0,52	108	0,52	140	0,49	172	0,48	204	0,50	236	0,50
13	0,50	45	0,50	77	0,52	109	0,52	141	0,47	173	0,52	205	0,43	237	0,48
14	0,48	46	0,48	78	0,47	110	0,50	142	0,50	174	0,48	206	0,46	238	0,47
15	0,48	47	0,47	79	0,53	111	0,52	143	0,49	175	0,46	207	0,47	239	0,51
16	0,47	48	0,48	80	0,50	112	0,48	144	0,49	176	0,54	208	0,50	240	0,50
17	0,50	49	0,49	81	0,50	113	0,53	145	0,54	177	0,48	209	0,46	241	0,45
18	0,50	50	0,50	82	0,53	114	0,54	146	0,50	178	0,50	210	0,49	242	0,53
19	0,51	51	0,52	83	0,54	115	0,45	147	0,52	179	0,49	211	0,55	243	0,55
20	0,50	52	0,52	84	0,43	116	0,48	148	0,48	180	0,50	212	0,48	244	0,47
21	0,43	53	0,44	85	0,45	117	0,55	149	0,54	181	0,50	213	0,55	245	0,48
22	0,51	54	0,46	86	0,46	118	0,53	150	0,43	182	0,50	214	0,52	246	0,46
23	0,50	55	0,48	87	0,47	119	0,44	151	0,50	183	0,55	215	0,50	247	0,52
24	0,52	56	0,52	88	0,52	120	0,55	152	0,55	184	0,53	216	0,48	248	0,54
25	0,55	57	0,48	89	0,54	121	0,50	153	0,54	185	0,51	217	0,54	249	0,50
26	0,48	58	0,48	90	0,50	122	0,48	154	0,50	186	0,49	218	0,50	250	0,46
27	0,50	59	0,46	91	0,54	123	0,52	155	0,52	187	0,48	219	0,49	251	0,50
28	0,54	60	0,52	92	0,48	124	0,48	156	0,50	188	0,50	220	0,48	252	0,51
29	0,50	61	0,54	93	0,49	125	0,54	157	0,49	189	0,48	221	0,48	253	0,47
30	0,53	62	0,44	94	0,53	126	0,51	158	0,45	190	0,50	222	0,50	254	0,50
31	0,52	63	0,46	95	0,53	127	0,52	159	0,45	191	0,55	223	0,50	255	0,52
32	0,48	64	0,53	96	0,52	128	0,54	160	0,48	192	0,52	224	0,46	256	0,50

99,9% значении k_i(вероятность изменения половины битов в выходном значении) лежать на интервале (0,41; 0,59). Среднее значении ε для раундов 1, 2, 5 и 8 ,соответственно равны 0.055, 0.0473, 0.051, 0.047. Чем меньше значение лавинного

параметра, тем сильнее лавинный эффект в преобразовании. Таким образом, алгоритм BC-2 демонстрирует достаточно сильный лавинный эффект. При малых изменениях в открытом тексте наблюдаются различия около половины битов выходного текста. Лавинный эффект оказывается явно заметным уже после первого раунда шифрования

Заключение

Желательным свойством любого алгоритма шифрования должна быть высокая чувствительность результата к изменению начальных данных — любые малые изменения открытого текста или ключа должны приводить к значительным изменениям в шифрованном тексте. Если криптографический алгоритм не обладает лавинным эффектом в достаточной степени, противник может сделать предположение о входной информации, основываясь на выходной информации.

Чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании. Таким образом, все рассматриваемые алгоритмы демонстрирует свойства достаточно сильного лавинного эффекта. При малых изменениях в открытом тексте наблюдаются различия примерно в половине битов выходного текста. Лавинный эффект оказывается явно заметным уже после первого раунда шифрования.

Работа выполнена в рамках программы целевого финансирования BR05236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» Министерства образования и науки Республики Казахстан.

Литература

1. Б. Шнайер, Прикладная криптография, 2-е изд: Пер. с англ. –Триумф, 2002. – 816 с.
2. В.Столлингс, Криптография и защита сетей: принципы и практика. 2-е изд./Пер. с англ. – М: Вильямс, 2001, - 672 с.
3. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа // Москва. Гелиос АРВ – 2006, - 376 с.
4. Жданов О. Н., Золотарев В. В. Методы и средства криптографической защиты информации //Успехи современного естествознания. – 2010. – №. 2. – С. 99-100.
5. Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen× S-Boxes // Turk J Elec Engin. - 2001. - Т. 9, № 2. – С. 137-145.
6. Рябко Б.Я., Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2014. – 173 с.
7. Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения: Отчет о НИР (промежуточный) / РГП на ПХВ «Институт информационных и вычислительных технологий» КН МОН РК; рук. Нысанбаева С.Е.; исполн.: Бияшев Р.Г. и др. – Алматы, 2018. – 145 с. – № ГР 0118РК01064. – Инв. № 0218РК0064.

ОСОБЕННОСТИ ЦИФРОВОЙ СТЕГАНОГРАФИИ КАК МЕТОДА ОБЕСПЕЧЕНИЯ СОКРЫТИЯ ИНФОРМАЦИИ

Дайырбаева Э.Н., Липская М.А.
e-mail: nurbekkyzy_e@mail.ru, limaan78@mail.ru,
Казахская академия транспорта и коммуникации им. М.Тынышпаева

Аннотация. *Для владельца какой-либо информации, либо для тех лиц, которые ею не владеют, она имеет всегда важную ценность. Поэтому в обязательном порядке появилась необходимость в принятии мер по защите передаваемой информации, либо по скрытию данных факта ее передачи. Вследствие этого, в данной статье рассматриваются особенности цифровой стеганографии, как методы обеспечения сокрытия информации*

Вступление

Стеганография — это искусство отправки скрытых или невидимых сообщений. Современная стеганография, как правило, имеет дело с информацией в электронной форме, а не с физическими объектами и текстами. Это имеет смысл для целого ряда причин. Прежде всего, размер информации, как правило, (обязательно) весьма мал по сравнению с размером данных, в которых она должна быть скрыта (текстовый контейнер). Во-вторых, само извлечение может быть автоматизировано, когда данные в электронной форме, так как компьютеры могут эффективно обрабатывать их и выполнить алгоритмы, необходимые для получения сообщения. Электронные данные также часто включают в себя избыточные, ненужные и незаметные пространства данных, которые можно использовать, чтобы скрыть сообщения. В каком-то смысле эти пустые пространства обеспечивают своего рода «скрытый отсек», в который могут быть вставлены секретные сообщения и отправлены принимающей стороне.

Стеганографическая информация может быть скрыта почти везде, и некоторые объекты контейнера больше подходят для скрытия информации, чем другие. Стеганография в изображениях стала более популярной в последние годы, чем другие виды стеганографии, возможно из-за большого потока изображений в электронном виде, доступного с появлением цифровых камер и высокоскоростной интернет-передачи. Стеганография в изображении часто включает в себя скрытие информации в естественно возникающих «шумах» изображения и предоставляет хорошие наглядные примеры для таких методов.

Развитие вычислительной техники в последнее время дало новый толчок в развитии компьютерной стеганографии. Исследуются новые области применения. Скрываемые сообщения теперь встраиваются в цифровые данные (изображения, видео и аудиофайлы). Также существуют методы по внедрению данных в текстовые файлы и даже в исполняемые файлы программ.

В настоящее время в стеганографии условно выделяют несколько направлений:

- классическая стеганография, которая включает в себя «некомпьютерные методы» сокрытия сообщений неэлектрической природы;

- компьютерная стеганография предполагает использование свойств форматов данных, обрабатываемых и передаваемых в инфокоммуникационных сетях;

цифровая стеганография основана на избыточности пересылаемых мультимедийных данных, представленных в цифровом виде, изначально имеющих аналоговую природу (изображения, видео, звук) [1].

Далее в статье речь идет о компьютерной и цифровой (преимущественно) стеганографии.

Стеганографическая наука не стоит на месте и продолжает бурно развиваться, о чем свидетельствуют многочисленные публикации и защиты диссертаций, конференции, патенты на изобретения и полезные модели, свидетельства о регистрации программ. Число приложений, позволяющих, как осуществлять скрытое встраивание

информации, так и проводить анализ на предмет обнаружения таковых вложений, находящихся только в открытом доступе в сети интернет, измеряется десятками. Таким образом, данная статья призвана дополнить и структурировать устоявшуюся классификацию стеганографических методов, представленную, а также осветить направления и тенденции перспективного развития цифровой и компьютерной стеганографии.

По целям использования методов цифровой и компьютерной стеганографии общепризнанными являются три направления:

- встраивание скрытых каналов передачи информации – целью встраивания является сокрытие факта передачи информации;
- встраивание цифровых водяных знаков (ЦВЗ) – цель встраивания состоит в подтверждении подлинности предаваемых данных и в предотвращении несанкционированного доступа к ним;
- встраивание идентификационных номеров (цифровые отпечатки пальцев) – с целью скрытой аннотации и аутентификации передаваемой информации [2].

Цифровые водяные знаки (ЦВЗ) используются для защиты от копирования, сохранения авторских прав. Невидимые водяные знаки считываются специальным устройством, которое может подтвердить либо опровергнуть корректность. ЦВЗ могут содержать различные данные: авторские права, идентификационный номер, управляющую информацию. Наиболее удобными для защиты с помощью ЦВЗ являются неподвижные изображения, аудио- и видеофайлы.

Технология записи идентификационных номеров производителей очень похожа на ЦВЗ, но отличие состоит в том, что на каждое изделие записывается свой индивидуальный номер (так называемые «отпечатки пальцев»), по которому можно вычислить дальнейшую судьбу изделия. Невидимое встраивание заголовков иногда используется, к примеру, для подписей медицинских снимков, нанесения пути на карту и т. п. Скорее всего, это единственное направление стеганографии, где нет нарушителя в явном виде.

Основные требования, предъявляемые к водяным знакам: надёжность и устойчивость к искажениям, незаметности, робастности к обработке сигналов (устойчивость— способность системы к восстановлению после воздействия на неё внешних/внутренних искажений, в том числе умышленных). ЦВЗ имеют небольшой объём, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Перед помещением ЦВЗ в контейнер водяной знак нужно преобразовать к подходящему виду. К примеру, если в качестве контейнера используется изображение, то и ЦВЗ должны быть представлены как двумерный битовый массив.

Для повышения устойчивости к искажениям часто применяют помехоустойчивое кодирование или используют широкополосные сигналы. Начальную обработку скрытого сообщения делает прекодер. Важная предварительная обработка ЦВЗ — вычисление его обобщённого Фурье-преобразования. Это повышает помехоустойчивость. Первичную обработку часто производят с использованием ключа — для повышения секретности. Потом водяной знак «укладывается» в контейнер (например, путём изменения младших значащих бит). Здесь используются особенности восприятия изображений человеком. Широко известно, что изображения имеют огромную психовизуальную избыточность. Глаза человека подобны низкочастотному фильтру, который игнорирует мелкие

элементы изображения. Наименее заметны искажения в высокочастотной области изображений. Внедрение ЦВЗ также должно учитывать свойства восприятия человека [3].

Во многих стегосистемах для записи и считывания ЦВЗ используется ключ. Он может предназначаться для ограниченного круга пользователей или же быть секретным. Например, ключ нужен в DVD-плеерах для возможности прочтения ими содержащихся на дисках ЦВЗ. Как известно, не существует таких стегосистем, в которых бы при считывании водяного знака требовалась другая информация, нежели при его записи. В стегодетекторе происходит обнаружение ЦВЗ в защищённом им файле, который, возможно, мог быть изменён. Эти изменения могут быть связаны с воздействиями ошибок в канале связи, либо преднамеренными помехами. В большинстве моделей стегосистем сигнал-контейнер можно рассмотреть как аддитивный шум. При этом задача обнаружения и считывания стегосообщения уже не представляет сложности, но не учитывает двух факторов: неслучайности сигнала контейнера и запросов по сохранению его качества. Учёт этих параметров позволит строить более качественные стегосистемы. Для обнаружения факта существования водяного знака и его считывания используются специальные устройства — стегодетекторы. Для вынесения решения о наличии или отсутствии водяного знака используют, к примеру, расстояние по Хэммингу, взаимокорреляцию между полученным сигналом и его оригиналом. В случае отсутствия исходного сигнала в дело вступают более изощрённые статистические методы, которые основаны на построении моделей исследуемого класса сигналов.

Встраиваемые ЦВЗ бывают трех типов:

- робастные;
- хрупкие;
- полухрупкие.

Робастность – устойчивость стегоконтейнера (объекта, содержащего в себе скрываемую информацию)

ЦВЗ к изменениям. В свою очередь, робастные ЦВЗ подразделяются на 3 вида. Видимые для всех, хотя бы одной стороны, либо ЦВЗ устойчивые к модификации и извлечению контейнера.

Хрупкие ЦВЗ чувствительны к любым изменениям контейнера. Они применяются с целью проверки целостности контейнера. В случае обнаружения модификации необходимо установить её вид и местоположение.

Полухрупкие преднамеренно создаются чувствительными к определенным изменениям контейнера. Например, пользователю можно изменить звучание частот, но нельзя удалить голос исполнителя из аудиозаписи [4].

Пример реализации стеганографии

Применение стеганографии с использованием IPTC метаданных.

IPTC – стандарт метаданных для цифровых изображений, который позволяет хранить подробную различную информацию, связанную с авторством, а не как EXIF который нацелен на техническую информацию. В метаданных IPTC могут храниться такие описательные поля, как ObjectName (заголовок), Keywords (ключевые слова), Caption (описание, есть несколько вариаций тега).

Основное отличие IPTC от EXIF в стеганографическом смысле, заключается в том, что IPTC-метаданные невозможно просмотреть без использования дополнительного ПО.

IPTC-метаданные легко можно изменить с помощью стороннего ПО. В данном примере показан способ изменения IPTC-метаданных с помощью программы ACDSee.

Для изменения этих метаданных необходимо:

− запустить выбранное нами ПО;

− открыть в нем изображение;

− перейти в “свойства” далее “метаданные”;

На экране появятся метаданные, которые можно изменить. Это IPTC, EXIF и метаданные ACDSee.

− выбрать IPTC-метаданные;

− изменить эти метаданные и сохранить изменения.

Выводы

Цифровая стеганография является распространённым и достаточно простым способом сокрытия цифровой передачи данных. Для следования основным требованиям стеганографии – надежности и незаметности, необходимо использовать различные устройства, например, декодер, стегодетектор.

Стегодетекторы различаются как по собственным функциям, так и по требуемой информации. От последнего зависит класс данной стегосистемы. Также были рассмотрены основные типы ЦВЗ и описаны их характеристики. У каждого типа есть свои преимущества и свои недостатки по определенным параметрам.

Существует множество различных способов реализации цифровой стеганографии. Один из самых распространённых способов данного процесса является изменение метаданных медиа-файлов. Мы рассмотрели пример реализации стеганографии с метаданными изображений.

Литература

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография/ М.: Солон-Пресс, 2009. – 272 с.

2. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ //Монография/ М.: Вузовская книга, 2009. – 220 с.

3. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. «Стеганографические системы. Критерии и методическое обеспечение» : Учебн.-метод. пособие / Под ред. д-ра техн. наук В. Г. Грибунина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2016. — 324 с. : ил. — ISBN 978-5-9515-0317-6

4. Грибунин В. Г., Жердин О. А., Мартынов А. П., Николаев Д. Б., Силаев А. Г., Фомченко В. М. Основы стеганографии // Под ред. д-ра техн. наук В. Г. Грибунина, г. Трехгорный, 2012.

КРИПТОГРАФИЧЕСКАЯ АТАКА НА АЛГОРИТМ «QAMAL» МЕТОДОМ БУМЕРАНГА

Дюсенбаев Д., Сақан Қ.
e-mail: dimash_dds@mail.ru, kairat_sks@mail.ru

Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В статье рассматривается оценка стойкости разрабатываемого институтом информационных и вычислительных технологии – симметричного блочного алгоритма «Qamal» с использованием атаки методом бумеранга. Рассмотрено каждое преобразование данного алгоритма по схеме атаки бумеранга. Кратко описана особенность программной реализации определения вероятностей нахождения допустимых квартетов открытого текста для дальнейшего анализа. Приведены результаты – вероятности определения допустимых квартетов, полученные экспериментальным путем.*

Введение

Способность криптосистемы противостоять атакам криптоаналитика называется стойкостью. Количественно стойкость измеряется как сложность наилучшего алгоритма, приводящего криптоаналитика к успеху с приемлемой вероятностью.

Последние десятилетие характеризуется резким увеличением числа открытых работ по всем вопросам криптологии, а криптоанализ становится одной из наиболее активно развивающихся областей исследований. Многие криптосистемы, стойкость которых не вызывала особых сомнений, оказались успешно раскрытыми. При этом разработан большой арсенал математических методов, представляющих прямой интерес для криптоаналитика.

Проведение криптоанализа для давно существующих и недавно появившихся криптоалгоритмов очень актуально, так как вовремя можно сказать, что данный криптоалгоритм нестоек, и усовершенствовать его или заменить новым. Для того, чтобы выявлять нестойкие криптоалгоритмы необходимо все время совершенствовать уже известные методы криптоанализа и находить новые. [1][2].

Краткий обзор атаки методом бумеранга

Данный метод практически является улучшенным дифференциальным криптоанализом. Отличиями являются: а) анализ ведется множеством квартетов открытых текстов и их соответствующих шифртекстов, б) изменение открытого текста может покрывать только часть шифра в связи с применением двухэтапного процесса $E_0()$ и $E_1()$. В результате, анализируя множество полученных квартетов открытых и закрытых текстов с определённой разностью, можно выделить ключ или его часть с наибольшей вероятностью.[3]

Алгоритм атаки (Рисунок 1).

1) N-раундовый алгоритм разделяется на две части по $N/2$ раундов.

2) $E_0()$ - процедура зашифровывания первой части алгоритма. Для квартета выбираются два открытых текста X_1 и X_2, разность между ними составляет некоторую величину dx, причем разность определяется битовой операцией XOR. После применения к текстам X_1 и X_2 функции E_0 получается разность $dx^* = E_0(X_1) \oplus E_0(X_2)$.

3) Зашифровываются тексты X_1 и X_2 зашифровываются с помощью процедуры шифрования второй части $E_1()$. В результате получаются шифртексты $Y_1 = E_1(E_0(X_1))$ и $Y_2 = E_1(E_0(X_2))$.

4) С помощью шифртекстов Y_1 и Y_2 определяются два других шифртекста Y_3 и Y_4, связанных с ними разностью dy следующим образом: $Y_3 = Y_1 \oplus dy$ и $Y_4 = Y_2 \oplus dy$.

5) Дальше для формирования квартета открытых текстов процесс производится в обратном порядке: к шифртекстам Y_3 и Y_4 применяется обратная функция E_1^{-1}, причем $E_1^{-1}(Y_1)=E_0(X_1)$ и $E_1^{-1}(Y_2)= E_0(X_2)$; $E_1^{-1}(Y_3) \oplus E_0(X_1)= E_1^{-1}(Y_4) \oplus E_0(X_2)=dy^*$.

6) В результате расшифровывания шифртексты Y_3 и Y_4 получаются тексты X_3 и X_4 следующим образом: $X_3= E_0^{-1}(E_1^{-1}(Y_3))$ и $X_4= E_0^{-1}(E_1^{-1}(Y_4))$, причем $X_1 \oplus X_2= X_3 \oplus X_4=dx$.

Допустимым квартетом открытых и закрытых текстов называется квартет $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ и (X_4, Y_4), для которого при заданном dy разность входных текстов X_1 и X_2 совпадает с разностью полученных по схеме бумеранга текстов X_3 и X_4 с использованием шифрованных текстов Y_1, Y_2, Y_3 и Y_4.

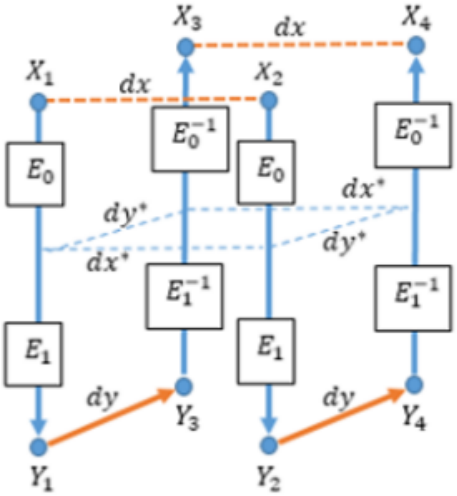


Рис. 1 Схема атаки методом бумеранга

Исследование алгоритма шифрования «Qamal» методом атаки бумеранга

Ключевым моментом исследования является нахождение множеств квартетов открытых текстов и соответстующих их шифртекстов. Как известно, блок шифрования данных алгоритма «Qamal» включает следующие преобразования: операция побитового сложения (*XOR*), *S*-блок замены и процедуры перемешивания *Mixer1* и *Mixer2*. [4]

Сначала рассматривается возможность нахождения необходимых для проведения атаки методом бумеранга квартетов по каждому преобразованию шифрования в отдельности, т.е. для случая функционирования независимо друг от друга. Стандартной длиной блока шифрования считается 128 бит (16 байтов). В дальнейшем, разделение по этапам бумеранга $E_0()$ и $E_1()$ зависит от сложности вычисления преобразований. С целью определения вероятности существования квартетов атаки бумеранга относительно каждого преобразования составлен алгоритм вычисления и реализовано программное обеспечение.

1) **Операция побитового сложения (*XOR*).** Для анализа рассматривается все 8 раундов шифрования, а этапы при формирования квартетов $E_0()$ и $E_1()$ распределяются симметрично, по четырем раундам. Согласно алгоритма метода бумеранга выпбираются следующие операции: берутся открытые тексты X_1 и X_2. В качестве этапов $E_0()$ и $E_1()$ принимается операция сложения открытого текста с секретным (рауновым) ключом: $E_{j-1}(X_j)= X_j \oplus k_i$, где j=1,2. Разность между X_1 и X_2 обозначается через dx: $dx= X_1 \oplus X_2$. Далее по схеме вычисляются $Y_1= E_1(E_0(X_1)) = X_1 \oplus k_s$ и $Y_2= E_1(E_0(X_2))= X_2 \oplus k_s$, здесь k_s – значение, полученное через битовое сложение раундовых ключей. Следовательно,

шифртексты Y_3 и Y_4 имеют следующий вид: $Y_3 = X_1 \oplus k_s \oplus dy$, $Y_4 = X_2 \oplus k_s \oplus dy$. Учитывая, что $E_{j-1}() = E_{j-1}^{-1}()$, составляющие элементы квартета вычисляются следующим образом:

$$X_3 = X_1 \oplus k_s \oplus dy \oplus k_s;$$
$$X_4 = X_2 \oplus k_s \oplus dy \oplus k_s..$$

Причем разность $X_3 \oplus X_4 = X_1 \oplus k_s \oplus dy \oplus k_s \oplus X_2 \oplus k_s \oplus dy \oplus k_s = X_1 \oplus X_2$.

Примеры. На следующих 16 примерах более подробно показаны шаги формирования необходимых квартетов (данные в шестнадцатеричном виде без обозначения *0x*:

X_1 ={87,E9,5E,62,5E,AA,78,AC,CA,54,8C,58,92,0C,5B,0F},

X_2 ={9E,8E,AA,A3,09,4C,96,7D,DD,87,9D,DA,01,2D,32,3D},

$dx = X_1 \oplus X_2$={19,67,F4,C1,57,E6,EE,D1,17,D3,11,82,93,21,69,32}.

Соответствующие шифртексты:

Y_1={41,22,DF,8D,94,A2,CB,C0,62,BB,BE,50,DC,4E,F3,90}

Y_2={58,45,2B,4C,C3,44,25,11,75,68,AF,D2,4F,6F,9A,A2}.

Разности dy выбираются случайным образом:

dy ={AB,CD,EF,98,76,54,32,10,FE,DC,BA,01,23,45,67,89}.

Отсюда:

$Y_3 = Y_1 \oplus dy$={EA,EF,30,15,E2,F6,F9,D0,9C,67,04,51,FF,0B,94,19};

$Y_4 = Y_2 \oplus dy$={F3,88,C4,D4,B5,10,17,01,8B,B4,15,D3,6C,2A,FD,2B}.

Теперь подчитываются X_3 и X_4 :

X_3 ={2C,24,B1,FA,28,FE,4A,BC,34,88,36,59,B1,49,3C,86};

X_4 ={35,43,45,3B,7F,18,A4,6D,23,5B,27,DB,22,68,55,B4}.

В конце вычисляются их разности и сверяются с разностью открытых текстов X_1 и X_2:

$X_3 \oplus X_4$={19,67,F4,C1,57,E6,EE,D1,17,D3,11,82,93,21,69,32}.

Отсюда получается, что $X_1 \oplus X_2 = X_3 \oplus X_4$.

Таким образом, относительно операции побитового сложения *XOR* алгоритма шифрования «Qamal» независимо от количества раундов с вероятностью $p=1$ удается формировать квартеты открытых и соответствущих закрытых текстов.

2) Нелинейное преобразование – S-блок замены. Проведен анализ возможности получения таких квартетов относительно *S*-блока замены алгоритма «Qamal». В этом случае для простоты формирования квартетов используются только два раунда шифрования. Первый этап атаки бумеранга $E_0()$ включает 1-ый раунд преобразования и $E_1()$ – 2-ой раунд. Для точного определения количество квартетов, удовлетворяющих условиям атаки бумеранга, создана программа, где входные параметры X_1, X_2 и *dy* меняются в диапазоне от 0 до 255. Количество всевозможных вариантов выбора соответствует числу 256^3 или 2^{24}. По результатам вычислений программы установлено, что в данном диапазоне найдено всего 63960 допустимых квартетов, что близко к числу $\approx 2^{16}$.

Таким образом, после второго раунда вероятность нахождения квартета для S-блока замены для метода составляет 2^{-8}. При определении квартетов учтены следующие условия:

а) для всех составляющих квартета элементов X_1, X_2, X_3, X_4: $X_i \neq X_j$, где $i, j = 1, 2, 3, 4$.

б) для разности dy: $dy \neq 0$.

На следующих трех примерах продемонстрирована процедура формирования квартетов (таблица В.10).

Примечание: Операторам E_i и E_i^{-1} соответствует преобразование S-блок и обратный S-блок, соответственно, i – номера раундов (этапов бумеранга).

В рассмотренных примерах по результатам проверки образованы следующие квартеты:

- в 1-ом примере: открытые тексты – 04, AE, E4, 4E и шифртексты – E8, B9, E4, 4E;
- во 2-ом примере: открытые тексты – 6E, 9D, 6D, 9E и шифртексты – D7, B1, 4C, 2A.

В 3-ом примере не удалось сформировать квартеты по заданным исходным параметрам.

Программный продукт определения количества допустимых квартетов относительно *S*-блока замены реализован согласно следующей блок-схеме (Рисунок 2).[5]

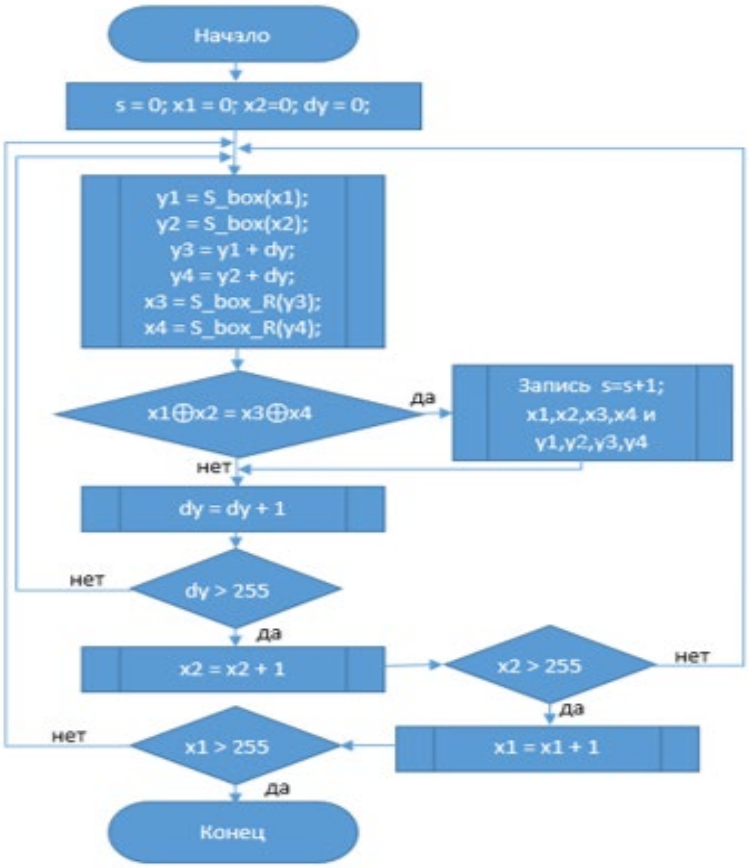


Рис. 2 Блок-схема алгоритма поиска квартетов по преобразованию S-блока

3) Операция перемешивания Mixer2. Для анализа рассматривается все 8 раундов шифрования. Этапы $E_0()$ и $E_1()$ разделены по четыре раунда. В качестве этапов $E_i()$ рассматривается строчное преобразования заданного массива – Mixer2. Для алгоритма метода бумеранга по преобразованию Mixer2 с целью определения

количества допустимых квартетов разработан программный продукт. Так как данное преобразование реализуется всеми четырьмя элементами строки массива, процесс полного перебора данных составляет 2^{96} операций. Составляющими элементами являются следующие векторы: $X_1 = \{x_{11}, x_{12}, x_{13}, x_{14}\}$, $X_2 = \{x_{21}, x_{22}, x_{23}, x_{24}\}$ и $dy = \{dy_1, dy_2, dy_3, dy_4\}$, где каждая компонента принимает 256 значений от 0 до 255. Поэтому, экспериментальные вычисления проводились только в определенном диапазоне исходных данных X_1, X_2 и dy.

4) Операция перемешивания Mixer1. Для анализа рассматривается 2 раунда шифрования. Этапы *E0()* и *E1()* разделены по одному раунду. Как ранее описано, Mixer1 производит колонное преобразование данных, записанных в матричном виде 4x4, 6x4 или 8x4. Экспериментальным путем определена вероятность формирования допустимых квартетов открытых и закрытых текстов. В случае длины блока шифрования 16 байт составляющие элементы атаки методом бумеранга имеют по четыре комонента: $X_1 = \{x_{11}, x_{12}, x_{13}, x_{14}\}$, $X_2 = \{x_{21}, x_{22}, x_{23}, x_{24}\}$ и $dy = \{dy_1, dy_2, dy_3, dy_4\}$, каждый, который меняется в диапазоне от 0 до 255. В итоге для уточнения чиленных данных необходимо произвести 2^{96} операций. Но с учетом высоких требований ко времени обработки и вычислительным мощностям подсчет был проведен до 2^{24} операций: при вычислении все составляющие элементы параметров X_2 и *dy* были зафиксированными.

Таким образом, после двух раундов при фиксированных восьми значениях и всевозможных вариантах восьми составляющих параметров X_1 и dy, принимающих 256 значений каждый, вероятность формирования квартетов для атаки бумеранга составляет $1/2^8$. Очевидно, что при уменьшении количества фиксированных составляющих элементов, вероятность формирования квартетов также будет уменьшаться. Поэтому, в случае полного перебора составляющих элементов вероятность появления квартетов будет слишком мала.

Основываясь на свойствах основных операций алгоритма «Qamal» относительно количества допустимых квартетов метода бумеранга была определена двухраундовая характеристика и ее вероятность. Если рассмотреть все операции алгоритма и учесть, что операция Mixer2 (в которой с вероятностью *p=1* можно было формировать допустимый квартет) рассеивает изменение одного байта на все четыре байта строки матрицы, то полученная вероятность формирования квартета Mixer1 однозначно будет уменьшаться. Вероятность того, что все четыре байта будут преобразованы в нужное значение, составит $\left({}^{1}/_{2^8}\right)^4 = {}^{1}/_{2^{32}}$. В итоге общая вероятность получения допустимого квартета после второго раунда будет $p = {}^{1}/_{2^{32}} * {}^{1}/_{2^8} = 2^{-40}$.

Учитывая, что после второго раунда вероятность p нахождения допустимого квартета полученная на 2^{24} операций из 2^{96} возможных операций в преобразовании Mixer1, достаточно мала, то дальнейшее увеличение количества операций стремительно снижает интересующую нас вероятность p. В итоге с увеличением числа раундов до восьми и количеством операций в Mixer1, равным 2^{96}, вероятность нахождения правильных пар текстов очень мала и стремится к сложности полного перебора алгоритма 2^{-128}, что позволяет сделать следующий вывод: применение атаки методом бумеранга для определения каких-либо слабостей алгоритма «Qamal» нецелесообразно.

Заключение

Как указано выше, применение на практике атаки методом бумеранга ограничено высокими требованиями к времени обработки и объёму данных. В настоящее время на практике атака методом бумеранга применяется в основном к шифрам с уменьшенным количеством раундов, где данный алгоритм до сих пор остается теоретическим достижением.

Работа выполнена в рамках программы целевого финансирования BR05236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» Министерства образования и науки Республики Казахстан.

Литература

1. Б. Шнайер. Прикладная криптография. 2-издание. Протоколы, алгоритмы и исходные тексты на языке С. Москва. : Триумф, 2002.

2. А.Г. Ростовцев, Н.В. Михайлова. Методы криптоанализа классических шифров. - https://studfile.net/preview/306445/(13.12.2019).

3. David Wagner (March 1999). "The Boomerang Attack" (PDF/PostScript). 6th International Workshop on Fast Software Encryption (FSE '99). Rome: Springer-Verlag. pp. 156–170. Retrieved 2007-02-05.

4. Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения: Отчет о НИР (промежуточный) / РГП на ПХВ «Институт информационных и вычислительных технологий» КН МОН РК; рук. Нысанбаева С.Е.; исполн.: Бияшев Р.Г. и др. – Алматы, 2018. – 145 с. – № ГР 0118РК01064. – Инв. № 0218РК0064.

5. Сақан Қ., Алғазы К. Программная реализация алгоритма симметричного блочного шифрования «Qamal» для исследования его криптографических свойств // Матер. науч. конф. ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2019. - С. 269-275.

ИГРОВАЯ СИСТЕМА ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБУЧЕНИЯ СТУДЕНТОВ В КУРСЕ СИСТЕМНОГО АНАЛИЗА

Жаннатова М.Т.

e-mail: moldir.zhannatova@narxoz.kz

АО «Университет «Нархоз», студентка 2-курса магистратуры специальности «Информационные системы»,

научный руководитель: к.э.н., ассоц. проф. Алдажаров К.С.,

Казахстан

Аннотация. *В Этой статье рассмотрена практическая разработка игровой системы обучения для повышения эффективности обучения студентов. Обучение на основе игр сочетается с образовательными и информационными технологиями. Из-за*

продолжающегося электронного обучения игровому обучению уделяется больше внимания. При обучении на основе игры содержание курса отображается в игре, чтобы обеспечить сценарную среду обучения, повторное самообучение, а постоянное взаимодействие и обратная связь могут повысить интерес и мотивацию обучения. Следовательно, игровое обучение может эффективно достигать цели обучения. В данной статье я использовала эксперимент, который проводился в научно-технологическом университете Тайваня и сделала анализ применимости данного метода для нашей образовательной системы.

Для оценки эффектов обучения в данной статье используются инструменты разработки 3D-игр и содержание курса, соответствующее контенту игрового уровня. Это экспериментальное обучение выполняется для курса системного анализа (на уровне бакалавриата третьего курса), студенты имеют опыт управления информацией. Учащиеся разделены на две группы для экспериментального проектирования: одна - экспериментальная группа, другая - контрольная группа. После внедрения игровой системы обучения баллы достижений и вопросник экспериментальной группы собираются практически, а также исследуется разница в успеваемости между экспериментальной и контрольной группами. Результаты показывают, что учебные мотивы студентов оказывают значительное влияние на учебные достижения, и учебные достижения студентов с игровым обучением лучше, чем у тех, кто использует традиционное очное обучение. И результаты могут предоставить соответствующие преподаватели в качестве ссылок.

Компьютерные игры отвечают реальным потребностям и интересам детей, становятся наиболее популярной компьютерной деятельностью и предоставляют новый способ взаимодействия. Некоторые из преимуществ игр заключаются в том, что они привлекательны, новы, обеспечивают лучшую атмосферу и помогают ученику сосредоточиться на задаче. Дети, как и все люди, любят учиться, когда им это не навязывают. Современные компьютерные и видеоигры предоставляют возможности обучения каждую секунду или ее часть (Пренский, 2003,). Джи (2003) утверждает, что «реальная важность хороших компьютерных и видеоигр состоит в том, что они позволяют людям воссоздать себя в новых мирах и одновременно достичь отдыха и глубокого обучения». Образовательная игра делает ученика центром обучения, что делает процесс обучения более простым, интересным и эффективным [1].

Исследование проводилось над студентами, которые проходили предмет системный анализ. Системный анализ - это процесс эффективного решения проблем, который делает «системный анализ» важной задачей. В этом эксперименте игры используются для улучшения скучного и сложного курса, где содержание курса соответствует игровым уровням, делая знания и навыки преподавания курса доступными через игровое обучение. В игре используется модель мотивации Келлера (ARCS). Модель ARCS - это подход к решению проблем, связанный с разработкой мотивационных аспектов среды обучения для стимулирования и поддерживать мотивацию студентов к обучению (Келлер, 1983). В этом исследовании использовали трехмерную игру, который основан на курсе системного анализа. В процессе разработки данной игры, создатели тесно сотрудничали с учителями, имеющие опыт преподавания. В процессе экспериментального исследования студентов поделили на две группы. Экспериментальная группа использовала «игровое обучение», а контрольная группа «традиционное обучение лицом к лицу». В контрольной группе обучаются 30 учеников,

а в экспериментальной группе - 33 ученика. Все учащиеся имеют одинаковый учебный контент и ресурсы. После окончания занятия все учащиеся должны сдать тест и заполнить анкету. Затем сравнивается разница между результатами теста и анкетным анализом обучения, основанного на игре, и несоответствие результатов обучения между подходом к обучению в игре и традиционным обучением «лицом к лицу» [2].

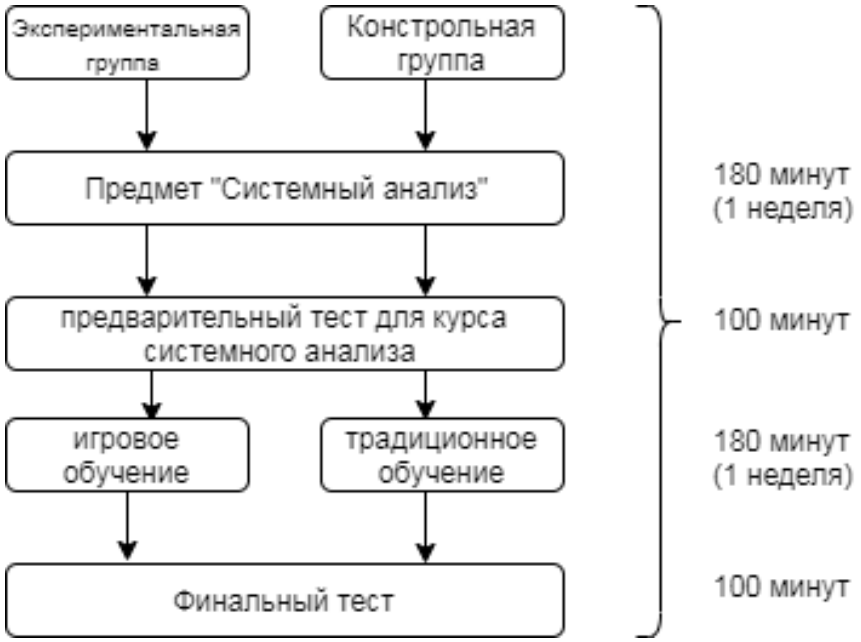


Рисунок – 1. Схема эксперимента для сравнения обучения, основанного на игре, и традиционного подхода «лицом к лицу».

История игры разворачивается в офисе компании. Поскольку в процессе системного анализа участвуют разные сотрудники, учащийся может выполнять разные роли и свободно выбирать, какой персонаж будет действовать, например, руководитель проекта, системный аналитик и программист, где разные роли соответствуют различным сценам в игре. В этом исследовании используется трехмерная сценарная игра на основе ARCS и стратегия обучения для разработки игровой системы обучения. В игре история разворачивается в компьютерной и интернет-сервисной компании, чьи клиенты и сложное оборудование получают все больше и больше. Игрок должен помочь компании оценить и разработать программное обеспечение, выполнять разные роли и задачи. Дизайн интерфейса: игра, которую разрабатывает это исследование, принимает во внимание историю сюжета, среду и возраст игроков, чтобы повысить аутентичность игры, использует офисную модель в качестве сцены, офисного работника - как людей и 3D-Max, чтобы завершить фактический интерфейс, который взаимодействует с игроками в системе.

В соответствии с упомянутым системным планированием, это исследование развивает ролевую игру, которая функционирует следующим образом: (1) Ситуация в игре: Конструкция игры, помимо дизайна игрового экрана, также включает в себя дизайн драмы и персонажей. История разворачивается в компьютерной и интернет-сервисной

компании, чьи клиенты и сложное оборудование получают все больше и больше. Поэтому эта компания хочет разработать системы, которые могут отвечать на вопросы клиентов и повышать эффективность. Игрок должен помочь компании оценить и разработать программное обеспечение, выполнять разные роли в процессе разработки и выполнять разные задачи в качестве разных ролей для завершения разработки программного обеспечения. (2) Дизайн интерфейса: игра, которую разрабатывает это исследование, принимает во внимание историю сюжета, среду и возраст игроков, чтобы повысить аутентичность игры, использует офисную модель в качестве сцены, офисного работника - как людей и 3D- Max, чтобы завершить фактический интерфейс, который взаимодействует с игроками в системе. В игре предусмотрено пять различных ролей на выбор. На рисунке 2 показано, как выбрать роль для игрового задания, а на рисунке 3 показано, что каждая роль соответствует разным ситуациям и задачам, и игрок может пройти разные роли, чтобы изучить все различные задания на разных позициях. В анализе требований, это исследование использует игру-лабиринт, которая покажет знак проблемы и положение игрока. При прохождении знака проблемы персонаж должен остановиться, а игрок должен решить текущую проблему, чтобы продолжать движение вперёд. В этой задаче множественный выбор. Помимо решения всех задач в лабиринте, рисунок 5 показывает, что игрок должен найти выход, чтобы повысить свой интерес и удержать внимание игрока на игровом обучении. В этом задании игрок должен различать требования на функциональные и нефункциональные. Экран включает в себя отсчёт времени, очки здоровья и оценки. Если ответ неправильный, количество очков здоровья уменьшится на единицу, и вопрос появится снова, и обратный отсчёт будет сброшен, чтобы дать игроку возможность исправить ошибку. Игрок должен ответить в ограниченное время, чтобы повысить сложность игры. В конце фазы обучения, показанной на рисунке 6, игрок должен пройти оценку, после чего он получит оценку, которая будет предоставлена учителю для справки.

Рисунок – 2. Выбрать персонаж

Рисунок – 3. Информация про персонажа

Рисунок – 4. Игроки определяют требования

Рисунок – 5. Тест оценки системы для роли

В этом исследовании была реализована система обучения на основе ролевых игр для курса системного анализа, и результаты обучения становятся значительными после системных оценок. Разработанная система применяет дистанционное обучение для экспериментов с игровым и традиционным обучением, а также для обсуждения влияния двух стратегий обучения на успеваемость и мотивацию. Исходя из результатов, некоторые результаты могут быть предоставлены соответствующим педагогам: это исследование показало, что на успеваемость не влияют приспособленность и пол, что согласуется с тем же выводом исследования .

По результатом исследования студентов Тайваня в экспериментальной группе, в которой учащиеся используют игровое обучение, успеваемость выше, чем до теста. Средняя мотивация составило 3,81> 3, что подчёркивает эффект обучения на основе игр с высокой мотивацией обучения. Экспериментальная группа демонстрирует более высокие достижения в обучении, чем контрольная группа. Этот результат показывает, что основанная на обучении система, очевидно, улучшает учебные достижения студентов. Что касается долгосрочного обучения, то применение системы обучения на основе игр в среде классной комнаты возможно и полезно.

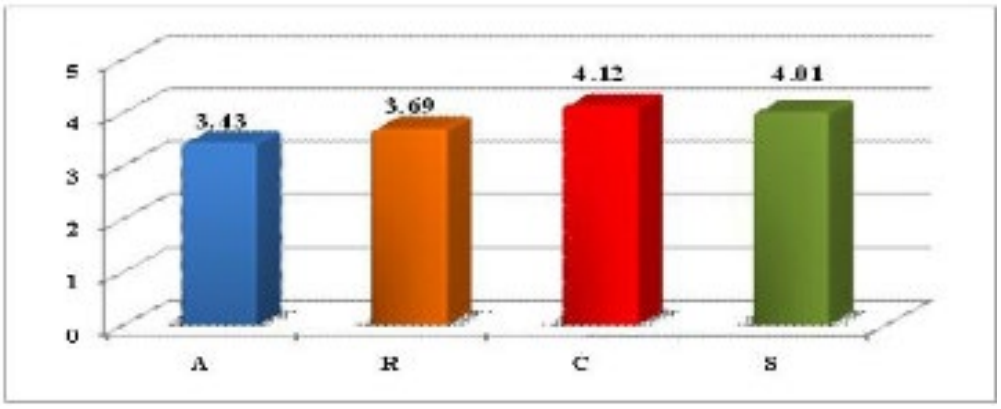


Рисунок – 6. Средний балл анкеты

На основе этого эксперимента можно смело заявить, что данный метод обучения надо и нужно применить в системе образования Казахстана. Одним из больших проблем является нехватка практического обучения студентов, чтобы дать возможность окунуться в сферу деятельности и понять все аспекты определённого предмета обучения. И в этом случае, такие игры могут способствовать решению данной проблемы, а также развивать в будущих специалистах мотивацию и интерес к обучению, так как данный метод может вовлечь игрока и увеличить его успеваемость.

Литература

1. Barendregt, W. & Bekker, T.M. (2011). Влияние уровня свободного выбора учебной деятельности на использование образовательной компьютерной игры. Компьютеры и образование, 56 (1), 80-90.

2. Шторм П. Быстрый, веселый и бесплатный игровой фреймворк с открытым исходным кодом HTML5, получено 22 июня 2016 г. с сайта http://phaser.io/.

УГРОЗЫ ИНФОРМАЦИОННОЙ (КИБЕР) БЕЗОПАСНОСТИ: ТЕРМИНОЛОГИЧЕСКИЙ АСПЕКТ

Жижимов В.В
e-mail: zhizhimov@mail.ru
Академия КНБ Республики Казахстан

Аннотация. *В статье рассматриваются угрозы информационной (кибер) безопасности и обосновывается необходимость согласования специальных терминов для организации всесторонней защиты объектов информатизации. Предложены определения терминам «киберугроза» и «уязвимость объекта информатизации», объясняющие их взаимосвязь.*

Ключевые слова: *информационно-коммуникационные технологии, электронные информационные ресурсы, объекты информатизации, термин, определение, кибербезопасность, киберугроза, уязвимость.*

Современные информационные технологии находят применение в различных сферах деятельности общества и предоставляют широкие возможности для улучшения всех аспектов жизнедеятельности человека.

Появление новых технологий дает возможность предоставлять услуги более высокого качества. Например, анализ потребностей населения с использованием технологий больших данных, может принципиально изменить сферу услуг и повысить качество обслуживания потребителей. С другой стороны, это создает проблемы, связанные с освоением новых информационно-коммуникационных технологий (далее – ИКТ) и безопасностью электронных информационных ресурсов. Относительная неизученность продуктов новых ИКТ, с учетом их качественного и количественного развития, предполагает наличие в них уязвимостей и, как следствие, появление новых угроз информационной безопасности.

Наиболее чувствительными в контексте угроз информационной безопасности являются объекты информатизации «электронного правительства» и критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ). В последние годы происходит резкий рост угроз информационной безопасности, направленных как на государственные информационные системы, так и на банковский и промышленный сектора.

На конференции по информационной безопасности SOC Day 2019 в г. Нур-Султан «Лаборатория Касперского» представила отчет об угрозах для систем промышленной автоматизации в Казахстане. В 36% случаев угроза компьютеру автоматизированных систем управления исходила именно из интернета – по этому показателю страна вошла в топ-15 государств, технологические компьютеры в которых чаще всего подвергались веб-атакам. Так, по данным представителя «Лаборатории Касперского» в Казахстане и Центральной Азии, ситуация с киберугрозами достаточно сложная, и если раньше мы

видели уязвимости корпоративных сетей и личных устройств, то злоумышленники, все чаще атакуют сложные индустриальные сети, ставя под угрозу стабильную работу КВОИКИ в нефтегазовой, энергетической, металлургической и иных отраслях [1].

Актуальность и важность темы защиты электронных информационных ресурсов и информационной инфраструктуры, подтверждается Глобальной программой кибербезопасности Международного союза электросвязи и Резолюцией Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования ИКТ и защиту от вредоносного воздействия программно-техническими методами [2, п.3].

Несмотря на наличие международных стандартов (ISO/IEC 27000), регламентирующих вопросы управления информационной безопасностью, термин «кибербезопасность» не имеет единого общепризнанного определения, в разных странах национальное понимание кибербезопасности значительно различается. Как следствие, различается и терминология в области кибербезопасности.

В Республике Казахстан под кибербезопасностью понимается состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации [2, п.1].

Такие распространенные угрозы кибербезопасности как эпидемии компьютерных вирусов, внедрение шпионских программ, воздействие вредоносных программных кодов и DoS/DDoS-атаки типа «отказ в обслуживании», являются также и угрозами информационной безопасности (угрозы безопасному, стабильному распространению информации и функционированию глобальных и национальных информационных инфраструктур), которые требуют принятия скоординированных и комплексных мер, осуществляемых как на национальном, так и на межгосударственном уровне.

В частности, в формате Организации Договора о коллективной безопасности имеется понимание, что компьютерные злоумышленники чаще всего не попадают под юрисдикцию государства, подвергшегося кибернападению. Преступники являются либо иностранцами, либо лицами без гражданства – «гражданами мира». Все это вынуждает искать общемировой консенсус в борьбе с угрозами и создавать общую систему информационной безопасности [3].

В этих условиях особое значение приобретает развитие партнерского взаимодействия и координация усилий в данной сфере. Республикой Казахстан уже достигнуты договоренности в области информационной безопасности в рамках Содружества Независимых Государств, Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества, включая перечень основных понятий в области обеспечения международной информационной безопасности [4]. Одним из важных моментов достигнутых договоренностей является совершенствование правовых подходов в области информационной безопасности. Большую роль в этом играет выбор применяемых терминов, их легитимное толкование и применение в различных нормативных правовых актах.

Несмотря на имеющиеся договоренности, существует многообразие подходов для понимания кибербезопасности, о чем в сообществе экспертов ведутся дискуссии. Исследователи в своих научных работах [5, 6] отмечают проблемы слабой

определенности понятийного аппарата в сфере кибербезопасности. При этом, заимствованные термины в области кибербезопасности часто имеют синонимы в области информационной безопасности, которым ранее уже были даны определения. Например, заимствованный термин «кибератака» соотносится с существующим термином «компьютерная атака», определенным в Концепции кибербезопасности [2]. Некоторые заимствованные термины применяются в нормативных правовых актах без определений (например, «киберзащита»). Зачастую предлагаются специализированные подходы к определению кибер-термина в зависимости от рассматриваемой сферы деятельности (политическая, военная, экономическая). Следовательно, проблема определения кибер-терминов является актуальной, необходимо выработать единые определения для того, чтобы избежать двусмысленности или неопределенности при их использовании.

Также, не существует единого общепризнанного определения терминов «киберугроза» и «уязвимость объекта информатизации». С учетом определения кибербезопасности в национальном законодательстве, термин «киберугроза» может рассматриваться как угроза информационной безопасности в сфере информатизации. Под угрозой информационной безопасности в Концепции кибербезопасности [2] понимается потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или компоненты информационной системы или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей.

Используя понятийный аппарат Закона Республики Казахстан «Об информатизации» [7], предлагается адаптированное определение: *Угроза информационной безопасности - потенциально возможное событие, процесс или явление, которые посредством воздействия на электронный информационный ресурс, объекты информационно-коммуникационной инфраструктуры могут прямо или косвенно привести к нанесению ущерба интересам субъектов информатизации.*

В настоящее время в Республике Казахстан в рамках мониторинга обеспечения защиты объектов информатизации "электронного правительства" и КВОИКИ в порядке определенным Правилами [8], проводится обследование данных объектов на предмет наличия уязвимостей, под которыми понимаются недостатки в программном или аппаратном обеспечении, обуславливающие возможность нарушения их работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном или аппаратном обеспечении.

Более широкое определение термина «Уязвимость (vulnerability) - слабость актива или контроля, которая может быть использована одной или несколькими угрозами» используется в стандарте СТ РК ISO/IEC 27000 [9]. Действительно, несвоевременное выявление и устранение уязвимостей объекта информатизации увеличивает угрозы информационной безопасности. В связи с чем, предлагается новое определение: *Уязвимость объекта информатизации - внутренние свойства электронных информационных ресурсов, программного обеспечения, информационно-коммуникационной инфраструктуры, которые могут быть использованы угрозой информационной безопасности.*

Предлагаемое определение позволяет установить взаимосвязь между терминами *«Уязвимость объекта информатизации»* и *«Киберугроза» (угроза информационной безопасности в сфере информатизации)*, что в целом соответствует международному опыту, накопленному в области менеджмента информационной безопасности.

В дальнейшем, представляется целесообразным продолжить исследования кибер-терминов для гармонизации их с терминологией в сфере информационной безопасности.

Литература

1. Казахстан вошел в топ-15 стран по веб-атакам на технологические компьютеры. - https://profit.kz/news/53178/Kazahstan-voshel-v-top-15-stran-po-veb-atakam-na-tehnologicheskie-komputeri (Дата доступа: 18.12.2019);
2. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 Об утверждении Концепции кибербезопасности («Киберщит Казахстана»);
3. Кунакбаев М.Ж. Об отдельных аспектах и коллективных мерах, принимаемых в формате ОДКБ в сфере информационной безопасности. – Минск: ИНБ, Материалы международной научно-практической конференции. Т1, 2019.
4. Закон Республики Казахстан от 1 июня 2010 года № 286-IV «О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности».
5. Татаринова Л.Ф. Соотношение понятий «информационная безопасность», «защита информации» и «кибербезопасность», «киберзащита» по законодательству Республики Казахстан. – Алматы, Вестник КазНУ, 2013г. - https://articlekz.com/article/15106 (Дата доступа: 18.12.2019);
6. Добринская Д.Е. Киберпространство: территория современной жизни. Вестник Московского Университета. Сер.18. Социология и политология. 2018. Т.24. №1, с52-67 - https://vestnik.socio.msu.ru/jour/article/view/363 (Дата доступа: 18.12.2019);
7. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;
8. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 13 августа 2019 года № 195/НҚ. О внесении изменения в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры»;
9. СТ РК ISO/IEC 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь».

ТОЛКОВАНИЕ КРИПТОГРАФИЧЕСКИХ ТЕРМИНОВ ПОНЯТИЯ «ШИФРОВАННАЯ СВЯЗЬ» В РЕСПУБЛИКЕ КАЗАХСТАН

Исакова С.У.
e-mail: s7665548@mail.com
Академия КНБ Республики Казахстан

Аннотация. *В данной статье рассматривается актуальность и необходимость совершенствования понятийного аппарата и единого толкования криптографических*

терминов в государственных органах Республики Казахстан в сфере защиты информации. Проанализированы некоторые криптографические термины. При анализе в основу были положены устоявшиеся в криптографической литературе толкования терминов и понятий, определения в существующих стандартах (в том числе зарубежных) и НПА Республики Казахстан в сфере защиты информации.

Ключевые слова: *защита информации, криптография, шифровальная машина, ручные шифры, специальная вычислительная техника, аппаратура линейного шифрования, шифрование, специальный, шифрованный.*

В настоящее время информация стала одним из основных ресурсов развития общества. Развитие информационных технологий (информатизация общества) ведет к созданию единого мирового информационного пространства, происходит постоянная гонка вооружений в информационном мире, увеличивается количество угроз, а соответственно развиваются методы и средства защиты информации.

К одним из методов защиты информации относится, и наука «Криптография», на основе которой разрабатываются и средства криптографической защиты информации (далее – СКЗИ).

Ядром любой науки является категориально-понятийный аппарат. Кроме того, одним из условий корректной реализации СКЗИ является четкая постановка (формулировка) задачи, единое понимание понятий и терминов сторонами (Исполнитель и Заказчик), что исключает неоднозначность толкования (понимания) предназначенных СКЗИ целей и функций.

На сегодняшний день область использования криптографических терминов увеличилась. Существенное расширение предмета исследований и круга исследователей стало источником появления в криптографии новых понятий и терминов, используемых в научных публикациях и в докладах на конференциях. Многие публикации по криптографии на русском языке появляются как переводы или обзоры англоязычной литературы. При этом не всегда имеет место адекватный перевод понятий, допускаются терминологические неточности, порой проявляется недостаточное знание соответствующей предметной области. Причиной данной проблемы является многозначность перевода терминов, т.е. основная трудность заключается не столько в переводе терминов, сколько в их идентификации, так как без достаточного владения языком математических, информационных, криптографических реалий невозможно выполнить точный и правильный перевод [1].

Следует учитывать, что тексты с криптографической спецификой, как и любой текст научно-технического жанра, насыщен терминами и терминологическими сочетаниями, которые являются основной нагрузкой текста, очень информативны и часто бывают ключевыми словами.

Отметим, что проблема исследования терминологии является одной из ключевых в исследованиях научно-технических тестов. Даже в родственных языках присутствуют несовпадения, и присутствует опасность изменения смысла текста при использовании неправильного варианта терминологического перевода. Из-за отсутствия привычных соответствий криптографических терминов возникают сложности при переводе.

Отсюда вытекает недопонимание некоторых теоретических положений, современных способов построения и анализа криптографических алгоритмов и т.д. Это, вместе с отсутствием постоянных курсов повышения квалификации (их физическое отсутствие, отсутствие финансирования и т.д.) ведет к недостаточной квалификации, что

в свою очередь ведет к низкой научно-исследовательской работе, недостаточной детальной проработке и выполнению требований и технических характеристик опытно-конструкторских разработок средств криптографической защиты информации.

Анализ проблем «корректного» перевода и использования криптографических терминов показал, что один и тот же термин может по-разному трактоваться в различных открытых источниках информации (статьи, доклады, книги, пособия и т.д.). Причем проблемы начинаются на уровне основных терминов: криптография, шифр, дешифрование и т.д.

Так, термин «криптография» по-разному определяется в следующих документах:

−словарь криптографических терминов под редакцией Погорелова Б.А. и Сачкова В.Н. [1];

−контрразведывательный словарь высшей краснознаменной школы Комитета государственной безопасности при Совете Министров СССР имени Ф.Э.Дзержинского [2];

−учебное пособие «Основы криптографии» Алферова А. П., Зубова А. Ю., Кузьмина А. С., Черемушкина А. В. [3].

Необходимость выработки общепринятого понимания основных понятий в данной области назрела давно, работы по систематизации криптографической терминологии ведутся (в частности, Академией криптографии РФ и Московским государственным университетом), однако решение этой задачи связано с большими трудностями в силу необходимости учета многочисленных нюансов, связанных с использованием сходной терминологии для многообразия конкретных областей применения криптографии, каждая их которых обладает своей спецификой [4].

Вышеизложенное свидетельствует о том, что проблема до сих пор не решена.

Теоретические и эмпирические исследования в рамках поиска однозначного толкования криптографических терминов позволят решить ряд актуальных задач:

- повысить достоверность и актуальность сведений из области мировых достижений криптографии для решения поставленных задач;

- способствовать эффективному взаимодействию подразделений государственных органов в области защиты информации;

- повысить эффективность проведения научных исследований и разработок в области криптографии (в том числе средств криптографической защиты информации).

Кроме того, во исполнение Послания первого Президента Республики Казахстан от 10 января 2018 года ввод единого толкования криптотерминов позволит:

- свободно владеть криптографическими терминами на английском, русском и казахском языках как одним из факторов перехода на трехъязычное обучение;

- интегрироваться в мировую научно-исследовательскую среду;

- пересмотреть подходы к обоснованности существующих переводов и терминологически приблизить государственный язык к международному уровню.

До настоящего времени разработка понятий и унификация терминов криптографии, используемых в государственных органах Республики Казахстан, не проводилась.

Так, в Законе Республики Казахстан «О связи» дано определение понятия шифрованной связи:

Шифрованная связь - защищенная связь с использованием ручных шифров, шифровальных машин, аппаратуры линейного шифрования и специальных средств вычислительной техники [5].

Однако, здесь понятия «Ручные шифры», «Шифровальная машина», «Аппаратура линейного шифрования», «Специальные средства вычислительной техники» в открытых нормативно-правовых актах не определены, что может привести к неоднозначному пониманию определения шифрованной связи.

В этой связи автором предлагаются следующие варианты толкования этих терминов.

Ручные шифры – это шифры, в которых шифрование и расшифрование информации может выполняться вручную или с применением простейших (не технических) приспособлений.

Шифровальная машина – аппаратура для шифрования (расшифрования) информации по алгоритму, определяемым ключом. Шифрование осуществляется путем автоматического преобразования, вводимого в машину открытого текста в случайную последовательность букв или цифр, расшифрование – на том же ключе, который использовался при шифровании.

Аппаратура линейного шифрования – шифровальная машина, в которой процессы шифрования и расшифровывания информации производятся непосредственно в процессе передачи (приема) информации по каналу связи.

Специальные средства вычислительной техники – разработанная для специалистов отдельной отрасли науки и техники (узкого профиля) совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем для решения задач особого назначения.

Данные толкования выработаны в результате анализа определений составляющих понятий из открытых источников [6]- [14] и из существующих стандартов Республики Казахстан в сфере защиты информации [15], [16].

Отметим, что в связи с большим количеством определений рассматриваемых понятий в рамках настоящего исследования отобраны те сущности, которые учитывают специфику области применения –криптографию.

Анализ понятий проводился в соответствии со стандартом ГОСТ Р ИСО 704-2010. «Терминологическая работа. Принципы и методы» [17]. Результаты могут быть использованы как практической деятельности государственных органов в сфере защиты информации, так и в учебных учреждениях Республики Казахстан.

Литература

1. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. – М.:МЦНМО, 2006.

2. Контрразведывательный словарь/ Каленская Л.В., Смирнов Ю.И. – научно-издательский отдел Высшей Краснознаменной школы КГБ при Совете Министров СССР имени Ф.Э.Дзержинского, 1972.

3. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – М.: "Гелиос АРВ", 2002.

4. Погорелов Б.А., Черемушкин А.В., Чечета С.И. К вопросу о терминологии, используемой в криптографии. Вестник Томского университета. Приложение. Материалы научных конференций, симпозиумов, школ, проводимых в ТГУ. 2003, № 6, 53-57.

5. Закон Республики Казахстан от 5 июля 2004 года № 567-II «О связи».

6. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. –М.: ИТИ Технологии, 2006.

7. Ефремова Т.Ф. Новый словарь русского языка. Толково-словообразовательный. -М.: Русский язык, 2000.

8. Большой энциклопедический словарь/под ред. А.Прохорова. – М.: Большая Российская энциклопедия, Норинт, 2000.

9. Большая политехническая энциклопедия. - М.: Мир и образование. Рязанцев В.Д., 2011.

10. Энциклопедия «Техника». — М.: Росмэн. 2006.

11. Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. 2000.

12. Толковый словарь русского языка/ под ред. Д.В.Дмитриева. –М.: Астрель: АСТ, 2003.

13. Словарь русского языка: в 4-х т./РАН, Ин-т лингвистич. исследований/ под. ред.А.П.Евгеньевой. -4 изд., стер.-М.: Рус.яз.; Полиграфресурсы, 1999.

14. Толковый словарь русского языка/ под ред. Д.Н.Ушакова (1935-1940). –М.: Lingua, 2010.

15. СТ РК ГОСТ 1695-2007. Информационная безопасность. Аттестация объектов информатизации и средств вычислительной техники. Общие требования

16. СТ РК ГОСТ Р 50739-2006. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

17. ГОСТ Р ИСО 704-2010. Терминологическая работа. Принципы и методы.

КОНЦЕПТУАЛЬНЫЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ ОЦЕНКИ (ПОДТВЕРЖДЕНИЯ) СООТВЕТСТВИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Исмаил Е.Е.
e-mail: ismaile@mail.ru
Алматинский университет энергетики и связи им. Г. Даукеева, Казахстан

Аннотация. *Рассмотрен подход и основные принципы организации оценки (подтверждения) соответствия в области информационной безопасности в соответствие с требованиями законодательства Республики Казахстан по техническому регулированию. Системно изложены основные понятия и принципы оценки (подтверждения) соответствия требованиям информационной безопасности. Даны рекомендации по созданию в Республике Казахстан системы оценки (подтверждения) соответствия в области информационной безопасности и необходимой нормативно-методической базы.*

Активное развитие информационных технологий, рост сложности современных информационных систем, возрастающая зависимость критически важных систем от безопасности информации, расширение угроз информационной безопасности определили актуальность вопросов оценки (подтверждения) соответствия заданным

требованиям информационной безопасности, в том числе создания систем сертификации.

1. Основные принципы оценки соответствия

Деятельность в области оценки (подтверждения) соответствия основывается на положениях и требованиях действующих законов, технических регламентов, стандартов, нормативных технических и методических документов.

В Республике Казахстан деятельность в области оценки (подтверждения) соответствия в Республике Казахстан регулируется законом «О техническом регулировании» [1].

Современное техническое регулирование, под которым понимается правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или связанным с требованиями к продукции процессам, а также в области оценки соответствия [1], основывается на следующих основных принципах:

1) создания единой и целостностной государственной системы технического регулирования;

2) установления единых обязательных требований в технических регламентах;

3) применения единых и правил установления требований к продукции, услуге, процессами.

Одним из основных элементов государственной системы технического регулирования Республики Казахстан является система оценки (подтверждения) соответствия требованиям, предъявляемых к объекту (продукции, процессу, услуге), сертификация же рассматривается как одна из форм оценки (подтверждения) соответствия.

Под «оценкой соответствия» (assessment of conformance) понимается любая деятельность, связанная с прямым или косвенным определением того, что предъявляемые к объекту оценки соответствия требования выполняются [2,3]. Это понятие обобщает разные виды деятельности и формы оценки соответствия.

Под формой оценки соответствия понимается определенный порядок удостоверения соответствия объектов установленным требованиям. Форма подтверждения соответствия устанавливает совокупность действий, результаты которых рассматриваются в качестве доказательств соответствия объекта требованиям, установленным техническими регламентами, стандартами или договорами.

Целью всех форм оценки соответствия является установление соответствия объекта предъявляемым требованиям. Но способы и методы проведения оценки отличаются для разных форм и объектов оценки соответствия.

В оценке соответствия участвуют три стороны: первая сторона представляет интересы поставщиков; вторая сторона покупателей; третья сторона лицо или орган, признаваемые независимыми от участвующих в рассматриваемом вопросе.

Важнейшей формой оценки соответствия является подтверждение соответствия (attestation, conformation of conformance). В Законе Республике Казахстан «О техническом регулировании», в основном, используется понятие «подтверждение соответствия», определяемое, как процедура, результатом которой является документальное удостоверение соответствия объекта требованиям, установленным техническими регламентами, стандартами, или условиям договоров [1].

Подтверждение соответствия может носить обязательный или добровольный характер. Обязательное подтверждение соответствия - процедура, посредством которой

осуществляется подтверждение соответствия объекта требованиям, установленным техническими регламентами.

Одним из основных принципов оценки соответствия является функциональный подход, заключающийся в представлении деятельности по оценке соответствия, как последовательности трех основных функций: «выбора» (selection), «определения» (determination) и «итоговая проверка и подтверждения соответствия» (review and attestation) [2].

Функция выбора предусматривает планирование и подготовку действий для сбора или представления всей информации, являющейся входными данными для следующей функции – определения.

К действиям в процессе реализации функции выбора может быть отнесено:

- выбор объекта оценки соответствия;
- выбор документов, устанавливающих требования к объекту оценки соответствия;
- выбор методов, программы и методик испытаний;
- выбор перечня документов, изучаемых при реализации функции определения;
- выбор или установление правил принятия решений о соответствии (несоответствии) требованиям при реализации функции проверки и подтверждения соответствия.

Основной целью *функции определения* является получение полной информации о выполнении заданных требований объектом оценки соответствия.

Действия по определению предпринимаются с целью получения полной информации о выполнении заданных требований объектом оценки соответствия

К действиям в процессе реализации функции определения может быть отнесено:

- испытания (testing) объектов отобранных в процессе реализации функции выбора. Стандарт ГОСТ ISO/IEC 17000 определяет испытания как «определение одной или более характеристик объекта оценки соответствия согласно установленному способу осуществления».
- инспекция (inspection) объектов с целью определения их соответствия заданным требованиям или на основе профессионального суждения общим требованиям;
- аудит (audit) - «систематический, независимый, и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания с целью установления степени выполнения заданных требований»;
- изучение документов (например, результаты межлабораторных сравнительных испытаний, проектной документации, инструкций по эксплуатации и т.п.).

Функция итоговой проверки и подтверждения соответствия предусматривает на базе полученной информации об объекте оценки соответствия, в соответствии с заранее установленными (на стадии выбора) правилами, принятие решения о соответствии объекта установленным требованиям. Функция включает в себя проверку (review) и собственно подтверждение соответствия (attestation). Смысл проверки (review) заключается в том, что перед подтверждением соответствия необходимо проанализировать полученную на стадии определения информацию и убедиться в том, что она достаточна и непротиворечива. Если полученная информация позволяет принять решение, то проводится подтверждение соответствия, т.е. выдача документа о том, что выполнение заданных требований продемонстрировано (или не продемонстрировано). В случае, когда на основе полученной информации невозможно сделать обоснованного вывода, то следует вернуться к функции выбора, пересмотреть принятые в ходе

реализации этой функции решения, и при необходимости повторить функцию определения, то есть получить новую, или уточнённую, или дополнительную информацию, достаточную для подтверждения соответствия.

Ещё одной дополнительной функцией в деятельности по оценке соответствия является *инспекционный контроль*. Объекты оценки соответствия могут менять свои характеристики во времени, во времени могут меняться потребности потребителя или измерительные возможности, поэтому может потребоваться периодическое повторение процедуры оценки соответствия (полностью или частично).

2. Основные задачи создания системы оценки (подтверждения) соответствия в области информационной безопасности

В соответствии со сложившейся международной практикой оценка соответствия производится в той или иной системе оценки соответствия, представляющую собой организационно-техническую систему, состоящую из совокупности объектов оценки соответствия, комплекса норм, правил, методов, процедур, органов и ресурсов для осуществления процесса оценки соответствия закрепленных объектов установленным требования.

Система оценки соответствия должна создаваться для совокупности объектов оценки соответствия, обладающей определенной общностью (функциональное назначение, принципы работы (применения), методы контроля и испытаний и т. д.), с учетом их особенностей.

Система сертификации является частным случаем системы оценки соответствия и включат в себя совокупность закрепленных объектов сертификации, комплекса норм, правил, процедур и ресурсов для выполнения работ по сертификации, независимого органа сертификации, правил функционирования и системы управления, которые в совокупности обеспечивают сертификацию закрепленных объектов.

Анализ практики создания различных систем сертификации позволяет предложить основные принципы создания системы сертификации в области информационной безопасности, которые можно сформулировать следующим образом:

1) *принцип системности,* который заключается в следующем:

- создание системы сертификации для совокупности объектов, обладающей определенной общностью (функциональное назначение, принципы работы (применения), методы контроля и испытаний и т. д.), с учетом их особенностей;
- обеспечение полноты функций системы сертификации в соответствии с международными требованиями, а также полноты тестирования объектов;
- обеспечение полноты охвата объектов сертификации в заданной области и их элементов;
- обеспечение полноты охвата нормативными документами объектов сертификации;
- достаточность набора регламентированных требований, процедур, схем сертификации с учетом категории безопасности оцениваемых объектов;
- обеспечение полноты охвата регламентированных требований к объектам сертификации аттестованными методиками испытаний.

2) *принцип достоверности результатов*: поскольку абсолютной уверенности в соответствии сертифицированных объектов предъявляемым требованиям не может быть из-за стохастического характера контролируемых свойств и результатов контроля, при сертификации приходится полагаться на правильное использование вероятностных

механизмов при получении и использовании результатов испытаний. Для обеспечения практической уверенности в достоверности конечной оценки объекта сертификации рекомендуется использовать разные методы;

3) принцип достаточности требований: для того чтобы объект был действительно безопасен, при сертификации необходимо контролировать все свойства, которые по отдельности или в комплексе могут представлять значимую угрозу;

4) принцип контролепригодности требований: все требования безопасности, проверяемые в ходе сертификации, должны задаваться настолько определенно, чтобы их можно было объективно проверить;

5) принцип нормативной определенности: все процедуры процесса сертификации должны быть регламентированы нормативными документами системы.

Для практического создания системы оценки (подтверждения) соответствия (системы сертификации) в области информационной безопасности должен быть решен ряд важных задач, к числу которых относятся:

1) создание и аккредитация специализированных органов подтверждение соответствия (сертификации) по видам однородных объектов;

2) создание, оснащение и аккредитация специализированных испытательных лабораторий, для проведения исследований, испытаний объектов оценки соответствия для в пределах своей области аккредитации (конкретные объекты и виды испытаний);

3) определение номенклатуры обязательных требований и показателей информационной безопасности и разработка соответствующих технических регламентов и взаимосвязанных стандартов, обеспечивающих выполнение требований, установленных техническими регламентами;

4) подготовка и аттестация экспертов-аудиторов по подтверждению соответствия в области информационной безопасности;

5) разработка стандартов, других нормативных технических и методических документов, необходимых для сертификации в области информационной безопасности;

6) разработка и реализация стандартизированных методов испытаний различных объектов по требованиям информационной безопасности;

7) реализация методов и средств испытаний для достоверного определения заданных показателей безопасности, воспроизведения условий эксплуатации, автоматизация процессов сертификации.

3. Создание нормативно-методической базы оценки соответствия требованиям информационной безопасности

Основными задачами нормативно-методической базы оценки соответствия являются регламентация:

- обязательных требований к объектам оценки соответствия требованиям информационной безопасности;
- общего порядка, правил, состава и содержания процедур процессов оценки соответствия требованиям информационной безопасности;
- методик, обеспечивающих участникам оценки соответствия возможность использовать наиболее эффективные приемы и методы работы, выполнять их по единой схеме и получать единообразные результаты;
- состава и форм технической, методической, отчетной документации.

Нормативно-методическая база оценки соответствия требованиям информационной безопасности должна создаваться в соответствии с требованиями

государственной системы технического регулирования Республики Казахстан, основных правил и процедура подтверждения и иных требования, необходимых для реализации целей подтверждения соответствия (сертификации) в области информационной безопасности.

Нормативно-методическая база оценки соответствия в области информационной безопасности должна создаваться на основе гармонизации с международными стандартами.

Структура нормативно-методической базы оценки соответствия в области информационной безопасности должна включать [4]:

- базовые нормативные документы;
- обеспечивающие нормативные документы;
- методические документы.

Базовые нормативные документы определяют:

- методологические подход к оценке соответствия требованиям информационной безопасности;
- обязательные требования и критерии их оценки на уровне технических регламентов и взаимосвязанных с ними международных, межгосударственных и национальных стандартов;
- общий порядок оценки соответствия требованиям информационной безопасности;
- требования к органам оценки (подтверждения) соответствия;
- участников оценки соответствия и распределение ответственности между ними.

Обеспечивающие нормативные документы регламентируют следующие основные вопросы:

- категорирование объектов оценки соответствия с учетом критичности выполняемых функций, важности обрабатываемой информации;
- формирование наборов требований безопасности и показателей для их количественной оценки;
- методы и процедуры проведения оценки соответствия объекта заданным требованиям безопасности;
- роли и обязанности участников оценки соответствия и др.

Методические документы включают модели, руководства, методики, позволяющие эффективно выполнять процедуры оценки соответствия и обеспечивать требования к условиям проведения и результатам проведения оценки соответствия.

Для совершенствования и развития существующей нормативно-методической базы оценки соответствия требованиям информационной безопасности, необходимо решение следующих первоочередных задач:

- четкая структуризация, дифференциация, формализация и регламентация требований к информационной безопасности;
- создание четкой системы критериев оценки информационной безопасности, охватывающей установленные категории систем, уровни ценности защищаемых активов, состав угроз информационной безопасности и условий функционирования;
- установление общей методологии и формализованных процедур выполнения работ по оценке соответствия требованиям информационной безопасности;
- четкая регламентация организационных и процедурных основ оценки соответствия требованиям информационной безопасности (видов работ на различных этапах жизненного цикла, состава и структуры составляемых документов и др.);

- регламентация и развитие форм, методов и технологий оценки соответствия требованиям информационной безопасности;
- установление требований к обеспечению объективности, достоверности, повторяемости и воспроизводимости результатов оценки соответствия требованиям информационной безопасности.

Заключение

Предложенные в работе рекомендации направлены на создание концептуальных, методических и организационных основ, нормативно-методической базы создания в Республике Казахстан системы оценки (подтверждения) соответствия в области информационной безопасности с использованием современных требований международных стандартов и передового зарубежного опыта.

Литература

1. Закон Республики Казахстан от 9 ноября 2004 года № 603-II «О техническом регулировании» (с изменениями и дополнениями по состоянию на 16.04.2019 г.).
2. ГОСТ ISO/IEC 17000-2012 Оценка соответствия. Словарь и общие принципы [Текст]. – Введ. 2013-09-01. – М.: Стандартинформ, 2014
3. Договор о Евразийском экономическом союзе (Раздел X Техническое регулирование, приложение № 9 Протокол о техническом регулировании в рамках ЕАЭС), 2014.
4. Руководящий документ «Безопасность информационных технологий». Концепция оценки соответствия автоматизированных систем требованиям безопасности информации (проект, первая редакция). – ФСТЭК России, 2004

УРОВНИ ОПРЕДЕЛЕНИЯ МОДЕЛИ ТИПИЗИРОВАННОГО АТРИБУТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Калимолдаев М.Н., Бияшев Р.Г., Рог О.А.
e-mail: mnk@ipic.kz , brg@ipic.kz, olga@ipic.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Рассмотрены применяемые в настоящее время модели разграничения доступа. Приведены их достоинства и недостатки. Описана разрабатываема модель типизированного атрибутного разграничения доступа. Показано, что она отвечает сформулированным требованиям безопасности. Предложена методика разработки ее архитектуры путем абстракции и разграничения полномочий, что дает основу для программной реализации модели. Основные операции предлагаемой техники абстракций - операции абстрагирования и конкретизации - непосредственно представляются операторами непротиворечивой системы λ-исчисления, которая строится в качестве прототипа программ на языках функционального программирования для реализации моделей ТАРД.*

1. Введение

В настоящее время информационные ресурсы, размещаемые в высокопроизводительных вычислительных средах, предоставляются широкому кругу пользователей в режиме коллективного доступа. При этом необходима правильная организация использования правил политик авторизации, определяющих допуск к ресурсам определенных видов различным пользователям согласно предоставленным полномочиям с одновременным запретом различных видов несанкционированного доступа.

Средства контроля доступа, используемые большинством приложений, как правило, обладают большой сложностью и требуют применения особых методов, облегчающих их разработку и эксплуатацию. В связи с этим возникает вопрос создания архитектур моделей путем абстракции и разграничения полномочий. С точки зрения пользователей программной архитектуры такой подход дает возможность решать задачи, связанные с их различными специализациями или ролями, что дает возможность создавать надежные средства защиты разнородных источников информации для пользователей разных категорий.

Далее приводится описание существующих моделей разграничения доступа, их достоинств и недостатков в сравнении с разрабатываемой моделью типизированного атрибутного разграничения доступа (ТАРД), в которой применяются указанные принципы построения архитектуры, делающие модель надежной и простой в использовании.

Основные модели разграничения доступа. Их недостатки. Требования к вновь создаваемым моделям. Среди многочисленных моделей разграничения доступа, разработанных с начала 70-х годов, основными являются модели дискреционного разграничения доступа DAC (Discretional Access Control), мандатного разграничения доступа MAC (Mandatory Access Control) и ролевого разграничения доступа RBAC (Role Based Access Control), безопасность защищаемых которыми информационных ресурсов, признается недостаточной [1-3].

Идентификация сущностей в этих моделях, называемых идентификаторными, выполняется путем присвоения субъектам и объектам уникальных имен, ввиду чего доступ субъекта к объекту осуществляется на основе проверки имен или приписанных им ролей. При этом не учитываются дополнительные параметры, что ведет к «грубому» разграничению доступа («coarse-grained access control») и служит причиной появления «избыточности прав доступа» у пользователей. Возникает необходимость решения вопросов идентификации путем обеспечения наименований, отражающих все характеристики сущностей.

Следующим недостатком является невозможность применения интегрированных политик разграничения доступа. Единственной политики безопасности, предоставляемой традиционными моделями, недостаточно для защиты данных в сложных системах, требующих одновременного выполнения нескольких критериев защиты. В связи с этим необходимо введение новой парадигмы – «множественной политики», требующей чтобы в системе была предусмотрена возможность последовательного или одновременного применения разных политик авторизации в зависимости от требований безопасности конкретной среды.

Система должна обладать средствами конструирования различных политик без реконфигурации самой системы, что позволяет создавать и применять политики для разграничения доступа по различным признакам, делая защиту многокритериальной.

Система также должна содержать средства администрирования полномочий для обеспечения возможности управления правами большого числа пользователей и машин.

Для решения перечисленных проблем был предложен атрибутный метод разграничения доступа (Attribute Based Access Control, ABAC) [4-6, 14]. Его основу составляет безидентификаторный подход, который заключается в обозначении субъектов и объектов наборами атрибутов и позволяющий принимать решение по управлению доступом без предварительного знания субъектов или их отношения к поставщику услуг. Политика авторизации предоставляет группам пользователей определенные виды доступа к заданным объектам на основе оценки значений их атрибутов.

Преимущество ABAC состоит в том, что оно позволяет создавать политики доступа на основе атрибутов пользователей и объектов, а не назначать роли, права собственности или метки безопасности вручную системным администратором. Это упрощает администрирование, устраняя необходимость ручного вмешательства при авторизации, а также создавая возможность автоматизации решения по управлению доступом для удаленных пользователей из других доменов.

Система именования сущностей атрибутами обеспечивает «точное» разграничение доступа («fine-grained access control»), не допуская избыточных прав доступа.

Языки спецификации моделей ABAC дают гибкость и выразительную мощность описаниям политик безопасности. При этом многие из них разрешают моделировать традиционные методы разграничения доступа – DAC, MAC, RBAC.

Преимущество данного подхода для представления атрибутных политик разграничения доступа заключается в его простоте и легкости использования. Создание новых правил, способных гибко и в сжатой форме описывать сложные политики, не представляет трудностей.

Недостатком ABAC является то, что создание выразительных вычислительных языков для спецификации атрибутных правил разграничения доступа делает задачи вычисления значений разнородных атрибутов в процессе конструирования и выполнения политик NP-полными или даже неразрешимыми. Также, отсутствие формальных определений и сложность администрирования препятствуют широкому применению моделей ABAC.

В данной статье приводится описание разрабатываемой авторами модели типизированного атрибутного разраничения доступа (ТАРД), отвечающей перечисленным требованиям к безопасности и обладающей следующими характеристиками:

- обеспечение высокой скорости вычисления на основе принципа обработки атрибутов одинаковых типов;
- возможность формального доказательства правильности решений о предоставлении доступа;
- обеспечение наглядности и контроля процесса администрирования;
- способность динамически конструировать новые модели разграничения доступа вместе с возможностью моделирования традиционных DAC, MAC, RBAC;
- модель непосредственно реализуема на языках функционального и логического программирования.

Предложена методика представления модели в виде уровней абстракции, как средства управления сложностью ее конструирования и функционирования, а также инструмента ее программной реализации.

2. MTARD как тип атрибутов безопасности

Разрабатываемая модель типизированного атрибутного разграничения доступа обеспечивает безопасное совместное использование информационных ресурсов и отвечает требованиям универсальности и гибкости управления безопасностью [7-15].

Модель предоставляет следующие возможности:

- идентификация сущностей группами признаков (атрибутов), исключающая избыточность прав доступа;
- предоставление средств динамического конструирования политик;
- использование множественных политик в рамках одной системы.

Модель TARD принадлежит классу моделей ABAC, но, в отличие от ABAC, атрибуты безопасности сущностей TARD типизированы.

Каждая сущность e в TARD идентифицируется одним или несколькими атрибутами:

$$e{:}T_i,\ i{=}\overline{1,N},$$

имеющими значения, принадлежащие независимым типам T_i. Решение о возможности доступа принимается на основе обработки однотипных атрибутов пары субъект-объект.

Модель TARD определяется как кортеж независимых типов

$$T = (T_i),\ i{=}\overline{1,N}.$$

Тип T_i представляющий собой математический объект, включает структурированный домен значений вместе с заданными на нем операциями. Он является механизмом, реализующим политику разграничения доступа в соответствии с определенным критерием. Тип служит ограничением на значения атрибутов и круг операций с атрибутами данного типа, что составляет основу принципа безопасности моделей TARD.

Формально тип определяется следующим образом:

$$T = (Dom,\ Op),$$

где *Dom* –структурированный домен:

$$Dom = (D,\ \sqsubseteq_{Str}).$$

D - полное частично упорядоченное отношением предшествования $\sqsubseteq$ множество названий всевозможных операций и их групп, разрешаемых субъектам для выполнения над объектами после получения доступа, и сгруппированных в соответствии с выбранной структурой домена $\sqsubseteq_{Str}$.

Str = (Set, List, Tree) означает вид структуры*: Set* - «множество», *List* - «список», *Tree* - «дерево». Спецификация политики безопасности *P(T)* задается конкретным видом структуры Str и значениями узлов домена типа *T* а также видом соответствующих данной структуре операций. Структура *Set* может быть использована для моделирования политик DAC, *List* – для политик MAC, а *Tree* – для политик RBAC.

Набор Op включает операцию типизации Type и операцию доступа Acc:

$$Op = (Type, Acc),$$

Операция типизации $Type(e) = e: T$ присваивает сущности e атрибут типа T в виде ее метки безопасности, имеющей вид некоторого элемента домена или структурированного подмножества узлов, подчиненных данному элементу.

Множественная метка безопасности сущности e в виде кортежа $(e: T_1, \ldots, e: T_K)$ присваивается в результате применения операций типизации независимых типов $T_1, \ldots, T_K$.

Метки безопасности субъекта содержат информацию о названиях разрешенных ему операций. В свою очередь, метки безопасности объекта содержат сведения об операциях, которые можно производить над данным объектом.

Операция доступа Acc сравнивает метки безопасности субъекта и объекта одинаковых типов, устанавливая факт наличия отношения $\sqsubseteq$ между ними, и разрешает/отвергает доступ субъекта к объекту:

$$Acc(Type(s), Type\ (o)) = true/false.$$

Множество семантических значений модели ТАРД содержит метки безопасности субъектов и объектов, а также результатов их сравнения на разных стадиях ее функционирования.

Механизм разграничения доступа по критерию, задаваемому типом T, можно представить в обобщенном виде следующим образом: $Acc(Type(s), Type(o)) = true$, если выполняется $Type(o) \sqsubseteq Type(s)$, и $false$ во всех остальных случаях.

Одновременное выполнение критериев всех типов T_i атрибутов пары субъект-объект после выдачи субъектом s запроса на доступ к объекту o

$$Acc(Type^i(s), Type^i(o)) = true\ ,\ i=\overline{1,K}$$

обеспечивает многокритериальное разграничение доступа, реализуя таким образом парадигму «множественной политики».

3. Уровни абстрактного представления и процесс функционирования модели ТАРД.

Абстракция является процессом удаления физических, пространственных или временных деталей или атрибутов объектов с целью фокусирования внимания на наиболее важных деталях. В результате создаются объекты, отражающие общие атрибуты различных конкретных сущностей.

Для представления абстракций применяются типы данных, подвергающиеся абстрагированию. В рассматриваемой модели ТАРД объектом абстрагирования является тип атрибутов разграничения доступа.

Конкретизация – это процесс наполнения схематизированной картины объекта частными признаками, за счет чего оказывается возможным движение от одного уровня абстракции к другому, более оптимальному для решения конкретных задач.

Основные операции предлагаемой техники абстракций - операции абстрагирования и конкретизации - непосредственно представляются операторами непротиворечивой системы λ-исчисления - аппликации и λ-абстракции - которая строится в качестве

прототипа программ на языках функционального программирования для реализации моделей ТАРД.

Модель ТАРД имеет многоуровневое определение, которое позволяет конструировать типы, представляющие собой различные политики безопасности, в процессе функционирования системы.

Архитектура модели ТАРД содержит:

- средства определения возможности доступа субъектов к объектам в соответствии с их полномочиями;
- средства двухступенчатого администрирования – для конструирования политик авторизации и для управления идентификацией сущностей в процессе разграничения доступа.

Определение модели включает типы следующих уровней:

$$T = (T_{META}, T_{OBJ}, T_{AM}),$$

где META - метауровень, OBJ – объектный уровень, *AM* – уровень матрицы доступа.

На уровне *META* тип представлен метатипом T_{META}, являющимся обобщенным представлением политики $P_{META}(T)$. Он служит для порождения политик типизированного атрибутного разграничения доступа объектного уровня $P_{OBJ}(T)$.

Типы объектного уровня T_{OBJ} представляют собой ряд конкретных политик разграничения доступа $P_{OBJ}(T)$, получаемых из метаполитики $P_{META}(T)$.

Тип T_{AM} уровня AM является реализацией политики типизированного атрибутного разграничения доступа $P_{OBJ}(T)$ в виде множества типизированных переменных, образующих матрицу доступа.

Функционирование многоуровневой модели ТАРД заключается в моделировании семантики следующего уровня путем интерпретации модели, представляющей предыдущий уровень.

В процессе работы на разных уровнях модель выполняет различные функции.

На уровне META осуществляется конструирование семантики уровня OBJ в виде типа T_{OBJ} специальной операцией интерпретации $I_{META}(Dom, Str, Op)$, которое заключается в определении вида структуры *Str* домена *Dom* типа T_{OBJ} как подструктуры домена *Dom* типа T_{META}, присвоении значений его элементам и определении вида соответствующих операций *Op*.

В результате создаются различные виды моделей разграничения доступа T^i_{OBJ}, предназначенные для выполнения политик разграничения доступа $P^i_{OBJ}(T)$:

$$T_{META}\,(I(Dom^{OBJ}, Str^{OBJ}, Op^{OBJ})) \rightarrow T^i_{OBJ},\ i=\overline{1,K},\ K \neq N.$$

Формирование матрицы доступа осуществляется операциями *Type* сконструированных моделей T_{OBJ}. При этом производится присвоение полномочий сущностям в виде их меток безопасности:

$$T_{OBJ}(Type(e)) \rightarrow T_{AM}.$$

На уровне AM производится обработка создаваемой матрицы доступа путем выдачи разрешения на доступ согласно критерию, задаваемому типом T_{OBJ}, в результате выполнения операции доступа *Acc*:

$$T_{AM}(Acc(Type^{OBJ}(s), Type^{OBJ}(o))) \rightarrow \{true, false\}.$$

Модели T^{i}_{OBJ} могут выполняться как последовательно так и параллельно, реализуя все аспекты множественной политики ТАРД.

Заключение

Приводится описание существующих моделей разграничения доступа, их достоинств и недостатков в сравнении с разрабатываемой моделью типизированного атрибутного разграничения доступа (ТАРД). Показано, что она отвечает основным требованиям построения моделей, обеспечивающим безопасное пользование разделяемыми ресурсами.

Рассмотрено создание архитектуры моделей сложных средств контроля доступа путем абстракции и разграничения полномочий. Предложена методика представления модели ТАРД в виде уровней абстракции типов атрибутов разграничения доступа, как средства управления сложностью ее конструирования и функционирования.

Литература

1. Sandhu R.S., Samarati P. Access control: principle and practice. Communications Magazine, IEEE, 32(9):40–48, 1994.

2. Hosmer H. 1993. The multipolicy paradigm for trusted systems. In Proceedings on the 1992-1993 workshop on New security paradigms (NSPW '92-93), J. Bret Michael, Victoria Ashby, and Catherine Meadows (Eds.). ACM, New York, NY, USA, 19-32. DOI=http://dx.doi.org/10.1145/283751.283768

3. David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. 2001. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.* 4, 3 (August 2001), 224-274. DOI: https://doi.org/10.1145/501978.501980

4. Karp A., Haury H., Davis M. (2010). From ABAC to ZBAC: The evolution of access control models. ISSA (Information Systems Security Association) Journal. 8. 22-30.

5. Hu V. C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., and Scarfone K. Guide to attribute based access control (ABAC) definition and considerations. NIST Special Publication, 800:162, 2014. http://dx.doi.org/10.6028/NIST.SP.800-162

6. Fisher B., Brickman N., Burden P., Jha S., Johnson B., Keller A., Kolovos T., Umarji S., Weeks S. Attribute Based Access Control. NIST Special Publication 1800-3, 2017. https://www.nccoe.nist.gov/publication/1800-3/ (Accessed August 2018).

7. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам // Проблемы информатики. – 2014. – № 1(22). – С. 43-55.

8. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа. // Известия НАН РК. Серия физико-математическая. – 2014. – № 5. – С. 33-41.

9. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Логический подход к организации многокритериального атрибутного разграничения доступа. // Совместный выпуск по материалам международной научной конференции «Вычислительные и информационные технологии в науке, технике и образовании» (CITech-2015) (24-27

сентября 2015 г.) Вычислительные технологии т.20, Вестник КазНУ им.Аль-Фараби, серия математика, механика и информатика №3(86) Часть 1. - С.275-278.

10. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Моделирование семантики типизированного атрибутного разграничения доступа // Журнал Проблемы информатики, - 2017, № 1. С. 25-37.

11. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Применение логики для построения моделей разграничения доступа к информации // «Доклады Национальной Академии Наук Республики Казахстан» 2017, №3. С. 48-54.

12. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Основы архитектуры программных систем для осуществления типизированного атрибутного разграничения доступа // Современные проблемы информатики и вычислительных технологий: Мат. науч. конф. (29-30 июня 2017 г). – Алматы, 2017, – С. 88-95.

13. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Многоуровневое представление модели типизированного атрибутного разграничения доступа // Современные проблемы информатики и вычислительных технологий: (Мат. Науч. Конф. 2-5 июля 2018 г.) – Алматы: ИИВТ МОН РК. 2018. – С. 111-120.

14. Калимолдаев М. Н. , Бияшев Р. Г. , Рог О. А. Анализ методов атрибутного разграничения доступа // ПДМ. 2019. № 44. С. 43–57. DOI: 10.17223/20710410/44/4

15. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Роль модели типизированного атрибутного разграничения доступа в выполнении задач защиты информации. // Труды XV Международной Азиатской школы-семинара "Проблемы оптимизации сложных систем" / Ин-т вычислительной математики и матем. геофизики СО РАН. Новосибирск, 26–30 августа 2019 г. Новосибирск: ИВМиМГ СО РАН, 2019. С 39-45. DOI: 10.24411/9999-018A-2019-10006

РЕАЛИЗАЦИЯ АЛГОРИТМА НПСС НА ОСНОВЕ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ

Калимолдаев[1] М.Н., Тынымбаев[1] С.Т., Кожагулов[2] Е.Т., Жексебай[2] Д.М., Хохлов[2] С.А., Ибраимов[2] М.К.

e-mail: Margulan.Ibraimov@kaznu.kz

[1]Институт информационных и вычислительных технологий КН МОН РК,
[2]Казахский национальный университет имени аль-Фараби,
Казахстан

Аннотация. *Аппаратная реализация на программируемых логических интегральных схемах (FPGA) умножителя полиномов по модулю необходимо для оптимизации вычислительных ресурсов, времени вычисления и т.д. В первую очередь это связано с необходимостью повышения производительности в обработке больших данных в автономных электронных устройствах. Применение программируемых логических интегральных схем повышает производительность вычислительных устройств в алгоритмах умножителя полиномов по модулю. В данной работе рассматривается аппаратная реализация систем счисления умножителя полиномов по модулю. Тестирование проводилось на отладочной плате Nexys 4 DDR4 Artix-7.*

Введение

Последние несколько десятилетий информация прогрессивно растет. Безопасность данных стала основной проблемой. Поэтому защита информации является одним из основных задач информационной технологии. При этом существует несколько алгоритмов шифрования данных [1-4]. Алгоритмы и методы различаются по уровню сложности и криптостойкости. Однако быстрота шифрования данных является основной характеристикой при реализации криптосистем. В работе [4] приведен алгоритм криптографии данных на основе умножителя полиномов по модулю, который отвечает вышеизложенным требованиям.

Система остаточных классов является системой представления данных в вычислительной арифметике, в которой целое число обозначается набором меньших чисел.

В системе остаточных классов целое положительное число A представляется в виде последовательности остатков или вычетов

$$A = (\alpha_1, \alpha_2, \dots, \alpha_n) \quad (1)$$

от его деления на заданные положительные целые числа $p_1, p_2, \dots, p_n$, которые называют основаниями системы. Числа α_i образуются следующим образом:

$$\alpha_i = A - \left[\frac{A}{p_i}\right] p_i, \ i = \overline{1,n} \ , \quad (2)$$

где $\left[A / p_i\right]$ обозначает целую часть от деления A на p_i. Из (2) следует, что цифра i-го разряда α_i числа A есть наименьший положительный остаток от деления A на p_i и $\alpha_i < p_i$. В этом случае образование цифры каждого разряда производится независимо друг от друга. В соответствии с китайской теоремой об остатках представление числа A в виде (1) будет единственным, если числа p_i попарно просты между собой. Объем диапазона представимых чисел в этом случае равен $P = p_1 p_2 \cdots p_n$. Здесь, аналогично позиционной системе счисления, диапазон представимых чисел растет как произведение оснований, а разрядность чисел растет как сумма разрядностей тех же оснований.

Как видно, основные преимущества применения непозиционной системы счисления заключаются в отсутствии переноса разрядов в операциях сложения и умножения, и, следовательно, в возможности параллельного выполнения операций по каждому из оснований системы, что существенно ускоряет процесс вычисления.

Стоит отметить, что большинство современных процессоров общего назначения не способны эффективно выполнять вычисления в непозиционной системе счисления. Для наиболее эффективной реализации вычислительных устройств на основе системы остаточных классов требуется разработать нестандартные схемные решения, которые эффективно выполняют вычисления в непозиционной системе счисления.

Основные преимущества, которые позволяют эффективно использовать модулярную арифметику в некоторых областях вычислительной техники: высокий уровень естественного параллелизма на уровне системы счисления, что с связано с отсутствием переноса разрядов в сложении и умножении, а также отсутствие распространения ошибок. В отличие от позиционной системы счисления все элементы вектора

равнозначны, и ошибка в одном из них ведет всего лишь к сокращению динамического диапазона. Этот факт позволяет проектировать устройства с повышенной отказоустойчивостью и коррекцией ошибок.

Особенности НПС дают значительные преимущества перед позиционной системой счисления при выполнении модульных операций сложения, вычитания и умножения. Особенно это актуально, если в качестве операндов выступают многоразрядные числа.

Основные принципы построения симметричного блочного шифра

Наиболее надежным и распространенным методом защиты информации от несанкционированного доступа является применение криптографии. Этот метод защиты информации дает процедуры и средства преобразования информации для скрытия её содержания. В настоящее время криптография нашла применение во многих областях деятельности, и при этом ее значимость необходимость с течением времени только увеличивается. А это значит, что актуальность поиска и исследования математических методов криптографического преобразования информации не уменьшается.

Главным инструментом сокрытия информации с помощью криптографических методов является шифрование. Симметричное шифрование состоит из следующих двух взаимно обратных преобразований:

- перед передачей данных по каналу связи или перед помещением на хранение, например, сохранением в виде файла на жесткий диск, они подвергаются зашифрованию с использованием секретного ключа. Обозначим эту операцию в следующем виде:

$$E_K(T), \tag{3.1}$$

где T – исходный открытый текст, K – секретный ключ шифрования, E – функция шифрования.

- для восстановления исходных данных из зашифрованных к ним применяется процедура расшифрования с помощью того же секретного ключа:

$$T = D_K(E_K(T)), \tag{3.2}$$

где D – функция расшифрования.

Одним из требований к алгоритму является то, что без знания секретного ключа расшифрование данных должно быть невозможно.

По способу организации использования секретного ключа шифры делятся на симметричные (шифрование с закрытым ключом) и ассиметричные (криптографические системы с открытым или публичным ключом). Симметричные шифры — способ шифрования, в котором для операции шифрования и расшифрования применяется один и тот же криптографический ключ.

По способу обработки исходных данных симметричные криптосистемы делятся на блочные и поточные шифры. В блочных шифрах данные обрабатываются в виде блоков определённой длины (обычно 64, 128 или 256 бит), применяя к каждому блоку функцию преобразования с использованием секретного ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки.

Предварительный расчет параметров полиномиальной НПСС

Работа криптосистемы на основе НПСС предусматривает выполнение предварительных расчётов параметров непозиционной полиномиальной системы. Данные расчёты включают в себя следующие шаги:

–создание базы данных неприводимых полиномов с коэффициентами над GF(2);

–определение необходимой длины *N* блока и ключа шифрования;

–формирование в соответствии с длиной блока системы оснований. Для формирования полиномиальной НПС при обработке блока длиной *N* бит из множества всех неприводимых многочленов степени не выше значения *N* выбираются рабочие основания.

–подбор и проверка содержания системы оснований. Все выбираемые основания должны отличаться друг от друга, даже если они являются неприводимыми полиномами одной степени. Тогда в этой системе любой многочлен степени меньше суммы степеней всех выбранных рабочих оснований имеет единственное представление в виде последовательности остатков (вычетов) от деления его на данные основания.

–предварительная интерпретация входного блока данных в виде остатков от деления на выбранную систему оснований. При этом сгенерированная ключевая последовательность так же может быть представлена в виде последовательностей вычетов, а для расшифрования необходимо вычислить обратный многочлен к каждому из этих вычетов по модулю соответствующего основания.

Общая схема работы программно-аппаратной криптосистемы на основе НПС показана на рисунке 1.

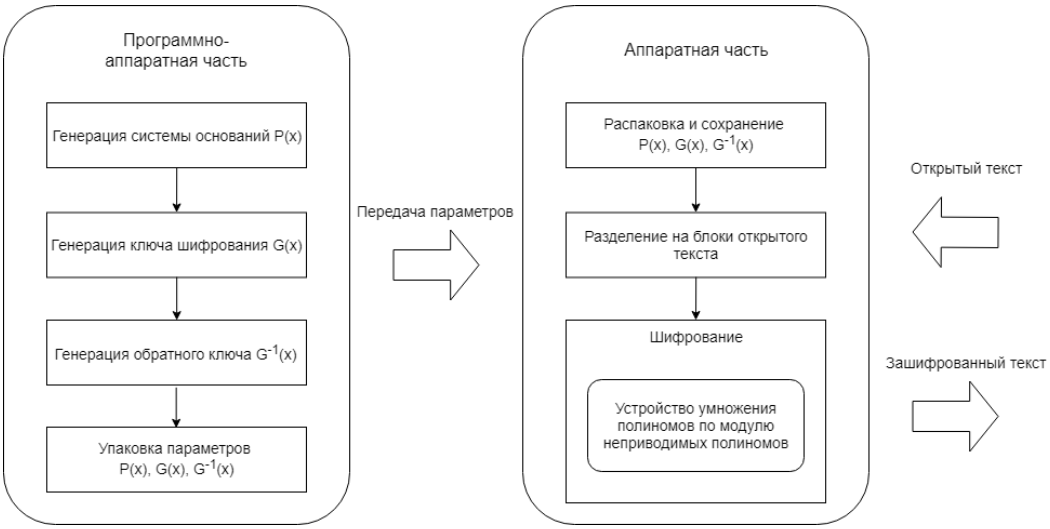


Рисунок 1. Работа программно-аппаратной криптосистемы на основе НПСС

Основная часть расчетов параметров НПС включает в себя формирование системы модулей полиномиальной системы остаточных классов. Рабочее основание системы формируется из предварительно рассчитанной базы данных неприводимых многочленов. Эти полиномы выбираются случайным образом в соответствии с предоставленными степенями для заполнения длины блока входных данных.

На рисунке 2 показана блок-схема основного блока вывода информации в VGA дисплей. Данный блок состоит из пяти входных данных (тактовая частота (CLK), вывод информации кодера или декодера на дисплей (codec), разрешающий сигнал кодированию информации (en), сброс программы драйвера VGA (RST_BTN), показ

исходной информации (sel)), пяти выходных данных (данные RGB (VGA_B, VGA_G, VGA_R), горизонтальные и вертикальные синхросигналы (VGA_HS_O, VGA_VS_O)).

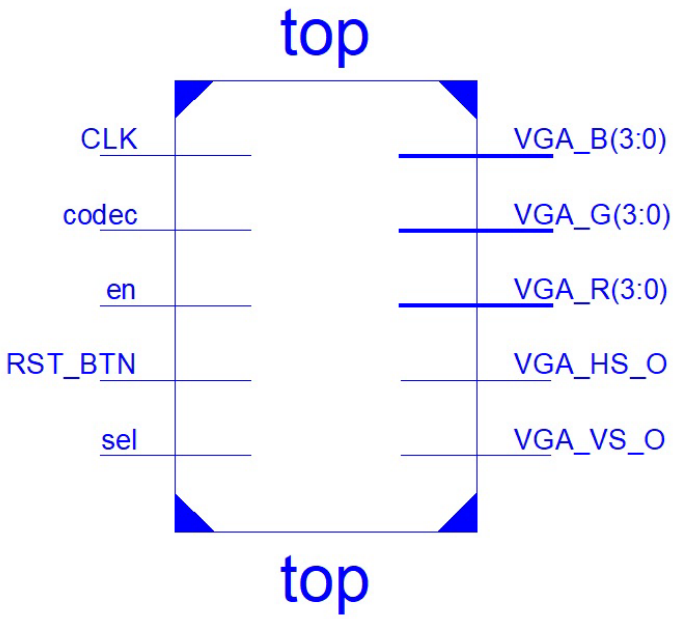


Рисунок 2. Блок-схема основного устройства вывода информации в VGA дисплей

Блок состоит из четырех мини-блоков (деление частоты (div_clk), драйвер VGA (vga640x480), блок исходной информации, кодер и декодер предложенного нами алгоритма (dataProcessing), блок показа информации в VGA дисплее (displayData)) (Рисунок 3). Алгоритм, описанный в работе [4], обрабатывается в блоке «Data Processing».

Для работы VGA-дисплея 640x480 с частотой 60 Гц тактовая частота для драйвера VGA должна быть 25 МГц. Поэтому блок деления частоты изменяет частоту с 100 МГц на 25 МГц. Блок dataProcessing генерирует информацию и передает в следующий блок (displayData), также данный блок кодирует исходную информацию и декодирует кодированную информацию. Эти данные передаются в блок displayData для отображения информации. Длина информации составляет 256 бит, а количества строк 4. Поэтому блок dataProcessing имеет 12 выходных данных (4 выхода для исходной информации, 4 – данные кодера и 4 – данные декодера).

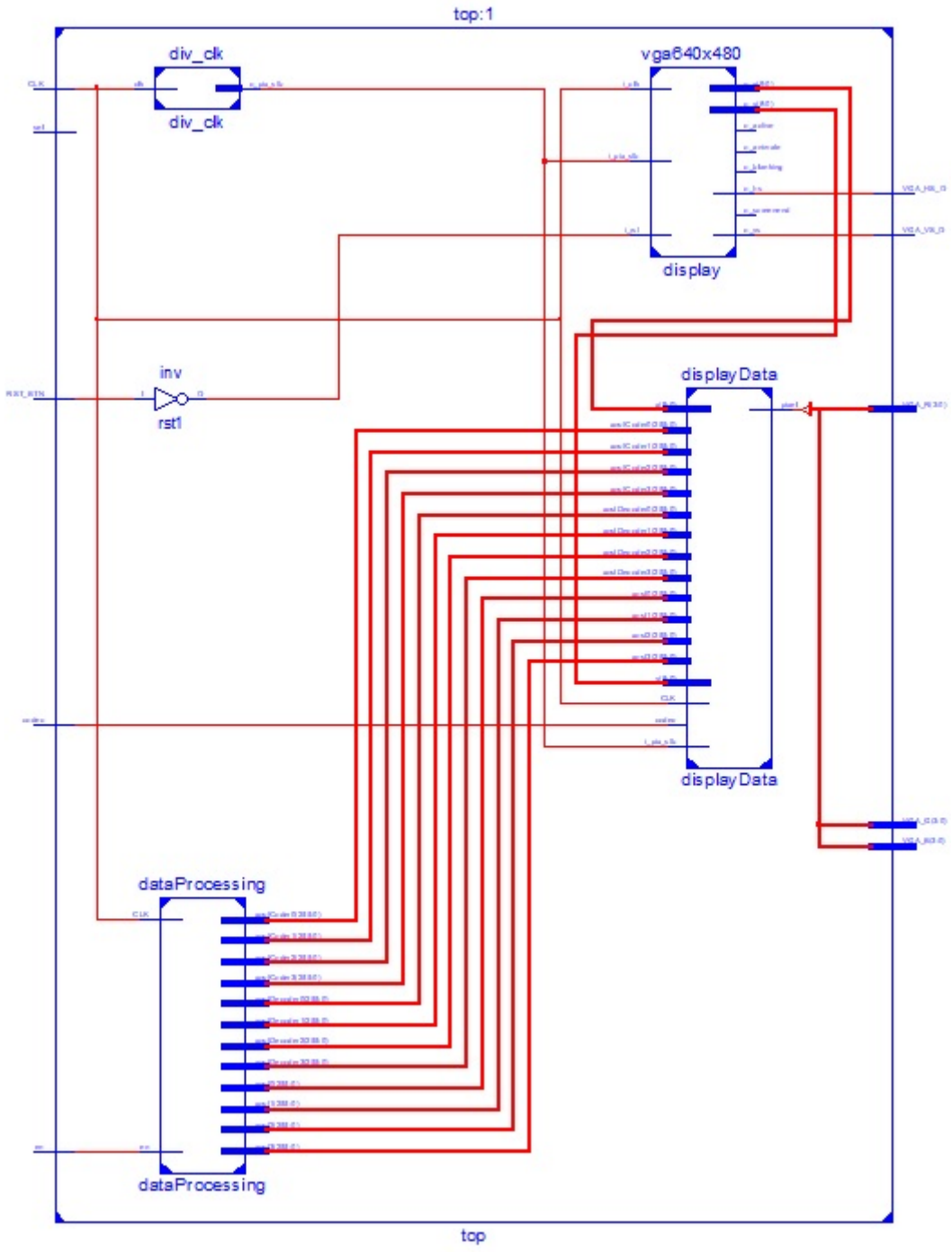


Рисунок 3. Блок-схема внутренней структуры основного блока вывода информации в VGA дисплей

Блок vga640x480 предназначен для генерации синхросигналов и передачи позиции пикселя (Рисунок 4). Данный блок имеет разрешение 640x480 пикселей. Позиция пикселя передается через выходы o_x и o_y, которые указывают вертикальное и горизонтальное положении. Для реализации блок используется логические элементы, умножители, сумматоры, вычитатель, компараторы и триггеры (Рисунок 5).

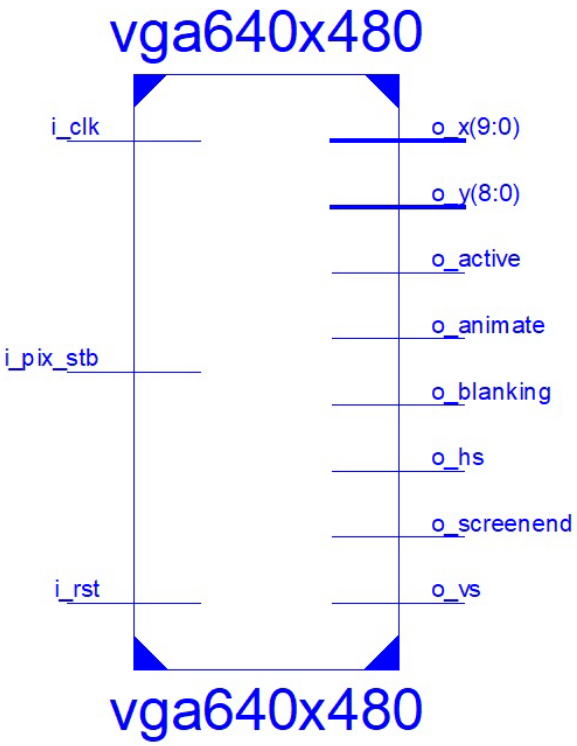


Рисунок 4. Блок драйвера VGA

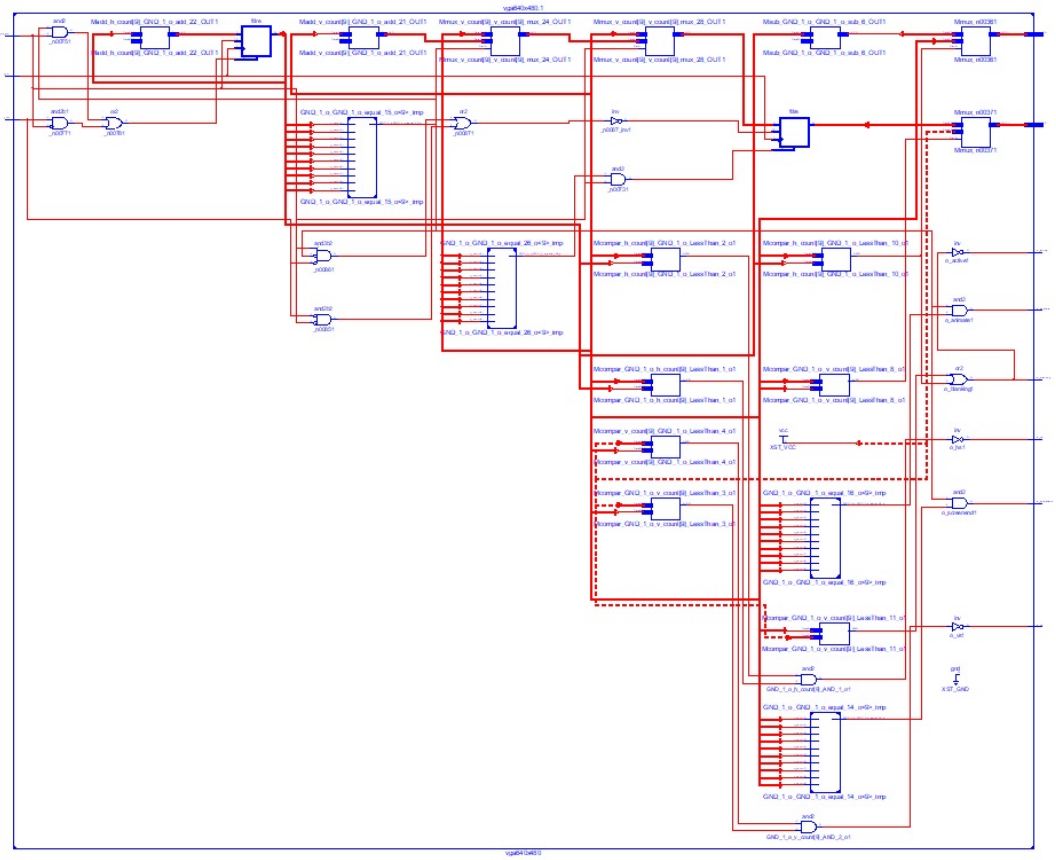


Рисунок 5. RTL схема драйвера VGA

Блок displayData обрабатывает информацию для показа в VGA-дисплей. Данный блок считывает и обрабатывает данные с блока dataProcessing и передает в блок pc_vga_8x16 (Рисунок 6). Блок pc_vga_8x16 реализует символьное ПЗУ для перевода ASCII коды символов в изображении размером 8x16 пикселей. Блок состоит из трех модулей (pc_vga_8x16_00_7F, pc_vga_8x16_80_FF и мультиплексор; Рисунок 7).

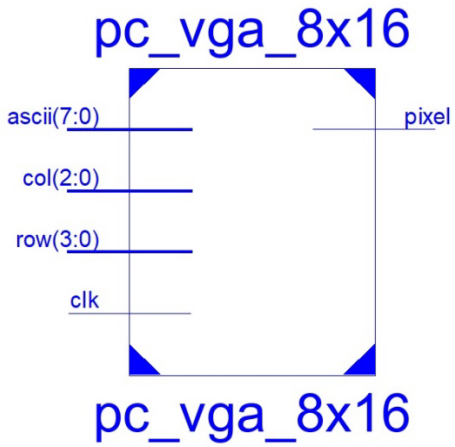


Рисунок 6. Блок-схема преобразователя ASCII коды символов в изображении размером 8x16 пикселей

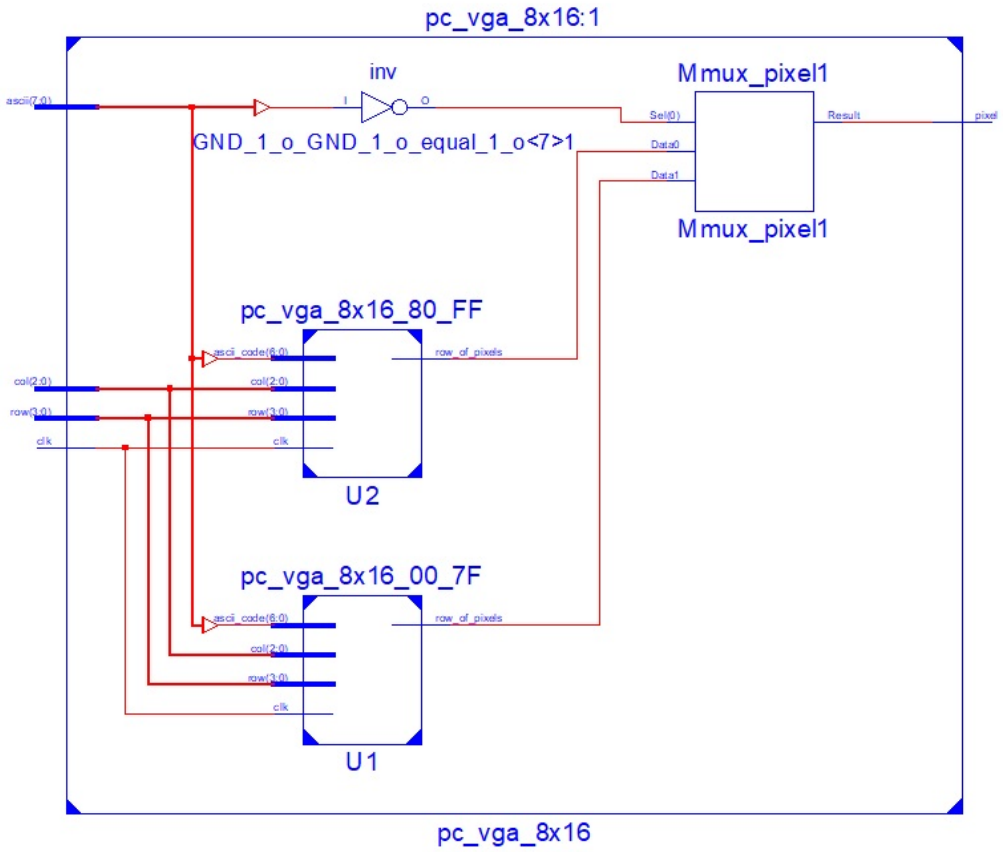


Рисунок 7. Преобразователь ASCII коды символов в изображении

Мультиплексор выбирает один из двух модулей преобразователя кодов ASCII в изображении размером 8x16 пикселя. На рисунке 8 показан модуль преобразователя ASCII кода. Модуль состоит из инвертора и блока памяти ПЗУ (Рисунок 9).

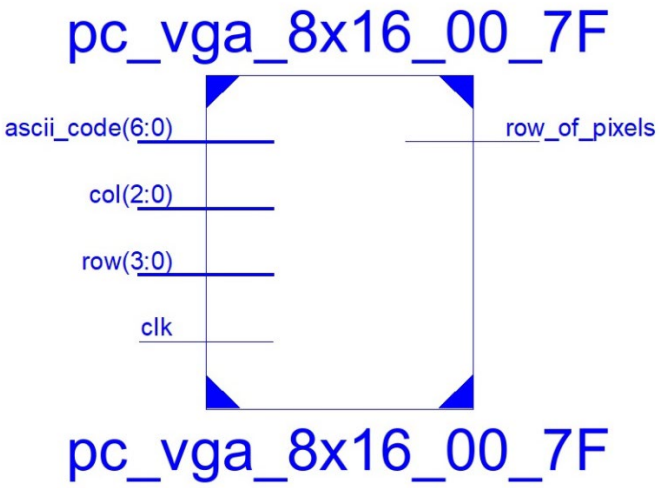


Рисунок 8. Модуль преобразователя ASCII кода символов в изображении

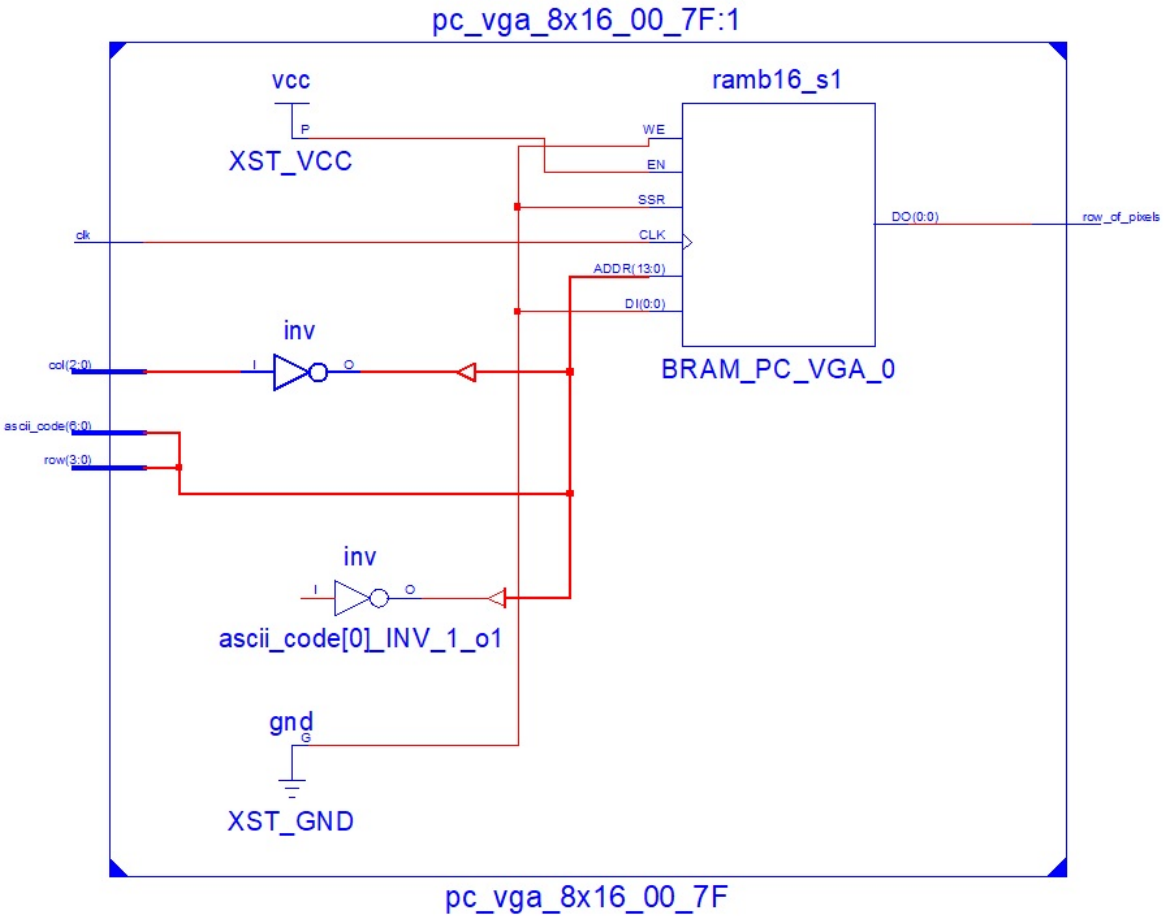


Рисунок 9. RTL схема модуля преобразователя кодов ASCII

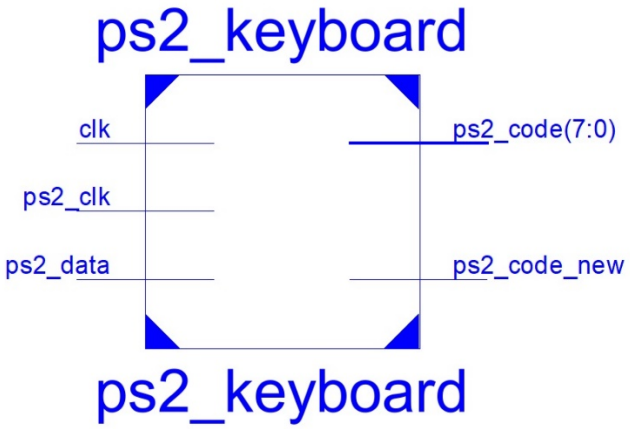


Рисунок 10. Ввод информационных данных через клавиатуру.

Информационные данные для шифрования вводились через клавиатуру (Рисунок 10). Длина строки состоит из 256 бит, обработка данных производилась блоками, соответственно разделенные небольшие блоки рассчитывались параллельно.

В данной работе показана возможность аппаратной реализации на программируемых логических интегральных схемах параллельно-последовательных вычислительных систем умножителя полиномов по модулю. Приводятся результаты основного блока схемы вывода информации, внутренней структуры, блоков: периферийных устройств, деление частоты, кодера, декодера, обработки данных, генерации синхросигналов, преобразователя ASCII кодов, объявление портов, локальных параметров, также RTL схема полученного результата.

Литература

1. Bos J.W., Halderman J.A., Heninger N., Moore J., Naehrig M., Wustrow E. Elliptic curve cryptography in practice //International Conference on Financial Cryptography and Data Security. – Springer, Berlin, Heidelberg, 2014. – P. 157-175.

2. Gura N., Patel A., Wander A., Eberle H., Shantz S.C. Comparing elliptic curve cryptography and RSA on 8-bit CPUs //International workshop on cryptographic hardware and embedded systems. – Springer, Berlin, Heidelberg, 2004. – P. 119-132.

3. Garg V., Arunachalam V. Architectural Analysis of RSA cryptosystem on FPGA //International Journal of Computer Applications. – 2011. – Vol. 26, №. 8. – P. 30-34.

4. Kalimoldayev M., Tynymbayev S., Gnatyuk, S. Ibraimov M., Magzom M. The device for multiplying polynomials modulo an irreducible polynomial //NEWS of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences. – 2019. – Vol. 2, №. 434. – P. 199-205.

5. Kahri F., Mestiri H., Bouallegue B., Machhout M. High speed FPGA implementation of cryptographic KECCAK hash function crypto-processor //Journal of Circuits, Systems and Computers. – 2016. – Vol. 25, №. 04. – P. 1650026.

6. Marzouqi H., Al-Qutayri M., Salah K., Schinianakis D., Stouraitis T. A high-speed FPGA implementation of an RSD-based ECC processor //IEEE Transactions on Very Large Scale Integration (VLSI) Systems. – 2015. – Vol. 24, №. 1. – P. 151-164.

7. Khan Z.U.A., Benaissa M. High speed ECC implementation on FPGA over GF (2 m) //2015 25th International Conference on Field Programmable Logic and Applications (FPL). – IEEE, 2015. – P. 1-6.

8. de Dormale G.M., Quisquater J.J. High-speed hardware implementations of elliptic curve cryptography: A survey //Journal of systems architecture. – 2007. – Vol. 53, №. 2-3. – P. 72-84.

9. Alkalbani A.S., Mantoro T., Tap A.O.M. Comparison between RSA hardware and software implementation for WSNs security schemes //Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010. – IEEE, 2010. – P. E84-E89.

АЛГОРИТМ ШИФРОВАНИЯ НА ОСНОВЕ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Калимолдаев М.Н., Тынымбаев С.Т., Магзом М.М.
e-mail: magzomxzn@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данном докладе приведены промежуточные результаты выполнения задачи проекта грантового финансирования КН МОН РК «Разработка программно-аппаратных средств для криптосистем на базе непозиционной системы счисления». Идея данного проекта заключается в разработке различных вариантов умножителей полиномов по модулю неприводимых полиномов и их программно-аппаратная реализация.*

Введение

С целью поиска путей повышения эффективности программно-аппаратных вычислений, методов обнаружения и исправления ошибок и создания высоконадежных компьютерных систем проводятся исследования в области непозиционных систем обозначений, таких как система остаточных классов (СОК) [1, 2]. В классической позиционной системе счисления значение каждой цифры в обозначении номера зависит от ее положения.

В непозиционных системах счисления, напротив, обозначение чисел основано на других принципах. В СОК многозначное целое число в позиционной нотации представляется как последовательность нескольких позиционных чисел небольшой разрядности. Эти числа являются остатками от деления исходного числа на модули СОК.

Применение СОК является эффективным способом выполнения с данными большого размера. В частности, использование СОК позволяет увеличить скорость выполнения операций за счет отсутствия переноса при сложении, разделения большого блока входных данных на более мелкие подблоки и их параллельной обработки. Перспективным направлением применения СОК в вычислительной технике является разработка криптографических средств защиты информации.

Алгоритмы криптографии, построенные на базе непозиционных полиномиальных систем остаточных классов (НПСС), позволяют повысить надежность алгоритма

шифрования за счёт ввода дополнительных секретных параметров в виде системы оснований полиномиальной СОК. Секретность в этом случае определяется так называемым «полным ключом», который зависит состоит из секретной ключевой (псевдослучайной) последовательности и выбранной системы оснований. Стойкость против полного перебора в этом случае зависит не только от длины секретной последовательности, но и от состава системы полиномиальных оснований, и от количества возможных перестановок оснований в этой системе. Чем больше длина полного ключа шифрования в НПСС, тем больше вариантов выбора систем рабочих оснований. Поэтому криптографическая стойкость разработанных алгоритмов шифрования с использованием НПСС существенно возрастает с увеличением длины электронного сообщения. Далее подробнее рассматривается метод применения НПСС в разработанных алгоритмах шифрования.

Построение непозиционной полиномиальной системы счисления

Первым этапом при выполнении шифрования на базе НПСС является построение непозиционной системы счисления. Рассмотрим шифрование блока данных длиной *N* бит разработанным ранее нетрадиционным алгоритмом шифрования [3-5].

В начале из множества всех неприводимых многочленов степени не выше значения *N* выбираются рабочие основания

$$p_1(x), p_2(x), \ldots, p_S(x). \tag{1}$$

Согласно китайской теореме об остатках, все выбираемые основания в системе счисления должны отличаться друг от друга, то есть быть уникальными для этой системы счисления. Рабочий диапазон данной системы определяется многочленом $P(x) = p_1(x), p_2(x), \ldots, p_S(x)$ степени m:

$$m = \sum_{i=1}^{S} m_i,$$

где S – число выбранных рабочих оснований. В этой системе любой многочлен степени меньше m имеет единственное представление в виде последовательности остатков (вычетов) от его деления на основания (1). Следовательно, сообщение длиной N бит может быть представлено в виде последовательности вычетов $\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)$ от деления некоторого многочлена $F(x)$ на рабочие основания $p_1(x), p_2(x), \ldots, p_S(x)$:

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)), \tag{2}$$

где $F(x) \equiv \alpha_i(x) (\mathrm{mod}\, p_i(x))$, $i = \overline{1, S}$.

Таки же образом, ключ длины *N* бит интерпретируется как система вычетов $\beta_1(x), \beta_2(x), \ldots, \beta_S(x)$, полученных в результате деления некоторого полинома $G(x)$ по той же системе оснований:

$$G(x)=(\beta_1(x),\beta_2(x),\ldots,\beta_S(x)), \tag{3}$$

где $G(x)\equiv\beta_i(x)(\mathrm{mod}\ p_i(x))$, $i=\overline{1,S}$.

Тогда базовое криптографическое преобразование в нетрадиционном шифре представляется в виде некоторая функция $H(F(x),G(x))$:

$$H(x)=(\omega_1(x),\omega_2(x),...,\ \omega_S(x)), \tag{4}$$

где $H(x)\equiv\omega_i(x)(\mathrm{mod}\ p_i(x))$, $i=\overline{1,S}$.

В соответствии с свойствами системы остаточных классов, операции в функциях $F(x)$, $G(x)$, $H(x)$ могут выполняться параллельно по соответствующим модулям многочленов $p_1(x),p_2(x),...,p_S(x)$, выбранных в качестве оснований НПСС. В этом алгоритме при его реализации могут использоваться разные шифрметоды.

Здесь элемент $\omega_i(x)$ криптограммы $H(x)$ вычисляется по известному ключу $G(x)$ путем умножения каждого его значения $\beta_i(x)$ на $\alpha_i(x)$:

$$\alpha_i(x)\beta_i(x)\equiv\omega_i(x)(\mathrm{mod}\ p_i(x)),\ i=\overline{1,S}. \tag{5}$$

Тогда обратный полином $\beta_i^{-1}(x)$ определяется из сравнения:

$$\beta_i(x)\beta_i^{-1}(x)\equiv 1(\mathrm{mod}\ p_i(x)),\ i=\overline{1,S} \tag{6}$$

Полученный полином $G^{-1}(x)=(\beta_1^{-1}(x),\beta_2^{-1}(x),...,\beta_S^{-1}(x))$ является обратным к полиному $G(x)$. Открытое сообщение в соответствии с выражениями (5) и (6) восстанавливается по следующим сравнениям:

$$\alpha_i(x)\equiv\beta_i^{-1}(x)\omega_i(x)(\mathrm{mod}\ p_i(x)),\ i=\overline{1,S}.$$

Предложенные алгоритмы шифрования основаны на описанном выше нетрадиционном шифре. При их разработке использованы такие криптографические процедуры, как сети Фейстеля, блоки замены и режимы шифрования.

Реализация алгоритма шифрования на основе полиномиальной СОК

С целью улучшения статистических характеристик нетрадиционного алгоритма шифрования, к исходным функциям преобразования (5) и (6) были применены следующие преобразования:

- для обеспечения условия конфузии были добавлены блоки нелинейной замены.
- для выполнения условия принципа диффузии применяются битовые перестановки.

Структура полученного нетрадиционного алгоритма шифрования показана на рисунке 1.

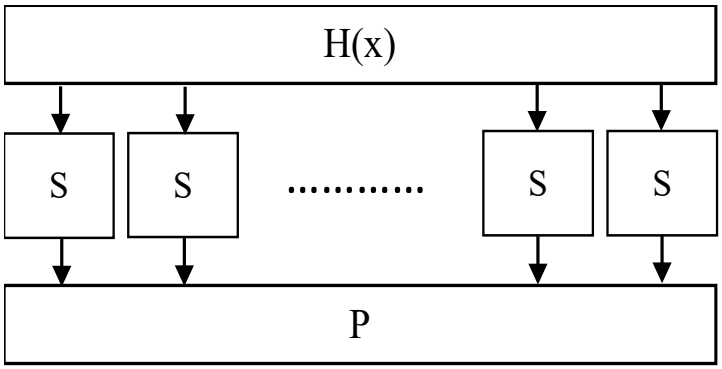


Рис. 1. Модифицированный нетрадиционных алгоритм шифрования

Пример шифрования на основе сети Фейстеля показан на рисунке 2.

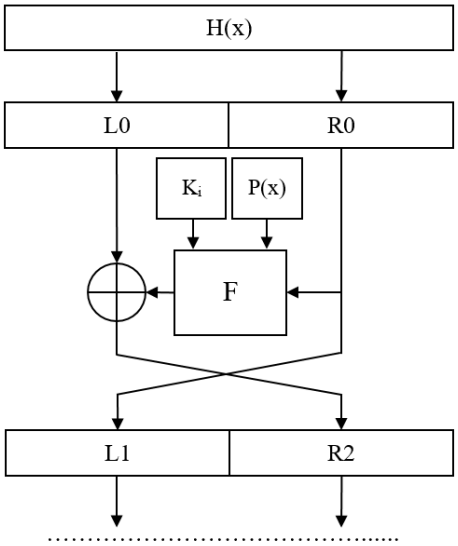


Рис. 2. Схема применения сети Фейстеля

В большинстве шифров с архитектурой сети Фейстеля используемая функция *F* в течение каждого раунда зависит только от одного из подключей, вырабатываемых из основного ключа шифра. Сеть с такого рода зависимостью функции преобразования называют гомогенной и гетерогенной в противном случае.

Известно, что независимо от количества раундов, никакая сеть Фейстеля не может противостоять атакам по связанным ключам, где ключи вырабатываются за счёт сдвига битовой последовательности на постоянную величину.

Для примера рассмотрим модель, в которой блок входных данный *F* длиной 128 бит разделяется на два подблока равной длины R_i и L_i.

При использовании гомогенной сети на каждом этапе шифрования используется отдельная ключевая последовательность $K^{(i)}$:

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i).$$

При использовании гетерогенной сети на каждом этапе функция шифрования F подблока зависит не только от раундового ключа $K^{(i)}$, но и от выбранной системы оснований (1)*:*

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i, P(\mathrm{x})).$$

В предлагаемых алгоритмах раундовые ключи получаются путём сдвига битовой последовательности ключа K на переменное количество разрядов, которое определяется степенью *i*-го многочлена в системе оснований, которая, как было отмечено ранее является частью секрета.

Применение гетерогенных сетей может значительно улучшить характеристики шифра, поскольку неравномерное изменение внутренних свойств сети в пределах допустимых границ делает изучение свойств шифра достаточно затруднительным занятием.

Для аппаратного выполнения рутинных операций умножения полиномов по модулю неприводимого полинома в (5) и (6) требуется устройство умножения. Основным устройством для выполнения рутинных вычислений при программно-аппаратной реализации разработанных алгоритмов шифрования на базе НПСС является умножитель полиномов по модулю неприводимых полиномов с коэффициентами из поля GF(2).

Пример разработанного устройства умножения на основе дерева сумматоров показан в схеме на рисунке 3.

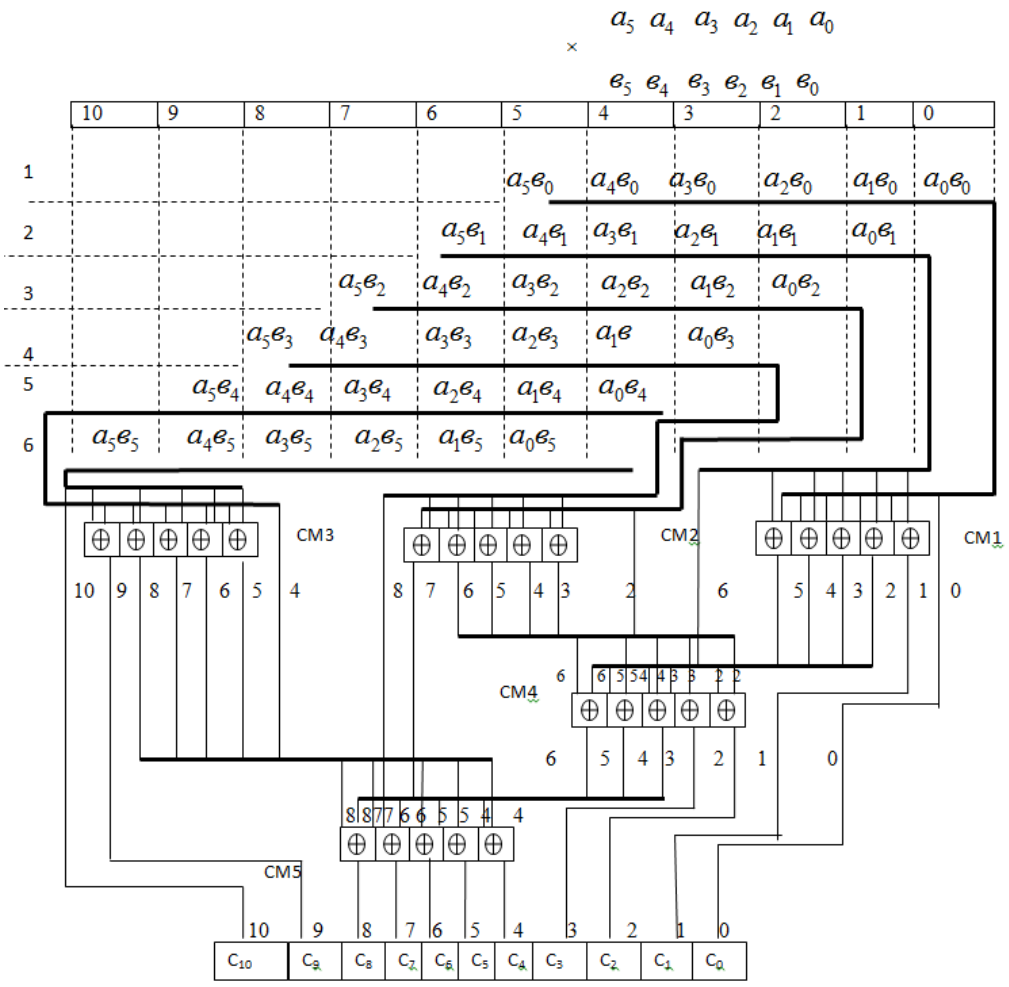


Рис. 3. Схема умножения 6-разрядных полиномов A и B
на дереве сумматоров

Для описания разработанного умножителя была использована среда проектирования Xilinx ISE Webpack. Описание схемы состоит из следующих компонентов:

Модуль верхнего уровня. В данном модуле определяются умножители matrixReducer, их входы и выходы.

Каждый модуль умножителя matrixReducer состоит из модуля конъюкторов строк матрицы и дерева сумматоров, и из модулей формирователя частичного остатка.

Модуль дерева сумматоров и конъюкторов строк матрицы.

Модуль формирователя частичного остатка.

Для каждого модуля был разработан файл тестов для проверки корректности реализации. Пример применения тестового вектора показан на рисунке 4.

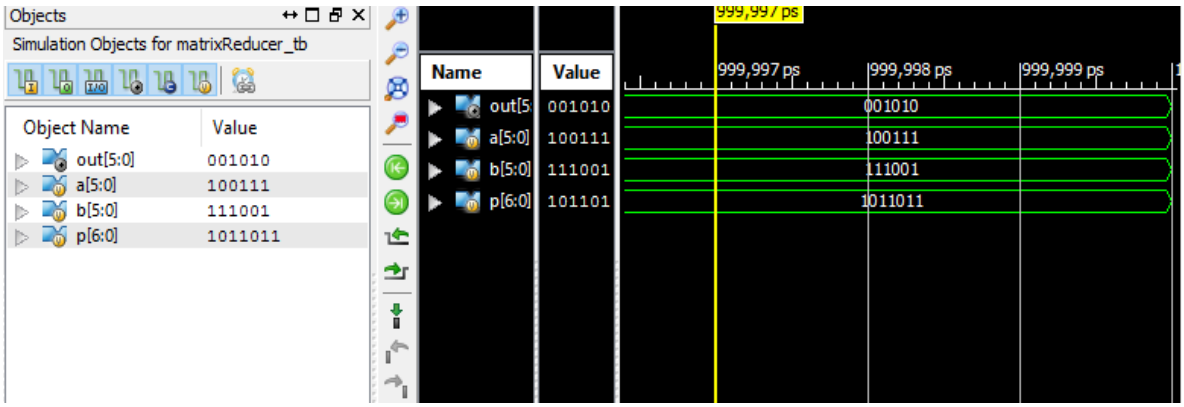


Рис. 4. Тестирование модуля умножения и приведения по модулю

Заключение

В ходе работы исследования и разработки алгоритма блочного шифрования на основе НПСС разработана программа расчета параметров полиномиальной НПС с функционалом выполнения арифметических операций над GF(2) и проверки шифрования с помощью базового алгоритма шифрования в непозиционной полиномиальной системы счисления. Разработанный функционал служит для выполнения рутинного вычисления, необходимого для аппаратной реализаций алгоритма симметричного шифрования данных на основе полиномиальной НПС. Разработана схема аппаратного умножителя полиномов по модулю неприводимых полиномов с коэффициентами из GF(2) на базе программируемой логики технологии FPGA. Проектирование схемы умножителя выполнено на основе матрицы конъюктеров с деревом сумматоров и формирователей частичных остатков.

Разработанный умножитель полиномов описан на языке HDL Verilog и реализован аппаратно на базе схемы программируемой логики на базе технологии FPGA Xilinx Spartan-6.

Литература

1. Svoboda A. Valach M. Operatorove obvody // Stroje Na Zpracovani Informaci – 1955. – Vol 3. – P. 247-295.

2. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Соаветское радио, 1968.

3. Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. - М., 1985. - 328 с.

4. Нысанбаев Р.К. Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан – Алматы: Гылым, 1999. – № 5. – С. 63-65.

5. Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M. Building modified modular cryptographic systems // International Journal of Applied Mathematics and Informatic. – 2015. – Vol. 9. – P. 103-109.

УМНОЖИТЕЛЬ ПОЛИНОМОВ ПО МОДУЛЮ С АНАЛИЗОМ ЗА ШАГ ДВУХ СТАРШИХ РАЗРЯДОВ ПОЛИНОМА-МНОЖИТЕЛЯ

Калимолдаев М.Н., Тынымбаев С.Т., Магзом М., Ибраимов М., Бердибаева Г.К.

e-mail: s.tynym@mail.ru

Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Рассматривается схемное решение для аппаратной реализации умножителя полиномов по модулю, где за шаг умножения анализируется два разряда множителя, что приводит к ускорению процесса умножения. Предложенный вариант умножителя может служить базовым блоком для аппаратной реализации криптосистем на основе непозиционной полиномиальной системы счисления.*

Программная реализация алгоритма шифрования и расшифрования на базе непозиционной полиномиальной системы счисления (НПСС) была рассмотрена в [1]. По сравнению с программным шифрованием аппаратное шифрование имеет ряд существенных преимуществ, одним из которых является его более высокое быстродействие.

Основным блоком аппаратной реализации криптосистем на базе НПСС является блок умножения полиномов по модулю неприводимых полиномов, где выполняются сложные вычисления по шифрованию и расшифрованию данных. Поэтому от быстродействия этого блока зависит быстродействие шифровального устройства.

Различные схемные решения умножителей полиномов по модулю были рассмотрены в работах [2-5].

В предлагаемой работе рассматривается схемное решение умножителя полиномов по модулю, где за шаг умножения анализируется два разряда полинома-множителя, что приводит к ускорению процесса умножения.

Функциональная схема предлагаемого умножителя приведена на рисунке 1. В состав умножителя входят: сдвигающий регистр RgB, имеющий цели сдвига на два разряда влево, регистр RgP для хранения неприводимого модулю P(x), регистр RgA для хранения полинома множимого A(x), формирователи частичных остатков PRF1 и PRF2, сумматоры по модулю 2 (AddM2.1, AddM2.2), блоки схем И3÷И7, блок синхронизаций (БСИНХ), который в свою очередь состоит из триггера Т, счетчика тактового сигналов (Count), блока схемы И2, схемы И1 элементов задержки DL.1÷DL.3. на входе БСИНХ подается сигнал «Start», тактовые сигналы Clok и двоичный код числа сдвигов К-1.

Разряды полинома-множителя B(x) подаются на входе RgB через блок схем И4. Двоичное изображение полинома-множимого A(x) подается на входе регистра RgA через блок схем И3, а неприводимый полином P(x) принимается в RgB через блок схем И5.

На рис.2 приведена структура PRF, который состоит из сумматора по модулю 2 и мультиплексора MS и инвертора. На инвертор подается старший бит (C_{old}) удвоенного значения предыдущего остатка. При значений $C_{old}=1$ (при этом $C_i>P(x)$) на выходы мультиплексора выдается с выходов сумматора AddM2 результат сложения $r_i=C_1 \oplus P$.

В противном случае, когда $C_{old}=0$, то на выходы мультиплексора MS в качестве результата выдается значение C_i. При этом $r_i= C_i$.

Работа умножителя начинается с подачи на вход БСИНХ сигнала «Start». По этому сигналу в регистр RgB принимается полином-множитель B(x), а в регистр РгР

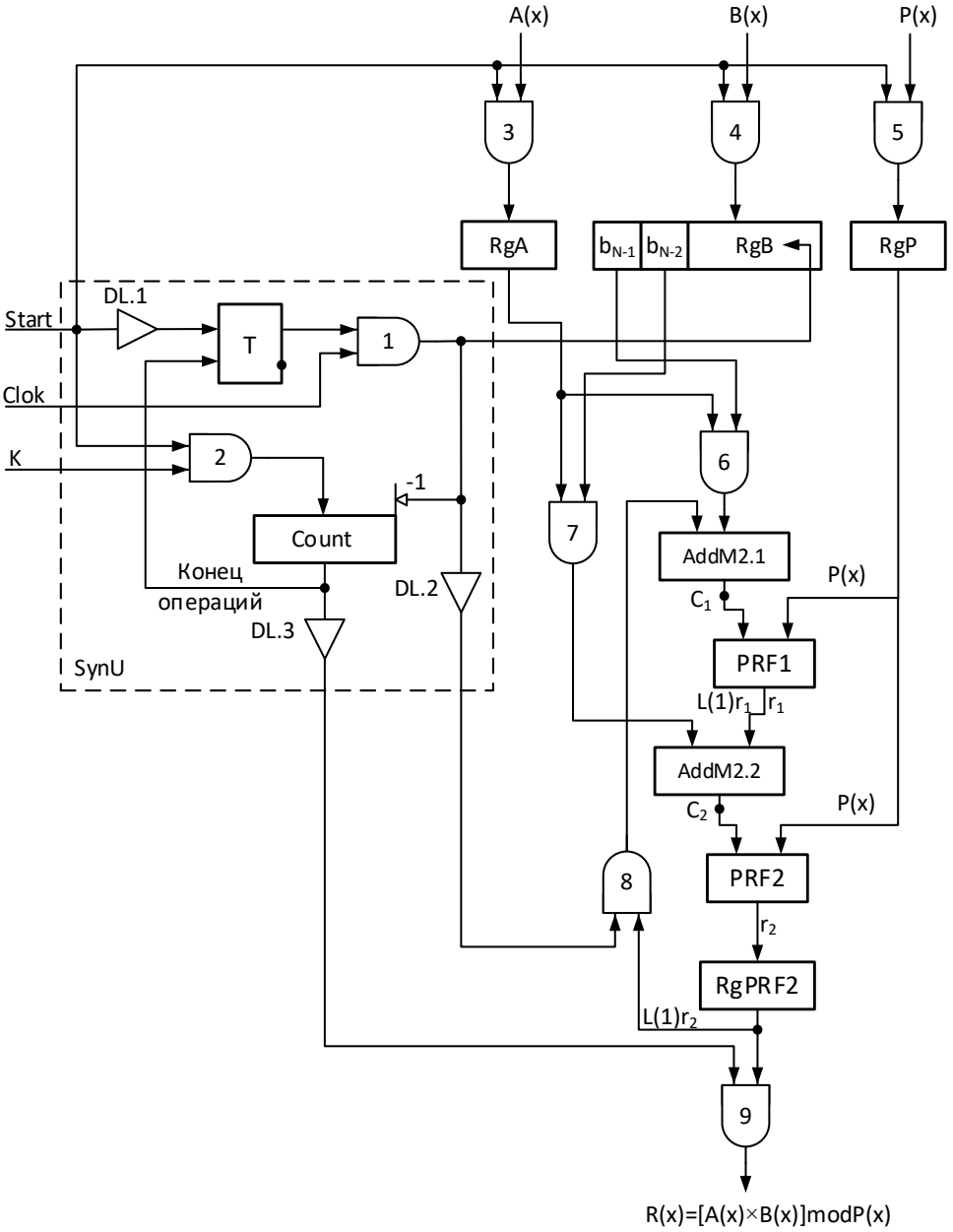


Рис.1. Функциональная схема умножителя полиномов по модулю Неприводимого полинома с анализом двух старших разрядов множителя за шаг

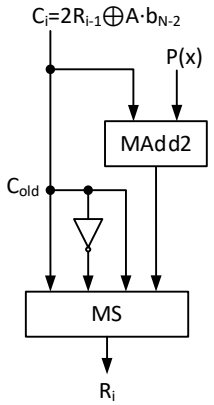


Рис. 2 Структура ФЧО

принимаются двоичные коэффициенты неприводимого полинома P(x). Двоичные коэффициенты полинома A(x) принимается в регистр RgA сигналом «Start» также в счетчик Count записывается двоичный код числа необходимых сдвигов К-1 через блок схем И2. После приема коэффициенты B(x) в старших разрядов регистра RgB фиксируется значение коэффициентов b_{N-1} и b_{N-2}. Выход старшего разряда регистра RgB b_{N-1} связан с управляющим выходом блока схем И6. Информационные выходы регистра RgA связаны с информационными входами блока схем И6. Следующий старший разряд регистра RgB b_{N-2} связан с управляющим выходом блока схем И7, а его информационные выходы связаны с выходами регистра RgA. С выходов блока схем И6 при $b_{N-1}=1$ значение A(x) подается на входы первого сумматора по модулю 2 – AddM2.1, а на вторые входы AddM2.1 подается нуль. При этом на выходах AddM2.1 имеем $C_1=0 \oplus A(x)$. Поскольку $A(x)<P(x)$, то на выходе PRF.1 формируется $r_i=A(x)$, который со сдвигом в сторону старшего разряда подается на входы второго сумматора по модулю 2 – AddM2.2 одновременно на вторые входы сумматора AddM2.2 подается A(x) при $b_{N-2}=1$. На выходах AddM2.2 формируется $C_2=A(x)\cdot b_{N-2} \oplus 2r_i$, который приводится по модулю P(x) на PRF.2, формируя частичный остаток r_2, который запоминается в регистре RgPRF2. Таким образом, после действия сигнала «Start» множимое A(x) умножается по модулю P(x) на биты старших разделов b_{N-1} и b_{N-2} полинома-множителя B(x).

На время формирования частичного остатка r_1 формирователем PRF.1 и r_2 формирователем PRF.2 и запоминания r_2 в RgPRF2 сигнал «Start» задерживается на элементе задержки DL.1. После чего сигнал «Start» проходит на единичный вход триггере T и переводит его в состояние 1, что позволяет первому импульсу Clok.1 проходить через схему И1 на вход сдвигающего регистра RgB и на вычитающий вход счетчика Count.

При этом регистр RgB сдвигается на два разряда влево, а показание счетчика Count уменьшается на единицу. Теперь в старших разрядах регистра RgB фиксируются биты b_{N-2} и b_{N-4}. Импульс Clok.1 задерживаясь на элементе задержки DL.2 на время сдвига регистра RgB поступает на управляющий вход блока схем И8. На информационные входы И8 подается удвоенное значение частичного остатка r_2, который импульсом Clok.1 передается на вход сумматора AddM2.1. На вторые входы при значении $b_{N-3}=1$ подается полином A(x). На выходах сумматора AddM2.1 формируется значение $C_3=A(x)\cdot b_{N-3} \oplus 2r_2$, который поступает на входы формирователя частичных остатков PRF1. На выходах PRF1 формируется частичный остаток r_3, который со сдвигом в сторону старшего разряда подается на входы сумматора AddM2.2. На вторые входы сумматора AddM2.2

подается результат логического умножения $A(x)\cdot b_{N4}$. При этом на выходах сумматора AddM2.2 формируется значение $C_4=A(x)\cdot b_{N-4}\oplus 2r_3$. Далее с помощью формирователя PRF.2 C_4 приводится по модулю P(x) вычисляя значение $r_4=C_4 \mathrm{mod} P(x)$.

Аналогично формируются другие частичные остатки. После подачи импульса $Clok._{K-1}$ регистр RgB сдвигается еще на два разряда влево и в его старших разрядах фиксируются множители b_1 и b_0. Счетчик Count установится в нулевое состояние и выработает сигнал «Конец операций», который и запрещает очередному импульсу Clok проходить на выходы схемы И1.

Далее импульсом $Clok._{K-1}$ на выходах PRF.1 и PRF.2 формируются r_{N-1} и r_{N-2} частичные остатки. Частичный остаток, полученный на выходах PRF.2, запоминается в RgPRF.2. После поступления сигнала с выхода элемента задержки DL.3 частичный остаток через блок схем И9 выводится на выход устройства. При этом величина задержки на DL.3 определяется временем формирования последних двух частичных остатков r_{N-1} и r_{N-2}.

Рассмотрим пример умножения полиномов по модулю неприводимого полинома. Пусть $A(x)=x^5+x^4+x+1$; $B(x)=x^5+x^3+x^2+1$. $P(x)= x^6+x+1$. Двоичное представления этих полиномов $A=110011_2$, $B=101101_2$ и $P=1000011_2$. Результаты вычисления приведены в таблице 1.

Табл. 1. Последовательность выполнения операции

	«START»	Clok.2	Clok.3
b_i, b_{i-1}	$b_5=1, b_4=0$	$b_3=0, b_2=1$	$b_1=1, b_0=1$
AddM2.1	$C_1=0+A(x)\cdot b_5=$ $=110011$	$C_3=2r_2\oplus A(x)\cdot b_3=$ 1001010 $\oplus$ 0110011 1111001	$C_5=2r_4\oplus A(x)\cdot b_1=$ $=0001000$
PRF1	$r_1=C_1 \mathrm{mod} P(x)=$ 0110011 $\oplus$ 1000011 0110011	$r_3=C_3 \mathrm{mod} P(x)=$ 1111001 $\oplus$ 1000011 0111010	$r_5=C_5 \mathrm{mod} P(x)=$ $=0001000$
AddM2.2	$C_2=2r_1\oplus A(x)\cdot b_4=$ $=1100110$	$C_4=2r_3\oplus A(x)\cdot b_2=$ 1110100 $\oplus$ 110011 1000111	$C_6=2r_5\oplus A(x)\cdot b_0=$ 0010000 $\oplus$ 110011 0100011
PRF2	$r_2=C_1 \mathrm{mod} P(x)=$ 1100110 $\oplus$ 1000011	$r_4=C_1 \mathrm{mod} P(x)=$ 1000111 $\oplus$ 1000011	$r_6=C_1 \mathrm{mod} P(x)=$ 0100011 $\oplus$ 1000011
RgPRF2	$r_2=0100101$	$r_4=0000100$	$r_6=0100011$

Проверка:

$$A(x)\cdot B(x)=(x^5+x^4+x+1)\cdot(x^5+x^3+x^2+1)=x^{10}+x^9+x^8+x^2+x+1;$$

$$x^{10}+x^9+x^8+x^2+x+1 \;\Big|\; x^6+x^5+1$$

$$
\begin{array}{l|l}
x^{10} + x^5 + x^4 & x^4 + x + 1 \\
\hline
x^9 + x^8 + x^5 + x^4 + x^2 + x + 1 & \\
x^9 \quad\quad + x^4 + x^3 & \\
\quad x^8 + x^5 + x^3 + x^2 + x + 1 & \\
\quad x^6 \quad + x^3 + x^2 & \\
\hline
\end{array}
$$

$x^5 + x + 1$, что соответствует → 100011_2.

Литература

1. Biyashev R., Kalimoldayev M., Nyssanbaeyeva S., Magzom M. Development of an encryption algorithm based on nonpositional polynomial notations // Proceeding of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). – Chiang Mai; Thailand, 2016. – P.243-245.

2. M. Kalimoldayev, S. Tynymbayev, S. Gnatyuk, M. Ibraimov, M. Magzom. The device for multiplying polynomials modulo an irreducible polynomial // News of the National academy of sciences of the Republic of Kazakhstan. series of geology and technical sciences, number 434 (2019), - P.199 – 2057

3. Калимолдаев М.Н, Тынымбаев С.Т, Магзом М.М, Ибраимов М.К, Кожагулов Е.Т. Устройство умножения полиномов по модулю непроводимых полиномов // Патент на изобретение РК №33810, Бюлл. №31 от 02.08.2019.

4. Biyashev R., Kalimoldayev M., Nyssanbaeyeva S., Magzom M., Development of an encryption algorithm based on nonpositional polynomial notations // Proceeding of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). – Chiang Mai; Thailand, 2016. – P.243-245.

5. Kalimoldayev M., Tynymbaev S., Magzom M., Ibraimov M., Khokhlov S., Abisheva A., Sydorenko V. Polynomials multiplier under irreducible polynomial module for high-performance cryptographic hardware tools // (2019) CEUR Workshop Proceedings, 2393, pp. 729-737. - https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069432716&partnerID=40&md5=35074925faba10fc9a96dd780cc09c63 (11/12/2019)

ОТКРЫТОЕ РАСПРЕДЕЛЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ САМОСЕРТИФИЦИРУЕМЫХ КЛЮЧЕЙ

Капалова Н. А., Варенников А.В.

e-mail: kapalova@ipic.kz, avarennikov@gmail.com

Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной работе рассматривается алгоритм безопасного (аутентифицированного) обмена криптографическими ключами, разработанный на основе самосертифицированных открытых ключей. В предложенной схеме открытые ключи не обязательно сопровождать отдельным сертификатом для аутентификации*

других пользователей. Идея заключается в том, что открытый ключ вычисляется как отправителем, так и получателем, сертификат «встроен» в открытый ключ, который он выдает, и, следовательно, не принимает форму отдельного значения.

1 Введение

Обеспечение информационной безопасности является одним из приоритетных направлений развития информационных технологий. Круг задач, решаемых в этой области, постоянно расширяется как в количественном, так и в качественном отношении. Одним из основных средств, используемых для защиты информации в компьютерных системах, являются криптографические преобразования. Современные криптографические методы используют криптографические ключи, которыми управляет система управления криптографическими ключами. Управление ключами является наиболее уязвимым местом криптографических приложений. Использовать криптографические технологии просто, однако безопасно хранить, использовать ключи и обмениваться ключами гораздо сложнее. Часто ненадежное управление ключами снижает качество даже исключительно хороших систем, так как безопасность алгоритма сосредоточена в ключе. Управление ключами включает процедуры генерации, накопления и распределения ключей [1-4].

Существующие методы генерации ключей можно разделить на аппаратные и программные. Основным требованием при этом является равномерность распределения по всему пространству возможных ключей. При генерации ключей аппаратным способом используются генераторы шума - электронные устройства, в которых протекает случайный физический процесс; при программной реализации - генераторы псевдослучайных последовательностей. Существуют определенные критерии при выборе генератора псевдослучайных чисел.

Организация накопления ключей связана с процедурами их хранения, учета и удаления. В достаточно сложной информационной системе один пользователь может работать с большим объемом ключевой информации, вследствие чего иногда возникает необходимость организации мини-баз данных по ключевой информации. Такие системы отвечают за принятие, хранение, учет и удаление используемых ключей. Информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются мастер-ключами и, как правило, не хранятся в компьютерной системе, для их преобразования используются криптографические алгоритмы. Количество используемых ключей зависит от числа абонентов, объема передаваемой информации и особенностей алгоритма шифрования. Сеансовые ключи должны уничтожаться.

Вопрос обновления ключей непосредственно связан с третьей проблемой управления ключами - распределением ключей. Распределение ключей - одна из фундаментальных задач криптографии, существуют несколько подходов:

– Физическое распределение.

– Выдача общего ключа участникам взаимодействия центром выдачи ключей - схема "абонентского шифрования".

– Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей пользователям.

– Сеть доверия. Используется в асимметричных криптосистемах. Пользователи сами распространяют свои ключи и следят за ключами других пользователей.

– Протоколы обмена ключами. Выработка секретного ключа и обмен им производится по незащищенным каналам связи между участниками взаимодействия, которые до этого не имели общего секретного ключа.

Недостаток методов, использующих центр распределения ключей, заключается в том, что в центре известно, кому и какие ключи назначены, что позволяет читать все сообщения, циркулирующие в информационной системе. При прямом обмене ключами возникает проблема аутентификации подлинности субъектов.

В зависимости от предъявляемых требований к уровню стойкости протоколы обмена ключами должны обладать рядом криптографических свойств.

1) Протокол обладает свойством контрибутивности, если сформированный ключ зависит от секретных данных, внесенных каждым из участников протокола.

2) Протокол обладает свойством совершенной опережающей секретности, если компрометация долговременных ключей (то есть долговременной секретной информации) не компрометирует сеансовых ключей (получаемых в результате выполнения протокола).

3) Протокол обеспечивает неявную аутентификацию ключа, если каждый участник протокола уверен, что никакая другая сторона не могла получить доступ к сеансовому ключу (за исключением злоумышленника внутри группы).

4) Протокол обладает свойством аутентичности, если он обеспечивает неявную аутентификацию ключа.

Из вышеизложенного следует, что управление ключами - это наиболее слабое место в криптографических приложениях. Безопасное хранение, использование ключей и обмен ключами являются важной частью СКЗИ. Для разработанной СКЗИ, точнее, для разработанных систем шифрования, будут проведены работы по построению системы управления криптографическими ключами и ее анализу. Проведены работы по разработке схемы распределение ключей с использованием самосертифицируемых ключей.

2 Открытое распределение криптографических ключей с использованием самосертифицируемых ключей

Известные схемы с открытым ключом были разработаны после предложенной в 1976 году концепции криптографии с открытым ключом [5]. В таких схемах у каждого пользователя есть пара ключей (СК, ОК). Первый, СК, является секретным ключом, известный только пользователю. Второй, ОК, является открытым ключом, который общедоступен. Два ключа, секретный и открытый, математически связаны.

Асимметричные системы шифрования из-за сложных вычислений, требуемых алгоритмами, уступают по скорости работы симметричным системам шифрования.

Симметричные криптосистемы быстрые, но имеют один существенный недостаток - это необходимость защищённой передачи ключей. Для преодоления этого недостатка прибегают к асимметричным криптосистемам. Например, для симметричного алгоритма генерируется случайный сеансовый ключ. Такой ключ, как правило, имеет размер от 128 до 512 бит (в зависимости от алгоритма). Этот ключ используется в симметричных алгоритмах для шифрования сообщения. Что касается самого случайного ключа, он должен быть зашифрован с помощью открытого ключа получателя сообщения, и именно на этом этапе применяется криптосистема с открытым ключом. Поскольку сеансовый ключ короткий, его шифрование занимает немного времени. Затем достаточно отправить сообщение, зашифрованное симметричным алгоритмом, а также соответствующий ключ

в зашифрованном виде. Получатель сначала расшифровывает ключ с помощью своего секретного ключа, а затем с помощью полученного ключа получает и всё сообщение.

Разрабатываемая система управления ключами предназначена для симметричных алгоритмов шифрования (разработанных в рамках других проектов лаборатории информационной безопасности ИИВТ КН МОН РК). Задача системы, каждый симметричный ключ (называемый сеансовым ключом) используется только один раз, и только для одного сообщения. Чтобы защитить сеансовый ключ, он зашифровывается открытым ключом получателя.

Для обеспечения подлинности (аутентификацию) отправителя и целостности сообщения используются множество методов и подходов, в том числе и самосертифицирующися открытые ключи.

В рекомендации CCITT X509 используется цифровая подпись [6], а в схемах, введенных Шамиром, открытый ключ - это не что иное, как идентификатор [7-9], в [10-12] используют схему цифровой подписи RSA и открытые ключи с самостоятельной сертификацией.

Предлагаемая схема основана на факторизации и задачах дискретного логарифма. Открытый ключ одновременно является гарантией его подлинности, который можно назвать самосертифицированным, и у каждого пользователя есть три атрибута (I, СК и ОК). Схемы с использованием самосертифицированных открытых ключей не основаны ни на сертификатах, поскольку не существует отдельного сертификата, ни на основе идентификационных данных, поскольку открытый ключ не ограничивается идентификацией. Как следствие, они способствуют уменьшению объема хранилища и вычислений (в частности, они не требуют хеш-функций на уровне полномочий), в то время как секретные ключи по-прежнему выбираются самим пользователем и остаются неизвестными другим участникам (и, в том числе, доверительному центру).

Разрабатываемая схема основана на модифицированной системе шифрования Эль-Гамаля и алгоритма RSA.

3 Модифицированная система асимметричного шифрования по схеме Эль-Гамаля.

Из результатов исследования схем распределения криптографических ключей и подходов по обеспечению аутентификации ключей, проведены работы по построению схемы открытого распределения криптографических ключей с использованием ранее предложенной модифицированной асимметричной системы шифрования Эль-Гамаля. Результаты разработки и исследования модификацированой системы асимметричного шифрования по схеме Эль-Гамаля с использованием непозиционных полиномиальных систем счисления (НПСС) опубликованы в работах [13-14]. Таким образом предлагаемая схема основана на гибриде модифицированной системы Эль-Гамаля и схемы RSA.

Разработанный ранее нетрадиционный асимметричный алгоритм шифрования электронного сообщения *M* по схеме Эль-Гамаля осуществляется следующим образом [14].

1) Вначале производится формирование НПСС: ее рабочими основаниями выбираются неприводимые многочлены

$$p_1(x), p_2(x),..., p_S(x) \tag{1}$$

над полем *GF*(2) степени m_1, $m_2, ..., m_S$, соответственно. Полиномы (1), с учетом порядка их расположения, образуют одну систему оснований. Все основания должны быть различными, и в том случае, если они имеют одну степень (для выполнения китайской теоремой об остатках). Рабочий диапазон НПСС определяется многочленом (модулем)

$$P_S(x) = p_1(x)p_2(x)\cdots p_S(x)$$

степени $m = \sum_{i=1}^{S} m_i$. В НПСС любой многочлен $F(x)$ степени меньше m имеет единственное непозиционное представление вида

$$F(x) = (z_1(x), z_2(x), ..., z_S(x)), \tag{2}$$

где $F(x) \equiv z_i(x)(\mathrm{mod}(p_i(x))$, $i = \overline{1,S}$. По виду (2) восстанавливается позиционное представление $F(x)$ следующим образом:

$$F(x) = \sum_{i=1}^{S} z_i(x)B_i(x), \text{ где } B_i(x) = \frac{P_S(x)}{p_i(x)}M_i(x) \equiv 1(\mathrm{mod}\, p_i(x)). \tag{3}$$

Выбор многочленов $M_i(x)$ осуществляется таким образом, чтобы выполнялось сравнение в (3).

2) Для каждого основания $p_i(x)$ выбирается примитивный элемент (многочлен) $\alpha_i(x)$ из полной системы вычетов по модулю $p_i(x)$, т. е. степени $\alpha_i(x)$ не превышают m_i, где $i = \overline{1,S}$. Тогда примитивный элемент в модифицированном нетрадиционном алгоритме шифрования интерпретируется как последовательность остатков от деления некоторого многочлена $\alpha(x)$ на основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно:

$$\alpha(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)) \ ,$$

где $\alpha(x) \equiv \alpha_i(x)(\mathrm{mod}\, p_i(x))$, $i = \overline{1,S}$.

Выбранные рабочие основания и соответствующие им примитивные многочлены $\alpha_i(x)$ держатся в секрете.

Для восстановления результата в позиционном виде по его остаткам определяются базисы НПСС по формуле (3). Для этого вычисляются многочлены $\delta_i(x) \equiv \frac{P_S(x)}{p_i(x)}(\mathrm{mod}\, p_i(x))$ и инверсные к ним полиномы $\delta_i^{-1}(x) \cdot \delta_i(x) \equiv 1(\mathrm{mod}\, p_i(x))$. Тогда базисы находятся по формуле $B_i(x) = \delta_i^{-1}(x) \cdot \frac{P_S(x)}{p_i(x)}$, которые также являются секретными параметрами алгоритма.

3) Затем пользователи *A* и *B* независимо друг от друга выбирают соответственно личные (закрытые) ключи l_A и l_B такие, чтобы $1 < l_A, l_B < 2^m$.

4) Потом пользователи *A* и *B* вычисляют третий элемент открытого ключа, соответственно:

$$\beta_A(x) = (\beta_{A_1}(x), \beta_{A_2}(x), ..., \beta_{A_S}(x)), \text{ где } \beta_{Ai}(x) \equiv \alpha_i^{l_A}(x)(\mathrm{mod}(p_i(x))),\ i = \overline{1,S};$$

$$\beta_B(x) = (\beta_{B_1}(x), \beta_{B_2}(x), ..., \beta_{B_S}(x)), \text{ где } \beta_{Bi}(x) \equiv \alpha_i^{l_B}(x)(\mathrm{mod}(p_i(x))),\ i = \overline{1,S}.$$

Все операции возведения в степень производятся в непозиционной полиномиальной системе счисления, поэтому вычисление этих операций может выполняться параллельно по модулям полиномов, выбранных в качестве оснований системы.

5) После этого стороны *A* и *B* обмениваются вычисленными значениями открытых ключей, $K_A(x) = (P_S(x), \alpha(x), \beta_A(x))$, $K_B(x) = (P_S(x), \alpha(x), \beta_B(x))$, соответственно, по незащищенному каналу в двоичном представлении.

6) Используя открытые ключи адресата пользователи *A* и *B* выполняют процесс шифрования E_k сообщения *M* по аналогии с традиционной схемой Эль-Гамаля: $E_k(M) = (C_1, C_2)$, где $C_1 = \alpha^r(\mathrm{mod}(P_S(x))$, $C_2 = M \cdot \beta^r(\mathrm{mod}(P_S(x))$, где *r* - случайно выбираемое число (рандомизатор) и $0 \le r \le 2^m$ (также для каждого рабочего основания можно выбирать разные рандомизаторы).

7) Для расшифрования D_k зашифрованного сообщения пользователи *A* и *B* используют свои личные ключи в соответствии с формулой: $D_k(C_1, C_2) = C_2 \cdot (C_1^{l_i})^{-1} \bmod P_S(x) = M$, где $i = A, B$.

Все вычисления в НПСС могут производиться параллельно по модулям рабочих оснований $p_1(x), p_2(x), ..., p_S(x)$, вследствие этого возможно существенное возрастание скорости выполнения операций.

4 Разработка схемы открытого распределения криптографических ключей.

Рассматриваемая схема предполагает, что пользователи по принципу доверие могут подтвердить подлинность открытых ключей друг друга. Допустим, пользователи *A* и *C* доверяют пользователю *B*. Для того чтобы установить доверие между *A* и *C* пользователь *B* выступает гарантом при проверке подлинности ключей.

Как описано выше, открытыми ключами пользователей *A*, *B* и *C* являются $K_A(x) = (P_S(x), \alpha(x), \beta_A(x))$, $K_B(x) = (P_S(x), \alpha(x), \beta_B(x))$ и $K_C(x) = (P_S(x), \alpha(x), \beta_C(x))$. Для того, чтобы открытые ключи обладали свойством самостоятельной сертификации (без центра доверия), используем алгоритм RSA. Краткое описание приведено ниже.

1) В процессе вычисления открытых ключей (пункты 1-4 раздела 3) дополнительно выбираются простые числа *p* и *q*;

2) Аналогично алгоритму RSA каждый пользователь: вычисляет $n=p \cdot q$, выбирает *e* и вычисляет *d*, где $e \cdot d = 1 \bmod \varphi(n)$;

3) Затем публикуются открытые ключи:

$K_A(x) = (P_S(x), \alpha(x), \beta_A(x), e_A, n)$, $K_B(x) = (P_S(x), \alpha(x), \beta_B(x), e_B, n)$ и

$$K_C(x) = (P_S(x), \alpha(x), \beta_C(x), e_C, n);$$

4) Далее пользователь *A* доказывает пользователю *C*, что он является именно *A*. Это можно сделать с помощью следующего протокола. Пользователь *B* вычисляет $S_A = (\beta_A(x) + I_A)^{d_B}$ для пользователя *A*, который принимается в качестве сертификата. По значению S_A можно убедиться, что оно принадлежит пользователю *A*. Для этого нужно вычислить значения $(S_A{}^{e_B} + I_A) \bmod n$ и проверить, совпадает оно ли с $\beta_C(x)$.

Заключение

Работа выполнена в рамках программы грантового финансирования AP05132568 «Разработка системы управления криптографическими ключами» Министерства образования и науки Республики Казахстан.

Литература

1. Barker E. Recommendation for Key Management – Part 1: General / NIST Special Publication 800-57, Revision 4. – 2016. – 160 p.

2. Barker E., Smid M., Branstad D., Chokhani S. A Framework for Designing Cryptographic Key Management Systems / NIST Special Publication 800-130, Revision 4. – 2013. – 120 p.

3. Капалова Н.А., Абишева А.Ж. Орталықтандырылған криптографиялық кілттерді басқару жүйесі // Матер. IV междунар. науч.-практ. конф. «Информатика и прикладная математика». – Алматы, 2019. – С. 569-575.

4. Варенников А.В. «Краткий обзор основных принципов разработки систем управления криптографическими ключами» // Матер. науч. конф. «Современные проблемы информатики и вычислительных технологий». – Алматы, 2019. – С. 154-160.

5. Diffie W. and Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. – 1976. - Vol.1, T.22. - P.644-654.

6. [X.509-00] ITU-T. Recommendation X.509: The Directory — Authentication Framework, 2000 // https://www.itu.int/rec/T-REC-X.509: 05.2019.

7. Fiat A. and Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Proc. of CRYPTO86, Advances in Cryptology. - Springer-Verlag, 1987. - P.186-194.

8. Shamir A. Identity-based cryptosystems and signature schemes // Proc. of CRYPT0'84. Advances in Cryptology. - Springer-Verlag, 1985. - P.47-53.

9. Guillou LC. and Quisquater J.J. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory // Proc. of EUROCRYPT88. Advances in Cryptology. - Springer-Verlag, 1988. - P. 123-128.

10. Paillts J.C. and Girault M. CRIPT: A public-key based solution for secure data communications // Proc. of SECURICOM. – 1989. - P.171-185.

11. Girault M. and Pailles J.C. An identity-based identification scheme providing zero-knowledge authentication and authenticated key exchange // Proc. of ESORICS. – 1990. - P.173-184.

12. Girault M. An identity-based identification scheme based on discrete logarithms modulo a composite number // Proc. of EUROCRYPT90. - Springer-Verlag, 1991. - P.481-486.

13. Капалова Н.А. Исследование криптостойкости алгоритма шифрования Эль-Гамаля на базе непозиционных полиномиальных систем счисления // Информационная безопасность. Матер. XII Межд. науч.-практ. конф. - Таганрог, ТТИЮФУ, 2012. – Ч. 1. - С. 253-258.

14. Капалова Н.А. Модифицированный алгоритм шифрования Эль-Гамаля на базе непозиционных полиномиальных систем счисления // Известия Национальной академии наук РК. – Алматы, 2013. – № 1. – С. 22-26.

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СИСТЕМ РАСПРЕДЕЛЕНИЯ СЕКРЕТА НА ОСНОВЕ ЛАТИНСКИХ КВАДРАТОВ

Кырыкбаев Н.С.
e-mail: kyrykbayev.nurbol@gmail.com
Казахский Национальный Технический Университет имени К.И.Сатпаева,
Казахстан, г. Алматы

Аннотация. *В статье рассмотрены вопросы проектирования системы распределения секретов на основе латинских квадратов. Данная задача предполагает построение схемы распределения секрета между участниками обмена и расчет числа критических множеств для конкретного числа участников этого обмена.*

Ключевые слова. *Схемы распределения секрета, латинский квадрат, криптография, шифрование, информационная безопасность.*

Введение

В системах, основанных на информации, целостность информации обычно обеспечивается за счет того, что определенные операции могут выполняться только одним или несколькими участниками, имеющими права доступа. Доступ достигается с помощью ключа, пароля или токена и управляется схемой управления безопасными ключами. Если ключ или пароль разделяются между несколькими участниками таким образом, что его можно восстановить только достаточно большая и ответственная группа, действующая в согласии, тогда достигается высокая степень безопасности.

Общие системы безопасности такого рода также используются в финансовых учреждениях, сетях связи, в вычислительных системах, обслуживающих образовательные учреждения и среды распространения. Однако наиболее известные примеры применения общих систем безопасности находятся в армии: например, при активации ядерного оружия несколько старших офицеров должны согласиться, прежде чем восстановить необходимый пароль.

Общие секретные схемы были впервые введены Блекли, Шамиром и Чаумом в 1979 году и впоследствии изучены многими другими авторами. Для общего обсуждения общих схем секретности и моделирования общих секретных схем использовался ряд математических структур. Некоторые из них представляют собой полиномы,

геометрические конфигурации, блок-схемы, коды Рида-Соломона, векторные пространства, матроиды, правые поля, полные многопартийные графы и ортогональные массивы.

Актуальность исследуемого вопроса состоит в том, что в большинстве приложений реального мира требуется, чтобы иерархия была встроена в общую систему безопасности. Для этого ключ и пароль распределяются между s-индивидами ранга 1, ..., r, так что если человек ранга i является недееспособным, тогда человек ранга j> i или набор индивидуумов ранга l < i, может заменить потерянные данные.

Практическая часть

Известно, что перестановки с структурой цикла (n / 2) + (n / 2) являются даже перестановками. Из n! / 2 даже перестановок точно 2 (n - 1)! / n имеют структуру цикла (n / 2) + (n / 2). Таким образом, если выбираем изотопизм равномерно случайным образом из An x An x An (где An - переменная группа), то имеет место вероятность быть подходящим.

$$(\frac{2(n-1)!/n}{n!/2})^3 = 64/n^6 \quad (1)$$

Вероятность (C, θcand) порождает латинский квадрат, когда θcand случайный.

Имеем p равное:

- Pr [(C, θcand) порождает латинский квадрат];
- Pr [ϕ−1(C), ϕ−1θcand ϕ) порождает латинский квадрат];
- Pr [(Cprior, ϕ−1θcandϕ) генерирует латинский квадрат];
- Pr [(Cprior, θ cand) генерирует латинский квадрат].

Так как θcand и ϕ−1θcandϕ равны в распределении. Это использовалось для упрощения метода, используемого в симуляциях. z

Для n = 6 генерируем 109 пар (Cprior, β) для случайного подходящего автотопизма β и находим 43409 порождаем латинский квадрат. Верхняя граница доверительного интервала Вальда составляет 4,5 x 10-5 с доверием 99,995%. При n = 10 сделали N: = 3,6 × 1011 выборок, и ни один латинский квадрат не был сгенерирован таким образом.

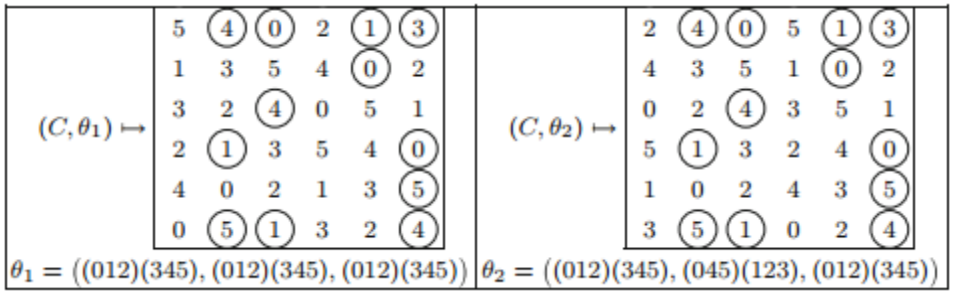


Рисунок 1 - Контур C (образованный круговыми элементами), для которых (C, θ1) и (C, θ2) генерируют два отдельных латинских квадрата.

Выбор среды разработки

Выбор пал на такие инструменты как Microsoft Visual Studio 2017 и C++ как язык программирования. Они идеально подходят под тип данных с которым я работаю.

Моделирование

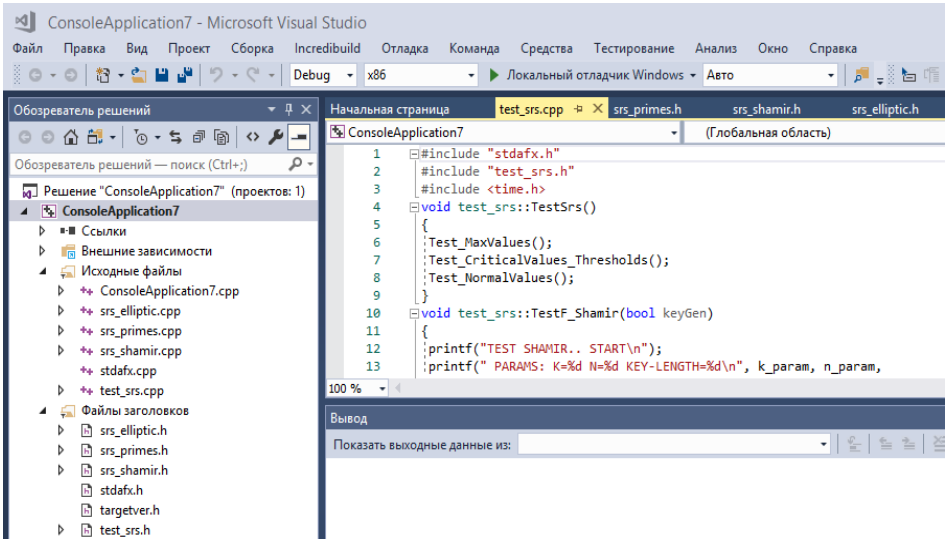


Рисунок 2 - Интерфейс и исходные коды программы в Visual Studio

Интерфейс среды разработки достаточно эргономичен и у новичка не возникнет особых трудностей с его освоением. Слева можно увидеть окно с тремя вкладками: проекты, файлы и службы. Во вкладке проекты находятся непосредственно папки проектов с разветвляющейся структурой. Во вкладке файлы мы можем открыть файл, запустить какой-либо отдельный модуль разрабатываемого приложения. Во вкладке службы мы видим первую ветвь - базы данных в которой имеется папка с необходимыми драйверами для подключения баз данных и др.

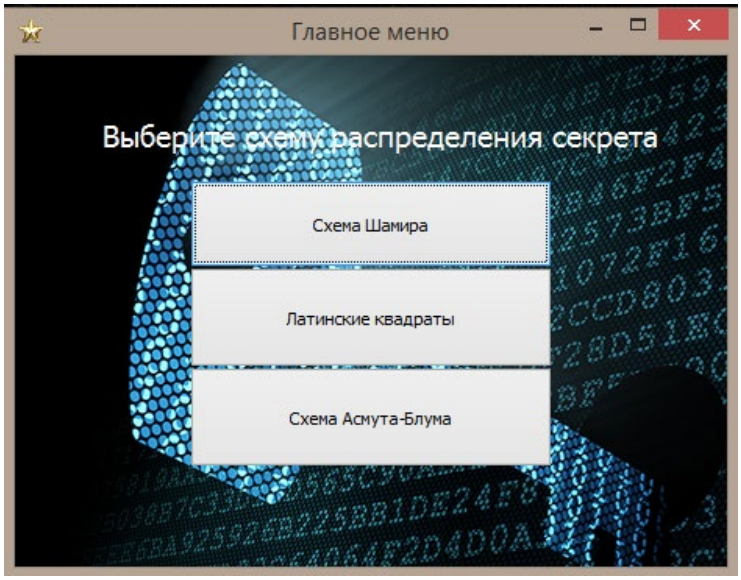


Рисунок 4 - Интерфейс программы

Здесь можно наблюдать главное меню программы, в которой указаны схемы распределения секрета, по которым были разработаны отдельные программы.

Результаты тестирования

Таблица 1 – Результаты тестирования всех трех СРС

Схема распределения секрета	N=5,K=3, |M|=512	N=K=32, |M|=512	N=K=128, |M|=512
СРС Шамира			
Время разделения	5 мс;	7 мс;	75 мс;
Время восстановления	1 мс;	2 мс;	27 мс;
Объем требуемой памяти	560 байт	20 байт	1006008 байт
СРС Асмута-Блума			
Время разделения	103 мс;	1145 мс;	3032 мс;
Время восстановления	1 мс;	4 мс;	97 мс;
Объем требуемой памяти	3456 байт	274432 байт	4243456 байт
СРС Латинских квадратов			
Время разделения	15 мс;	1058 мс;	85193 мс;
Время восстановления	1 мс;	617 мс;	47326 мс;
Объем требуемой памяти	1365 байт	6432 байт	99456 байт

Заключение

В статье привел пример проектирования и реализовал программу для схемы секретного обмена на основе автокопий на основе латинского квадрата, которая решает множество проблем, возникающих в предыдущих предложенных схемах секретного совместного использования в Латинском квадрате. Эти проблемы преодолеваются, прежде всего, с помощью секретного автотопизма (симметрии), а не секретного латинского квадрата. Мотивированные значительной критикой в отношении секретных схем использования латинского квадрата в прошлом, проводим тщательный анализ предлагаемой схемы с точки зрения сложности и безопасности.

Эта работа еще раз показывает, что латинские квадраты могут быть полезны для разработки практических схем секретного обмена, и может обеспечить практическую альтернативу установленным схемам. Предлагаемая схема также имеет существенную выгоду по сравнению с традиционными схемами: проверка, например Участники, могут быть уверены, что вернувшаяся тайна действительно является правильной тайной. В одном будущем направлении, которое может быть предпринято этим исследованием, заключается в поиске способов определения того, какие акции являются неправильными, а ситуация, когда возвращаются некорректные доли. Один из методов заключается в том, чтобы сделать общедоступную криптографическую функцию хэш-функции для акций, хотя это (а) кажется «излишним» для данной проблемы, и (б) может использоваться для любой схемы секретного обмена. Другая возможность заключается в кодировании случайных записей латинского квадрата L в акции, однако это открывает новые возможные уязвимости безопасности.

Литература

1. McKay B. D. and Wanless I. M. On the number of Latin Squares // Ann. Combin. 2005. No. 9. P. 335–344.

2. Laywine C. F. and Mullen G. L. Discrete mathematics using Latin squares. New York: Wiley, 1998. Trithemius J. Polygraphiae. 1518.

3. Shannon C. Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. No. 15(2). P. 125–156.

4. Massey J. L., Maurer U., and Wang M. Non-Expanding, Key-Minimal, Robustly-Perfect, Linear and Bilinear Ciphers // Adv. Cryptology — EUROCRYPT'87. Berlin, Heidelberg: Springer Verlag, 1988. P. 237–247.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ОЦЕНКИ АКУСТИЧЕСКОЙ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ

Кзылбаев М.С.
e-mail: kzylbayev.mukhammed@gmail.com
Казахский национальный исследовательский технический университет имени К. И. Сатпаева, Казахстан

Аннотация. *Защита акустической информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта технической защиты. Важными этапами защиты акустического канала являются оценка и периодический контроль изоляционных свойств ограждающих конструкций. В статье представлена разработанная программа, которая предусматривает возможность предварительной оценки помещений с использованием дополнительного оборудования. Рассмотрены основные алгоритмы работы программного обеспечения. Представлен анализ результатов и оценена точность разработанного программного обеспечения.*

Ключевые слова: *акустический канал, утечка речевой информации, контроль безопасности помещений, акустическая изоляция помещений, формирование протокола, автоматизированная система оценки.*

1. Введение

В современном информационном обществе информация является одним из важных ресурсов любого государства. Наиболее распространенной и наиболее незащищенной формой передачи данных является акустическая.

В условиях конкурентной практики и стремления к достижению научно-технического превосходства важную роль играют различные виды технического мониторинга. С другой стороны, разведывательные средства и системы рекогносцировки речевой информации постоянно совершенствуются и подвергаются модификации. Поэтому защита от утечки данных по техническим каналам была сформирована как неотъемлемая часть контрпроверки к мониторингу, особенно к техническим компонентам.

Основные требования к встречной проверке мониторинга присущи мерам защиты информации. Мероприятия по защите акустической информации подразделяются на пассивные и активные методы [3].

Одним из основных методов пассивной защиты акустической информации является обеспечение требуемых изоляционных свойств ограждающих конструкций контролируемой зоны. Поэтому оценка изоляционных свойств ограждающих

конструкций является актуальной проблемой и является основой для принятия мер по защите речевой информации.

2. Канал утечки акустической информации

Речевая (виброакустическая) информация может быть подслушана с помощью микрофонов воздушной проводимости, зафиксирована с помощью микрофонов твердой среды (виброметров, велосиметров, акселерометров) или непосредственно прослушана человеком. Структура акустического канала утечки информации показана на рисунке 1.

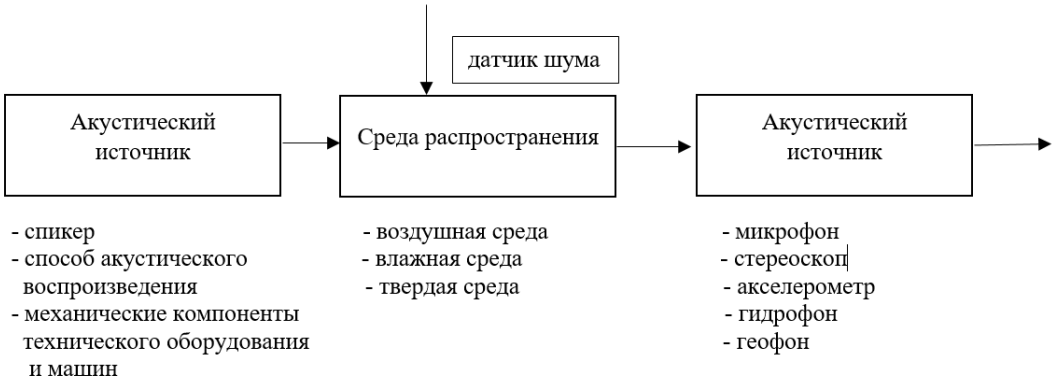


Рис. 1 Структура акустического канала утечки информации.

Спектр речевого сигнала изменяется в процессе произнесения различных звуков. В этом процессе одни гармонические составляющие усиливаются, другие подавляются. Области спектра, в которых сосредоточена основная мощность акустического сигнала, называются формантами. Форматы звуков речи располагаются в диапазоне частот от 150-200 до 8600 Гц. Основная энергия формантной мажоритарной части сосредоточена в диапазоне частот 300-3000 Гц, что позволило ограничить спектр речевого сигнала, передаваемого по стандартному телефонному каналу этой полосой [2-5]. Среда распространения носителя информации от источника к приемнику может быть однородной и неоднородной, она может образовываться последовательными участками различных физических сред: воздуха, деревянных дверей, стеклянных окон, бетонных или кирпичных стен, различных горных пород на поверхности земли и др. Но даже в однородной среде ее параметры не постоянны, они могут существенно отличаться в различных точках [1].

Основным информационным показателем утечки речевой информации по акустическому (виброакустическому) каналу является вербальная разборчивость речи. Этот информационный показатель нормализуется и используется для принятия решения о наличии утечки речевой информации[3].

Вербальная разборчивость речи W рассчитывается по формуле:

$$W = \begin{cases} 1{,}54R^{0.25}[1-\exp(-11R)], & \text{if } R < 0{,}15, \\ 1-\exp\left[\dfrac{-11R}{1+0.7R}\right], & \text{if } R \geq 0{,}15, \end{cases} \quad (1)$$

-где R-интегральный показатель артикуляции речи.

Интегральный показатель артикуляции определяется по формуле:

$$R = \sum_{i+1}^{5} r_i, \quad (2)$$

где r_i – октавной индекс артикуляции речи. Индекс октавном артикуляции определяется по формуле:

$$r_i = k_i \left\{ z - \frac{0{,}78 + 5{,}46\exp[-4{,}3 \cdot 10^{-3}(27{,}3 - |E_i - A_i|)]}{1 + 10^{0{,}1|E_i - A_i|}} \right\} \quad (3)$$

- где $z = \begin{cases} 0, & if\ E_i \le A, \\ 1, & if\ E_i > A, \end{cases}$;

A_i – параметр формата спектра речевого сигнала в октавном диапазоне, dBA;

K_i – весовой коэффициент октавной полосы;

E_i – октавный параметр отношений: акустический (виброакустический) сигнал / шум, при возможном размещении звуковых приемников (микрофонов) и виброприемников (вибродатчиков) аппаратуры акустической речевой разведки (в месте возможного прослушивания речи без использования технических средств).

Из Формулы (3) следует, что для снижения разборчивости речи необходимо уменьшить соотношение "уровень речи / уровень шума" (сигнал / шум) в местах возможного размещения датчиков аппаратуры акустической разведки.

Снижение отношения сигнал / шум возможно либо за счет снижения уровня речевого сигнала (пассивные методы защиты), либо за счет повышения уровня шума за счет создания акустических и вибрационных помех (активные методы защиты). Снижение силы акустических (речевых) сигналов достигается за счет звукоизоляции помещений, которая направлена на локализацию источников акустических сигналов внутри них[4].

Звукоизоляция оценивается по величине потерь мощности акустического сигнала и обеспечивается архитектурными и инженерными решениями, а также применением специальных строительных и отделочных материалов[1]. В случае, если звукоизоляция помещений не обеспечивает требуемой эффективности защиты информации, применяются специальные звукопоглощающие материалы.

3. Оценка защиты от утечки по акустическому каналу. Программное обеспечение ASL

Для оценки защиты от утечки через акустический канал разработано программное обеспечение ASL. Это программное обеспечение разработано с использованием объектно-ориентированного языка программирования C # на платформе программного обеспечения версии 4.5.2

Созданное программное обеспечение ASL обеспечивает следующие функции:

1. Проводить автоматизированные измерения и расчеты изоляционных свойств ограждающих конструкций, что значительно упрощает процедуру анализа полученных данных и снижает затраты на проведение измерений;
2. Формирование и ведение базы данных актуальной информации об объекте и результатах измерений;
3. Рассчитать показатели защищенности выделенных помещений от утечки акустического канала при заданных стандартизированных показателях защищенности информации;

4. Сформировать необходимые протоколы и выводы.

Функционирование программы организовано в 4 основных этапа, которые последовательно связаны между собой (Рисунок 2).

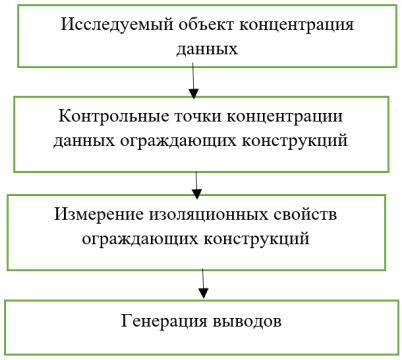


Рис. 2 Управления-схема программы на языке жестов.

Первым шагом в анализе безопасности объекта через акустический канал является концентрация данных. Эти данные включают в себя:

- общая информация;
- условия размещения исследуемого объекта;
- перечень организационно-распорядительной и эксплуатационной документации;
- дополнительная информация.

Второй этап программы ASL предполагает уточнение контрольных точек ограждающих помещений, для которых будет произведена оценка звукоизоляционных свойств. Следует отметить, что в результате первого и второго этапа формируется полный отчет о проверке помещений. Также в программе предусмотрено сохранение полученных данных в базе данных для дальнейшего повторного использования.

Отличительной особенностью программного обеспечения ASL является возможность формирования автоматизированного комплекса для проведения аудита акустической защиты помещений с использованием дополнительного оборудования.

Разработанное программное обеспечение основано на методе измерения звукоизоляционной способности ограждающих конструкций защищаемых помещений, в котором передающая измерительная система должна содержать: генератор шума; усилитель; акустическую систему. Структурная схема оборудования для создания звукового сигнала приведена на рисунке 3. Приемная измерительная система должна содержать: шумомер с микрофоном.

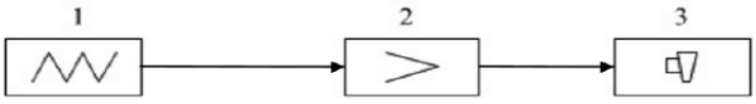


Рис. 3 Контрольно-технологическая схема оборудования, генерирующего тестовый сигнал.
(1-генератор шума, 2-усилитель мощности, 3 - акустическая система)

Разработанное программное обеспечение позволяет усилить мощность генерации шума с помощью ПК. Рекомендуется использовать ноутбук с поддержкой Bluetooth в качестве ПК для дополнительного удобства. это объясняется тем, что в качестве акустической системы можно использовать беспроводной динамик необходимой мощности. Для автоматизированной записи результатов измерений рекомендуется использовать шумомеры CEM модельного ряда DET с дополнительной конфигурацией COM-порта.

При переходе к шагу 3 раздела "измерение изоляционных свойств" необходимо учитывать, что каждая компьютерная томография выполняется в два этапа. Первый этап измерения проводится в помещении, второй-измерения в контрольно-пропускном пункте. Поэтому перед началом сканирования пользователь должен выбрать опорную точку и расположение шумомера, а также указать порт подключения шумомера.

Программное обеспечение ASL позволяет проводить измерения в быстром или точном режиме. Разница между этими режимами заключается в количестве измерений в наборе для каждого октавного диапазона. Для быстрого сканирования число измерений равно 10, а для режима точности - 100. На рисунке 4 показано окно программы ASL в процессе сканирования.

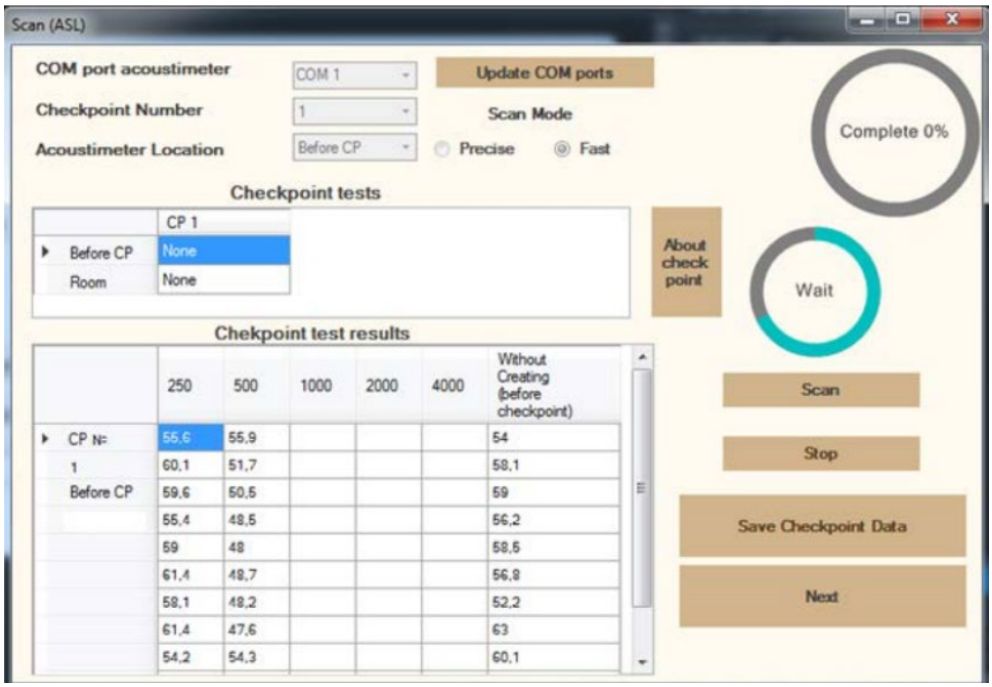


Рис. 4 Окно программного обеспечения ASL во время сканирования.

В качестве тестового сигнала программа генерирует пилообразный сигнал. Октавные уровни испускаемого испытательного сигнала в помещении калибруются в ручном режиме, регулируя уровень громкости акустического источника. Частота выходного акустического сигнала изменяется в автоматическом режиме.

При сохранении данных контрольных точек программа выполняет статистический анализ данных на наличие аномальных значений. Принцип этого метода заключается в определении среднего значения и дисперсии в каждой октавной полосе. Значение измерения, которое превышает отклонение в размере двух отклонений, отмечено в

таблице измерений. Сохранение данных ограничивается количеством неудовлетворительных баллов по критериям отбора. Если количество таких точек превышает пороговое значение 20% хотя бы в одном октавном диапазоне, пользователь получает уведомление о том, что результаты не могут быть сохранены. Для успешного сохранения данных пользователь должен устранить факторы, повлиявшие на неверный результат, и повторить измерения.

4. Оценка и тестирование созданного программного обеспечения

Качество программного обеспечения можно оценить, как соответствие четко установленным функциональным и эксплуатационным требованиям. Основными требованиями к разработанному программному обеспечению ASL являются удобство использования и адекватность результатов. Полученные результаты программного обеспечения должны быть оценены до сертификации и выпуска, так как это является основным фактором, влияющим на качество продукта. Выполнение остальных требований оценивается пользователями в процессе эксплуатации разработанного программного обеспечения.

Оценка результатов работы программного обеспечения ASL проводилась путем сравнения с данными, полученными непосредственно с шумомера. Разработанный программный продукт сканирует внутренний тестовый сигнал, показатель шума и общее значение отношения сигнал / шум в контрольной точке. Для оценки было решено использовать значения сигнала / шума в контрольных точках. Объем контрольных измерений равен 50. Программное обеспечение ASL снимает показания с интервалов времени 0,5 секунды, но физиологическая особенность человека не позволяет вести запись на этой частоте. Поэтому количество контрольных измерений было сокращено до 25. Результаты измерения в октавном диапазоне 250 Гц приведены на рисунке 3. Сравнительный анализ данных, полученных двумя методами, выявил несущественное отклонение значений сигнал / шум с помощью программного обеспечения ASL и шумомера. Это отклонение связано с округлением показаний шумомера до десятичного знака. Поэтому показания программного обеспечения ASL можно считать равными значениям шумомера. Например, на рисунке 5 имеется разброс показаний относительно фактического значения. Это связано с наличием такого внешнего фактора, как переменный фоновый шум в контрольных точках. При выполнении измерений без вспомогательного программного обеспечения пользователь должен выполнить анализ данных вручную. Программное обеспечение ASL позволяет упростить эту процедуру.

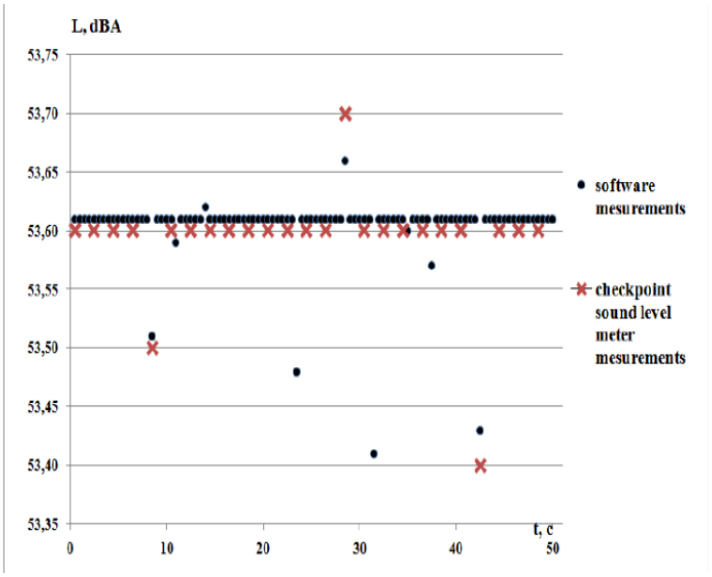


Рис. 5 Измерение сигнала / шума в октавном диапазоне 250 Гц

Завершив оценку программного обеспечения САУ, доказано, что разработанный программный продукт, измеряющий уровень сигнала / шума, имеет достоверные данные на выходе и упрощает процедуру анализа полученных данных.

5. Выводы

На данный момент на рынке представлено большое количество различных аппаратных и программных решений для оценки эффективности обеспечения безопасности помещений, которые имеют ряд преимуществ и недостатков. Основным недостатком оценочных комплексов является их стоимость. Разработанное программное обеспечение позволяет оценить изоляционные свойства для собственных целей перед аттестацией или периодическими испытаниями.

Для совершенствования программы в дальнейшем предлагается использовать метод измерения вербальной разборчивости, результаты которого будут являться количественным показателем. Также ведется работа по расширению перечня шумомеров, совместимых с разработанным программным обеспечением.

Литература

1. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. — М.: Гелиос АРВ, 2005. – 960 с.

2. Диогенес Ю. Кибербезопасность / Ю.Диогенес – ДМК Пресс.2019 – 58-80с.

3. Коллинз М. Защита сетей. Подход на основе анализа данных / М. Коллинз – ДМК Пресс.2019-15-20с.

4. Никифоров С.Н. Методы защиты информации. Защищенные сеты / С.Н.Никифоров – Лань. 2018.- 90-120с.

5. Михайлова У.В., Хусаинов А.А. Особенности и проблемы, возникающие при разработке моделей угроз информационной безопасности /У.В. Михайлова, А.А. Хусаинов - Безопасность информационного пространства: сб. материалов XV Всеросс. науч.-практич. конф. студентов, аспирантов и молодых ученых. под ред. Д.И. Дик. Курган: ФГБОУ ВО «Курганский государственный университет». 2016. с. 72-75.

6. Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для оценки уровня сформированности компетенций специалиста по информационной безопасности / И.И.Баранкова, У.В. Михайлова - Информационное противодействие угрозам терроризма. 2015. Т. 2. № 25. с. 26-30.

УПРАВЛЕНИЕ АУТЕНТИФИКАЦИЕЙ И АВТОРИЗАЦИЕЙ В МУЛЬТИПЛАТФОРМЕННЫХ СИСТЕМАХ

Магзом М.М., Тананова Д.Д.
e-mail: magzomxzn@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данном докладе рассмотрены вопросы управление процессами аутентификации и авторизации в мультиплатформенных системах, состоящих из различных микросервисов. Сложности реализации и поддержки подобных систем заключается в обеспечении гибкости политики безопасности, управлении учетными данными пользователей, их ролями и доступами в системе. Предложен подходи реализации системы аутентификации и авторизации на основе BPM системы.*

Введение

Аутентификации пользователей – важнейший компонент системы информационной безопасности, и ее значение трудно переоценить. Система аутентификации подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа [1].

Авторизация пользователей – это процесс подтверждения прав на совершение определенных операций. Он необходим для обеспечения безопасности при совершении действий, для разграничения прав пользователей, для защиты от злоумышленников.

Таким образом, аутентификация — процедурой проверки легальности пользователя или данных, например, проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных, или проверка цифровой подписи письма по ключу шифрования, или проверка контрольной суммы файла на соответствие заявленной автором этого файла. Авторизация же производит контроль доступа к различным ресурсам системы в процессе работы легальных пользователей после успешного прохождения ими аутентификации [2].

В данном докладе предлагается подход к выполнению процедур аутентификации и авторизации в мультиплатформенных системах. Основные задачи при разработке подобных систем заключаются в обеспечении гибкости политики безопасности, управлении учетными данными пользователей, их ролями и доступами в системе. Рассмотрит структуру мультиплатформенных систем.

Архитектура мультиплатформенных систем

Сегодняшние сети и построенные на их основе информационные системы назвать статичными. Распределенные и мультиплатформенные системы, облачные сервисы,

системы виртуализации и микросервисы привели к тому, что управлять при помощи традиционных инструментов становится невозможно. Серверы могут перемещаться, сервисы появляются и отключаются.

Традиционно, простейший и популярный вариант архитектуры информационных систем – монолитная. Обычно простые проекты начинают с неё, и здесь нет никакой изоляции и распределённости: один монолит обрабатывает все запросы.

Отчего возникают следующие проблемы:

- отказоустойчивость;
- горизонтальное масштабирование;
- применение одной технологии или языка и невыгодность переписывать огромный монолит;
- сложность рефакторинга из-за хранения кода в одном месте и куча legacy кода, который необходимо поддерживать;
- трудности работы в команде разработчиков;
- чтобы использовать повторно, придётся дробить компоненты архитектуры.

Второй по популярности вид архитектуры – пара монолитов, объединение из монолита и сервисов или даже микросервисов. То есть вы сохраняете монолит, а доработки выполняете с использованием современных технологий.

Это частично решает проблемы отказоустойчивости, масштабируемости и одного стека технологий.

Микросервисная архитектура – не новая идея, а разновидность сервис-ориентированной архитектуры. Сервис-ориентированная архитектура предусматривает модульность разработки и слабую связанность компонентов, поэтому получаем изолированную и распределённую систему.

Главный минус – общая шина данных Enterprise Service Bus с огромными спецификациями и сложностями работы с абстракциями и фасадами.

Общие структуры описанных подходов показаны на рисунке 1.

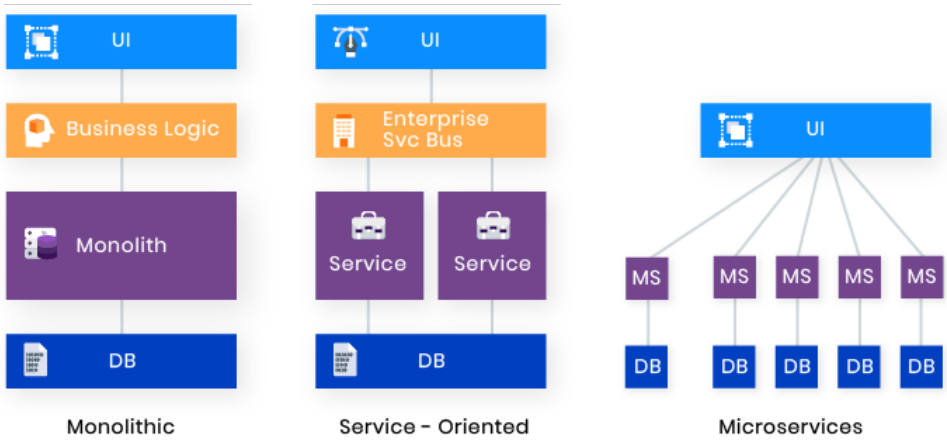


Рис. 1. Подходы к организации информационных систем

Архитектура системы аутентификации и авторизации на основе микросервисов

Микросервисная архитектура наследует от предшественницы изоляцию и распределённость. Здесь база данных не используется как шина данных, за исключением

отдельных случаев в пользу производительности. По классической схеме компоненты изолируются и на уровне кода, и на уровне базы. Кроме того, часто используется событийной (event-driven) архитектура. Её использование приводит к уменьшению связанности микросервисов и хорошо подходит для децентрализованных данных и решения проблем сквозной функциональности.

Для микросервисов применяют контейнеризацию с оркестрацией. В части оркестрации, часто используются уже упомянутый Enterprise Service Bus (ESB) шина, а также Business Process Modelling (BPM) решения. В данной работе рассмотрим решение на основе BPM платформы Camunda [4].

Учитывая, что данные для управления безопасностью и доступами в мультиплатформенных системах могут включать в себя работу с множеством микросервисов и других информационных ресурсов, актуальными являются вопросы управления аутентификацией и авторизацией во всей информационной системе в соответствии с требованиями бизнес-процессов.

Рассмотрим традиционную архитектуру системы аутентификации и авторизации.

1. Клиент системы

Это веб-страница, мобильное приложение, либо другое оконечное приложение, через взаимодействие с которым пользователь выполняет вход в систему и работает с ней.

2. Сервис аутентификации

3. Проверяет введённые пользователем секретные данные, например, логин и пароль, сопоставляет с пользователем в сервисе управления пользователями.

4. Сервис авторизации

Проверяет права доступа идентифицированного пользователя.

5. Сервис управления пользователями.

Хранит данные о пользователях. Эти данные могут хранится в сторонних ресурсах, например, в Active Directory.

6. Сервисы данных

Предоставляет пользователю требуемые данные предварительно проверяя его права на доступ в сервисе авторизации.

Пример взаимодействия этих сервисов показан в диаграмме последовательности на рисунке 2.

Рис. 2. Последовательность аутентификации и авторизации

Рассмотрим описание последовательности шагов на этой диаграмме:

1. Приложение запрашивает у пользователя авторизацию на доступ к серверу ресурсов.
2. Если пользователь авторизует запрос, приложение получает разрешение на авторизацию (authorization grant).
3. Приложение запрашивает авторизационный токен у сервера авторизации (API) путём предоставления информации о самом себе и разрешении на авторизацию от пользователя.
4. Если подлинность приложения подтверждена и разрешение на авторизацию действительно, сервер авторизации (API) создаёт токен доступа для приложения. Процесс авторизации завершён.
5. Приложение запрашивает ресурс у сервера ресурсов (API), предоставляя при этом токен доступа для аутентификации.
6. Если токен действителен, сервер ресурсов (API) предоставляет запрашиваемый ресурс приложению.

Фактический порядок шагов описанного процесса может отличаться в зависимости от используемого типа разрешения на авторизацию, но в целом процесс будет выглядеть описанным образом. Очевидно, что аутентификация и авторизация будет затрагивать несколько информационных ресурсов и потребует взаимодействия нескольких микросервисов.

Для обеспечения гибкости реализации системы следует избегать знания микросервисов друг о друге. Для этого необходимо внедрить механизм оркестрации микросервисами. При этом один конкретный сервис из указанного списка не должен брать на себя роль «командующего» процессом управления аутентификацией и авторизацией.

Для управления данными процессами предлагается использовать BPMS Camunda. Camunda предоставляет Workflow Engine – платформу для управления (микро-) сервисами и управления человеческими задачами. Workflow Engine выполняет бизнес-процессы, описанные в виде диаграммы на языке стандарта BPMN 2.0 [5]. С BPMN

возможно выразить организацию оркестровки, потоки человеческих задач, обработку событий и многое другое на диаграммах, которые являются технически выполнимыми, но все же понятными для всех участников процесса.

Переложим показанную на рисунке 2 диаграмму последовательности на схему BPMN. Основные задачи выполняются автоматизировано в рамках так называемых сервисных задач. Каждая сервисная задача выполняется обработчиком из соответствующего микросервиса. При этом возможно использование сервис аудита, куда событийно записываются действия пользователей и других микросервисов. На рисунке 3 показан пример такой схемы на стандарте BPMN 2.0.

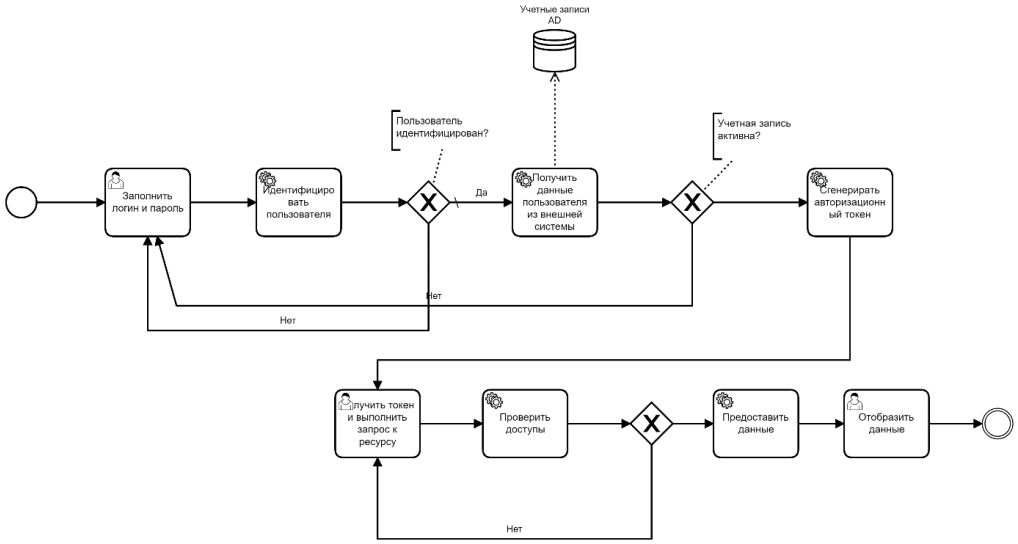


Рис. 3. Пример BPMN диаграммы процесса аутентификации и авторизации

Заключение

В данном докладе предлагается использование механизма оркестрации процессами аутентификации и авторизации на основе Camunda Workflow Engine. Данный подход позволяет увеличить гибкость системы, изолировать используемые микросервисы друг от друга, а управление процессом переложить на движок BPMS. При это структура и взаимодействие компонентов может меняться путем модификации схемы BPMN без значительных изменений самих компонентов системы.

Литература

1. Информационная безопасность: современные реалии, Грошева Е. К., Невмержицкий П. И., 2017.

2. Авторизация // https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F

3. Top 10 BPMS (Business Process Management Systems) In 2019 // https://thedigitalprojectmanager.com/bpms-bpm-software/

4. Camunda Platform // https://camunda.com/

5. BPMN Specification - Business Process Model and Notation // http://www.bpmn.org/

ПРОБЛЕМЫ ПОДГОТОВКИ И ОБУЧЕНИЯ В ВОЕННЫХ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ РЕСПУБЛИКИ ИТ-СПЕЦИАЛИСТОВ ДЛЯ ОРГАНОВ УПРАВЛЕНИЯ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ КАЗАХСТАН, ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ ПРОБЛЕМ

Метелев В.Н., Кожахметов К.Б.
e-mail: svo5858@mail.ru, svo5858@yandex.ru
Национальный университет обороны имени Первого Президента Республики Казахстан – Елбасы, Казахстан

Аннотация. *Рассматриваются проблемы подготовки и обучения ИТ-специалистов (информационного противоборства) в военных ВУЗах республики. Дается краткая характеристика состояния информационной безопасности в оборонном ведомстве, раскрывается система подготовки военных специалистов в области кибербезопасности. Приводится краткий анализ уровня знаний обычных пользователей – магистрантов военного университета на основе собственного проведенного анкетирования. Предлагаются некоторые подходы к решению проблемы повышения уровня базовой подготовки будущих абитуриентов и магистрантов. Приводятся примеры опыта других стран по системе поиска, отбора и подготовки специалистов кибербезопасности. Представляются предложения по методике определения потребностей в военных ИТ-специалистах, перечень возможных вариантов обучения военнослужащих на различных курсах на базе казахстанских и зарубежных учебных заведений и в коммерческих организациях*

Ключевые слова: *информационная безопасность, кибербезопасность, безопасность информационных систем, информационное противоборство, инновационные технологии, научный потенциал, профессионализация специалистов кибербезопасности, профилирующие дисциплины, международный сертификат.*

Специалисты оборонного ведомства совместно с представителями других государственных органов на базе Министерства цифрового развития, оборонной и аэрокосмической промышленности принимают активное участие в разработке нормативной базы по вопросам информационной безопасности.

В Министерстве обороны выстроена система безопасности, позволяющая предотвратить несанкционированный доступ к защищаемым сведениям и ресурсам: таким как сайт Министерства обороны, почтовый сервер, информационные системы, автоматизированные системы управления, сетевое оборудование, автоматизированные рабочие места исполнителей локальной вычислительной сети министерства.

Вместе с тем, как и во всей казахстанской экономике, Вооруженные Силы остро нуждаются в специалистах информационно-математического профиля. В связи с этим, проблемы подготовки военных кадров в сфере информационно-коммуникационных технологий и обеспечения информационной (кибер) безопасности для органов военного управления находится в центре внимания руководства Министерства обороны.

Специалистов указанного профиля для Вооруженных Сил готовит кафедра защиты информации Военно-инженерного института радиоэлектроники и связи (в среднем ежегодная потребность – 25 человек). В системе послевузовского образования

подготовка осуществляется на базе кафедры информационной безопасности Национального университета обороны, а также в, военных ВУЗах Российской Федерации, Турецкой Республики и Республики Беларусь.

Существующая в настоящее время система подготовки специалистов информационной безопасности для ВС РК в какой-то мере удовлетворяет потребности органов военного управления. Но имеется необходимость более квалифицированной подготовки военнослужащих в сфере обеспечения безопасности информационных систем.

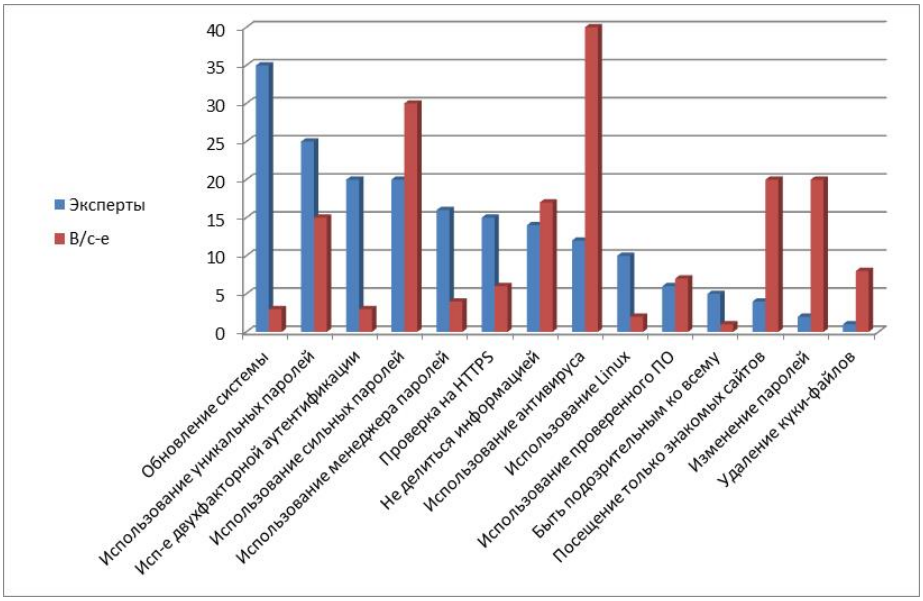


Диаграмма 1 - Результаты опроса экспертов и военнослужащих по кибербезопасности

Проведенное исследование среди личного состава магистрантов (обычные пользователи) и специалистами по безопасности (эксперты), направленное на изучение ответов, данных на вопрос «Пронумеруйте способы защиты вашей информации в киберпространстве по мере убывания безопасности» показывает огромное расхождение между тем, что любители считают правильным делать для своей защиты, и тем, что реально обеспечивает безопасность (уровень знаний в этой области характеризует диаграмма 1).

Каковы возможные причины невысокой подготовленности военнослужащих в сфере кибербезопасности?

Следует отметить низкую базовую подготовку и, в первую очередь, по математике будущих абитуриентов и магистрантов. И, скорее всего, это общая проблема казахстанских высших учебных заведений. Здесь необходимо перестроить работу местных органов военного управления (департаментов, управлений по делам обороны) - молодежь необходимо отбирать через ДДО (УДО) из числа одаренных воспитанников республиканских военных школ-интернатов, Интеллектуальных школ, где учебные программы по предметам естественно-математического цикла имеют высокий уровень сопоставимости с международными признанными программами (A-Level IB SingapureHigher и др.), выпускников по госпрограмме «Болашак» [1].

По опыту других стран, полагаем, что самой оптимальной будет многоступенчатая система поиска, отбора и подготовки специалистов: колледж - институт – магистратура, докторантура (очная и с использованием дистанционных образовательных технологий). Для этого необходимо создать для обучаемых условия для карьерного роста и оплаты труда на уровне, сопоставимом с передовыми (коммерческими) компаниями (по примеру США, Турции и др. стран). Ниже (на диаграмме 2) приведено сравнение оплаты труда специалистов киберподразделений в гражданской и военной сфере.

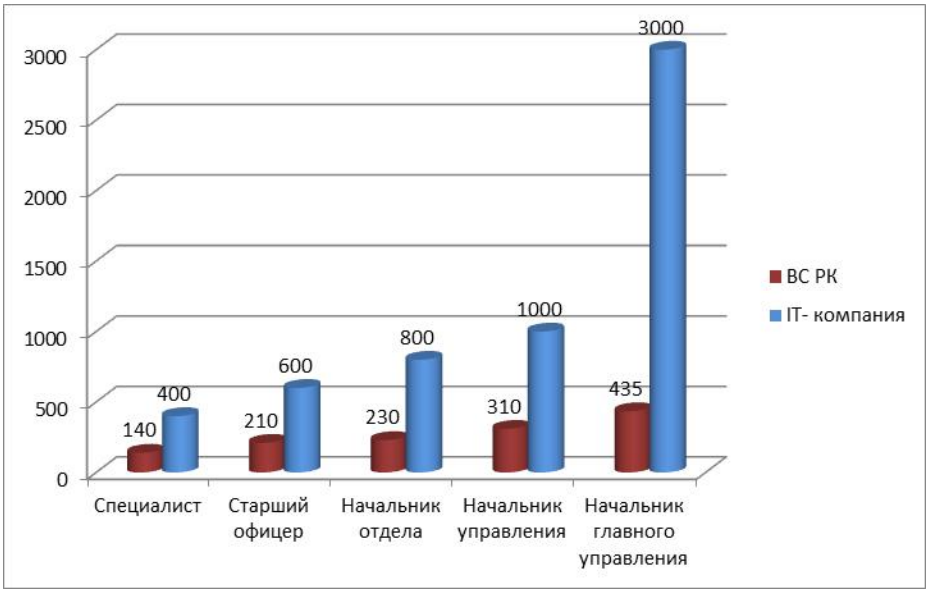


Диаграмма 2 - Сравнение уровня заработной платы специалистов киберподразделений

Кроме того, в образовательные программы военных ВУЗов – Актюбинский Военный институт, Военный институт Сухопутных войск, – в обязательном порядке необходимо включать дисциплину (дисциплины), в учебно-методическом комплексе которой (которых) заложены основы информационной (кибер) безопасности и информационного противоборства.

В целом необходима прозрачность разработанной методики определения ежегодной потребности в ИТ-специалистах (компетенция Департамента кадров Министерства обороны), которая позволяла бы правильно распределять в ВС РК уже подготовленных военнослужащих для воинских частей и учреждений согласно организационно-штатной структуре.

В целях повышения уровня квалификации военнослужащих, отвечающих за эксплуатацию и техническое сопровождение серверного и коммутационного оборудования, необходимо предоставить им возможность обучения на курсах по следующим направлениям:

- администрирование ОС Red Hat Linux, Windows Server 2012;
- системы управления базами данных SQL, Oracle;
- администрирование коммутационного оборудования Cisco, Juniper;
- администрирование ПО «1С».

Данные курсы возможны на базе казахстанских и зарубежных учебных заведений и в коммерческих организациях (к примеру, Военно-космическая академия им. А.Ф.

Можайского, Российская Федерация, Академия КНБ РК). АО «ГИС Центр Казахстан», «Hewlett-Packard», «Cisco» и др. готовы предоставить возможность такого обучения.

Представляется возможным Министерству обороны реализовать и другие подходы к проблеме подготовки (укомплектования) IT-специалистами органов военного управления.

К примеру: готовить специалистов IT-профиля в гражданских (коммерческих) организациях республики; продолжить (возобновить, осуществить) обучение (в дальнейшей перспективе) по программам различных обучающих дисциплин известных компаний мирового уровня, специализирующихся на решении вопросов кибербезопасности, таких как, SAP, Cisco, Juniper, Tpales, Check Point и др. Это может решить проблему подготовки кадров в условиях современного IT–рынка. В Казахстане уже есть успешные проекты, которые стартовали и продолжают свое развитие. Так, 11 ведущих вузов страны, включая Назарбаев Университет и Финансовую академию при Министерстве финансов республики включились в образовательный процесс инновационных технологий [2].

Целесообразность интеграции подготовки специалистов технических специальностей в гражданских вузах и системе военного образования очевидна.

Будущих офицеров инженерного профиля и гражданский инженерный персонал для Вооруженных Сил целесообразно готовить в университетских комплексах, обеспечив преемственность профилированного среднего общего и высшего профессионального технического образования по оборонным специальностям. В состав такого комплекса предлагается включать государственные технические университеты, готовящие инженеров для оборонной промышленности.

Подход к подготовке офицерских кадров из числа студентов гражданских вузов давно существует в мировой практике. К примеру, в общей численности офицерского корпуса в вооруженных силах США выпускники курсов вневойсковой подготовки составляют около 70%. Ежегодно в среднем около 50% выпускников курсов вневойсковой подготовки поступает в регулярные формирования (около 4 тысяч офицеров в год только для сухопутных войск). В вооруженные силы США часто отбираются наиболее подготовленные выпускники ведущих университетов страны – Гарвардского, Колумбийского, Йельского и Калифорнийского, а также ряда специализированных учебных заведений – Крипто-математического института, Института вычислительной техники и информатики, Института международных проблем и т.д.

Подготовка военных специалистов в гражданских вузах имеет ряд преимуществ: экономическая целесообразность; более высокий научно-педагогический потенциал гражданской высшей школы и уровень профессиональной подготовки гражданских вузов, возможность подготовки военных специалистов по уникальным военно-учетным специальностям, подготовка по которым в военных вузах нецелесообразна[3].

Необходимо осуществлять более тесный обмен опытом, подготовку специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов в области информационной безопасности в рамках региональных (межправительственных) актов о сотрудничестве, к примеру, и таких как:

- Шанхайская организации сотрудничества;
- Организация договора о коллективной безопасности;
- Организация по безопасности и сотрудничеству в Европе.

На указанные форумы, семинары, тренинги, учения как отечественных, так и зарубежных организаций привлекать магистрантов 1 и 2 курсов кафедры (если они проводятся в г. Нур-Султан).

Полагаем возможным и в дальнейшем изучать, анализировать и внедрять положительный опыт других стран в этой сфере деятельности. К примеру, специфика IT-сферы такова, что программисты могут работать удаленно. Аутсорсинг IT - отрасли широко применяется в США, которые используют индийских программистов. Так, в США широко задействуется «Red Team» - возможно использовать специалистов «Red Team» в учениях по тематике кибербезопасности и/или информационного противоборства.

Профессорско-преподавательский состав названных выше кафедр Национального университета обороны и ВИИРЭС считает, что требуется повысить научный потенциал этих подразделений. Для этого необходимо оптимизировать организационно-штатную структуру кафедр, изменить функции и задачи имеющихся там лабораторий, в учебном процессе факультета шире использовать компьютерное моделирование и тренажерные комплексы.

Обществу нужны специалисты в различных предметных областях, владеющие информационными технологиями в рамках своей профессии. И, как отмечают российские специалисты, процесс совершенствования профессиональной подготовки будущего И-Т специалиста станет более эффективным, если в образовательном процессе вуза будет (будут):

применяться методика формирования навыков имитационного моделирования;

использоваться профессиональные программы (AnyLogic Arena) [4].

Требуется внести изменения в учебные планы и ввести ряд новых дисциплин, которые станут профилирующими. К примеру, на кафедре защиты информации ВИИРЭС (специальность «Кибербезопасность в военном деле») - построение защищенной инфраструктуры; форензика; реверс-инжиниринг (анализ вредоносных программ); Shell-скриптинг (bin/bash); администрирование серверных операционных систем; администрирование серверных ОС (на рисунке 1 показан предлагаемый перечень профилирующих дисциплина на кафедре информационной безопасности университета).

Рисунок 1 - Предлагаемый перечень профилирующих дисциплина на кафедре информационной безопасности

В целях повышения профессионализации специалистов кибербезопасности в Вооруженных Силах необходимо разработать профессиональные стандарты, совершенствовать требования по практическим навыкам и техническим знаниям, тем самым улучшать профили защиты и параметры контроля защищенности информационных ресурсов и систем. Одно из требований к IT-специалистам - наличие международного сертификата в области информационной безопасности (CISSP, аббревиатура появилась в начале 90-х годов). В настоящее время данным статусом уже обладают почти 90 000 человек в 146 странах мира. За основу практик управления информационной безопасностью взяты стандарты серии ISO 27000, 27001, 27002, а также публикации американского института стандартов (NIST).

Статус CISSP официально признан мировым киберсообществом и ведущими государствами. Специалист по информационной безопасности, назначенный на руководящую должность в этой области деятельности, считаем, обязан обладать сертификатом CISSP. Получить статус CISSP может специалист, сдавший сертификационный экзамен и имеющий необходимый практический опыт в области информационных технологий и информационной безопасности (см. рисунок 2) .

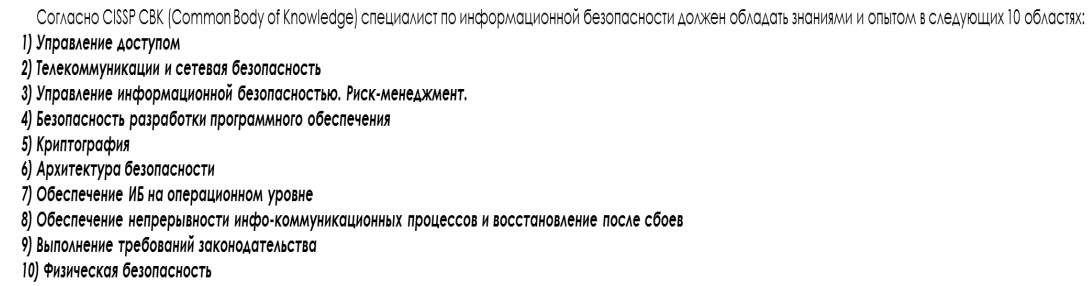


Рисунок 2 - CISSP (Certified Information Systems Security Professional - «Сертифицированный специалист по информационной безопасности»)

С учетом современных форм вооруженной борьбы, ведения информационного противоборства через киберпространство, полагается необходимым изменить систему подготовки специалистов информационной (кибер) безопасности (примерная структура этих изменений показана на рисунке 3).

Рисунок 3 – Перспективная схема подготовки специалистов киберподразделений

Как отмечают казахстанские эксперты, на сегодняшний день порядка 90% развитых стран абсолютно открыты для притока высококвалифицированной рабочей силы с уникальными знаниями и навыками.

Передовые страны уже давно сделали акцент на росте и развитии человеческого капитала ка основы устойчивого развития государства, общества и экономики. Доказан тот факт, что рост человеческого капитала ведет к общему росту экономики страны, а также увеличение человеческого капитала на 1% приводит к ускорению темпов роста ВВП на душу населения на 1-3%.

Развитые страны в ходе глобальных процессов сделали переоценку своих национальных ценностей и приоритетов. Сегодня национальное богатство развитых стран только на 20% составляют природные ресурсы, на 16% - физический капитал и остальные 64% занимают знания, умения и распоряжения ими [5].

Таким образом, если мы не сможем привлечь нашу талантливую молодежь в ИТ-сферу, то вероятность того, что она сможет реализовать свои возможности заграницей, весьма велика.

Литература

1. Шамшидинова К. Инициатива в образовательном пространстве Казахстана // Союз Евразия.– 2017. - № 25. С.27-31.

2. SAP. Цифровизация на рынке труда: будущее за IT. // Союз Евразия.– 2017. - № 25. С.78,79

3. Баймуханов К.А., Когабаев М.А. Основные принципы формирования системы подготовки военных кадров в Республике Казахстан. // Научный сборник АО «Центр военно-стратегических исследований», г. Астана, АО «ЦВСИ», 2011. - С.292-297.

4. Гусева Е.Н., Ефимова И.Ю., Варфоломеева Т.Н. Методика формирования навыков имитационного моделирования у ИТ-специалистов. // Открытое образование.– 2019. - № 1. С.4-13.

5. Мадиев С.Н. Человеческий капитал – основа устойчивого экономического роста страны// Союз Евразия.– 2017. - № 25. С.62-65.

ЕДИНЫЙ ИНТРАНЕТ ПОРТАЛ ДЛЯ ОПРЕДЕЛЕНИЯ РЕЙТИНГА ПРЕТЕНДЕНТОВ НА ГОСУДАРСТВЕННУЮ СЛУЖБУ РК

Мухаев Д.К.
e-mail: daryn.mukhayev@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В работе проанализированы недостатки существующей системы отбора претендентов на государственную службу РК, выявлены недостатки системы, указаны пути их устранения. В целях оптимизации систем отбора претендентов предложено использовать преимущества технологий дистанционного обучения.*

Информационная безопасность понимается как защищенность информации на любых носителях от случайных и преднамеренных несанкционированных воздействий естественного и искусственного свойства, направленных на уничтожение, разрушение, видоизменение тех или иных данных, изменение степени доступности ценных сведений. Помимо профессиональных способностей сотрудники, рано или поздно сталкивающиеся с закрытой информацией, должны обладать высокими моральными качествами, порядочностью, исполнительностью и ответственностью. Они добровольно соглашаются на определенные ограничения в использовании информационных ресурсов и вырабатывают в себе самодисциплину, самоконтроль действий, поступков и высказываний.

Человеческий фактор должен постоянно учитываться в долговременной стратегии фирмы и ее текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов. То есть в основе любой системы защиты информации лежит человеческий фактор, предполагающий осознанное соблюдение им установленных правил защиты информации. Человеческий фактор должен постоянно учитываться в долговременной стратегии и ее текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов.

Для подготовки специалистов в Казахстане накоплен значительный опыт в сопровождении тестирования и обучения для государственного и частного сектора. Имеется техническая база для проведения тестирования любой сложности и обучения в залах тестирования во всех областных центрах страны. Залы тестирования оснащены необходимой оргтехникой. Эти преимущества используются для предоставления услуг сопровождения тестирования и обучения с использованием цифровых технологий.

При центрах подготовки в регионах осуществляется пробное тестирование на государственном и русском языке для кандидатов на административную и правоохранительную службы. Это позволяет кандидатам объективно оценить свои знания, преодолеть психологический барьер и, в целом, повысить правовую грамотность.

Система государственной службы постоянно совершенствуется в соответствии с требованиями времени и благодаря реформе Плана Нации, озвученной в ….

В 2016 году вступил в силу новый Закон «О государственной службе Республики Казахстан» [1]. Он направлен на обеспечение открытого конкурсного отбора,

продвижения по службе на основе уровня компетентности и уровня вознаграждения в зависимости от результатов проводимого конкурса. Прием на государственную службу начнется с низовых должностей. Такой подход позволяет избежать условий протекционизма, покровительства и случайности в системе государственной службы. Прием на государственную службу впервые будет проходить на низовых позициях на основе трехэтапного конкурсного отбора [2].

Конкурс состоит из нескольких этапов. Первый этап является самым сложным этапом. На этом этапе кандидат проверяется на знание законодательства и компетенции. В настоящее время существует 15 законов, которые каждый кандидат должен знать, чтобы поступить на государственную службу. Предотвращая явление коррупции на государственной службе, правительство требует от кандидатов хорошего знания закона. Наш портал поможет всем кандидатам изучить законы и успешно завершить тестовую часть.

Впервые об открытых онлайн-курсах отбора стало известно более десять лет назад, когда специалистами Университета Манитобы (Канада) удалось запустить курс «Коннективизм и соединительные знания», который собрал более двух тысяч подписчиков. С ростом числа и популярности первых онлайн-курсов стало ясно, что это не новая модная тенденция, а современный ответ на вызовы времени, который позволяет устранить многие недостатки и упущения, присущие традиционным подходам образовательной системы. Нерелевантный материал и устаревшие методы работы с информацией – основная причина отставания от требований времени во всех учебных организациях. Масштабные задачи пытались решить не на высшем уровне правительством, а на низовом уровне, что привело к использованию методам ознакомления и распространения знаний в современном мире через Интернет [3].

Архитектура является первым подходом процесса разработки в создании прочной основы развития. Подход позволил оценить все риски, компоненты, требования и варианты использования проекта. Кроме того, был проведен весь необходимый анализ возможных решений и алгоритмов.

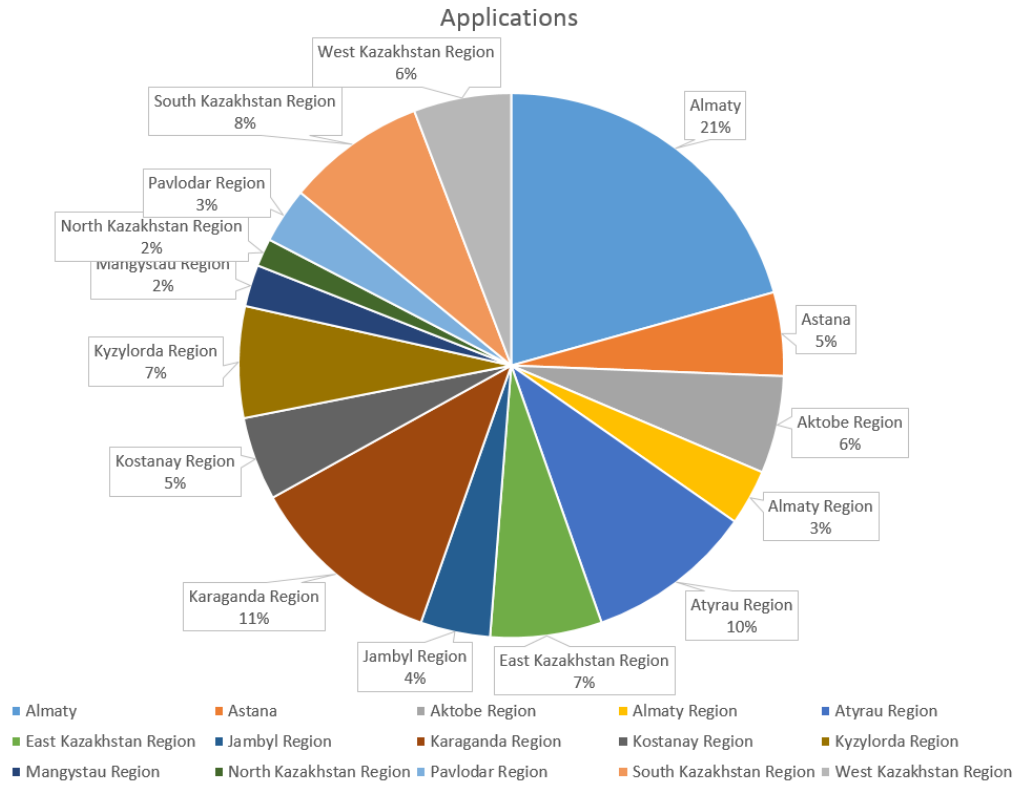


Рисунок 1. Диаграмма анализа опроса по регионам Казахстана

Перед запуском этого проекта нами был проанализирован спрос и предложения услуг путем изучения географии запросов (заявок) граждан всех регионов Казахстана на участие в конкурсе, который показал, что до 26% клиентов были из Алматы и Астаны, что означает, что большинство граждан, подавших заявки на конкурс, не имеют возможности посещать офлайн-курсы.

Это явилось основной причиной создания онлайн-портала для подготовки кандидатов, который позволит часть проблем подготовки граждан на себя.

Цель данной работы состояла в разработке единого интранет-портала для поддержки претендентов на государственную службу РК. Эта технология устраняет необходимость ежедневных посещений автономных курсов, что позволит сократить финансовые затраты и сэкономить время. В ходе анализа существующих систем была выявлена необходимость разработки портала не только с тестами, но и с подготовительными курсами для государственных служб, что позволяет кандидатам повышать уровень и закреплять знания законодательства Республики Казахстан.

В работе были проанализированы все возможные причины неудач кандидатов во время тестирования. По результатам анализа в этом проекте была принята и сформулирована исследовательская задача.

Далее дано описание практической части. Подробно представлена клиентская часть и серверная часть приложения. Было внедрено несколько технологий, позволяющих общаться с преподавателями курсов с помощью текстовых сообщений и видеосвязи. Кроме того, система тестирования, разработанная в рамках проекта, по структуре идентична системе государственного применения.

В последней главе проект дана экономическая эффективность проекта, которая показало положительный результат. Предлагаемая концепция Интранет-портала для определения рейтинга претендентов на государственную службу РК эффективна в силу востребованности гражданами Казахстана [4].

Заключение

В работе изложены основные принципы, лежащие в основе информационной системы подготовки лиц, допущенных к отбору на государственную службу РК. Сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания кадров. Повышение ответственности кадров за выполняемую работу, сохранность ценных сведений, активное участие в принятии управленческих решений требует нового содержания при оценке таких критериев, как образование, профессионализм, личная культура, моральные качества и этика работников. Люди рассматриваются как самый ценный ресурс фирмы и решают, с одной стороны, производственные и коммерческие задачи, а с другой - получают во владение ценные и конфиденциальные сведения и обеспечивают их правильное использование и сохранность.

В докладе проанализированы недостатки существующей системы и внедрены все новейшие технологии дистанционного обучения. Кроме того, были выявлены возможные причины сбоев государственных испытаний и указаны пути их устранения.

Портал создан на одном из популярных фреймворков, причины выбора которого были обоснованы в проекте. В дальнейшем любой пользователь сможет работать с этим порталом, благодаря тому, что для создания портала был использован MVC.

Использование портала позволит каждому кандидату подготовиться к поступлению на государственную службу, находясь вне центров тестирования претендентов, тем самым значительно повысить эффективность процедур отбора претендентов.

Литература

1. "Что нужно знать о новом законе," KyzmetToday.kz, [Online].Available: http://www.kyzmettoday.kz/dissovet/item/647-chto-nuzhno-znat-o-novom-zakone-o-gosudarstvennoj-sluzhbe-respubliki-kazakhstan. [Accessed 06 January 2016].

2. "Политическая элита Казахстана: Отбор в корпус "А" провалили большинство кандидатов," 5 October 2017. [Online]. Available: https://tengrinews.kz/kazakhstan_news/politicheskaya-elita-kazahstana-otbor-korpus-a-provalili-328010/ [Accessed 5 October 2017].

3. S. Norman, "5 Advantages Of Online Learning: Education Without Leaving Home," [Online]. Available: https://elearningindustry.com/5-advantages-of-online-learning-education-without-leaving-home. [Accessed 10 March 2016].

4. C. Thompson, "How Khan Academy Is Changing the Rules of Education," [Online]. Available: https://www.wired.com/2011/07/ff_khan/. [Accessed 07 November 2015].

АНАЛИЗ BIG DATA ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ ПО ДАННЫМ NETFLOW

Оразмуханбет А.Б.
email: alpamys_.kz@mail.ru
Институт Кибернетики и Информационных Технологий,
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Казахстан

***Аннотация**. В прошлом кибератаки организовывались простым и случайным образом. Однако нападения в настоящее время осуществляются систематически и длительно. Кроме того, большой объем вычислений и непрерывные изменения в распределении сетевых данных затрудняют анализ данных и обнаружение аномального поведения внутри сети. По этой причине решения для работы с большими данными стали незаменимыми. В этой статье впервые были рассмотрены исследования обнаружения сетевых аномалий и атак на больших данных. Затем был проведен анализ общедоступных данных большой сети с использованием нового подхода к обнаружению аномалий без контроля. Наконец, были оценены результаты, полученные из тематического исследования, была достигнута точность 96%. Результаты были визуализированы после уменьшения размера с помощью анализа главных компонентов. Выявленные аномалии могут обеспечить полезные выходные данные для понимания поведения сети, различения атак, обеспечения лучшей кибербезопасности и защиты критических инфраструктур.*

Введение

Кибербезопасность приобретает все большее значение, поэтому множество стран начали делать большие инвестиции для защиты своих важнейших инфраструктур. В 2016 финансовом году бюджетный запрос для Департамента государственной безопасности США Network Security Distribution Department составил $ 479,8 млн [1]. По данным Norton, жертвы киберпреступности потратили $ 126 млрд по всему миру с 2015 года [2]. Причина этих огромных инвестиций в кибербезопасность заключается в том, что киберпреступности становятся все более интеллектуальными, сложными и разрушительными.

Обычные системы защиты неэффективны, потому что они в основном не могут обнаружить эти атаки из-за их сигнатурной структуры, и трудно одновременно выполнять как операции, так и анализ огромного количества данных безопасности. Таким образом, системы управления информацией и событиями безопасности (SIEM) в настоящее время заменяются системами анализа безопасности Big Data[3]. Аналитика безопасности Big Data приобретает все большее значение, так как записи не нужно удалять через определенный промежуток времени, на сложные запросы можно ответить за короткое время, неструктурные данные можно легко анализировать, а кластерные вычислительные инфраструктуры обладают повышенной надежностью [3].

Одним из интеллектуальных решений, используемых компаниями для защиты своих сетей от возникающих угроз, является сбор потоков IP-трафика и развертывание систем обнаружения аномалий на основе мониторинга сетевого трафика [4]. В направлении исследований сетевого анализа и обнаружения вторжений на больших

данных был предложен новый подход к обнаружению неконтролируемых аномалий. Он направлен на определение аномалий, вызванных атакой UDP flood от конкретных IP-адресов.

1. Обнаружение аномалий и анализ Big Data

Обнаружение аномалий (или обнаружение выбросов) - это идентификация редких предметов, событий или наблюдений, которые вызывают подозрения, значительно отличаясь от большинства данных. Под обнаружением аномалий трафика понимаются отклонения в использовании сетевых ресурсов, доступ к которым предоставляется посредством сетевого трафика для работы веб-сервисов и сетевых приложений.

Обнаружение аномалий на сегодняшний день является одним из активно развивающихся направлений в области обеспечения кибербезопасности. Это связано с тем, что аномалии в большинстве случаев являются начальной стадией сетевых атак, которые могут повлечь как негативные нематериальные последствия, так и финансовые убытки для организаций, имеющих существенное представительство в интернет пространстве.

Как правило, такие аномалии являются результатом разведки для дальнейшего использования обнаруженных проблем в системе безопасности с целью получения коммерческой выгоды. Выявление и классификация аномалий предполагает непрерывный процесс мониторинга событий в компьютерных системах и сетях, в связи с чем требуется обработка больших объёмов данных, генерируемых этими источниками.

Big Data – это массивный сбор данных, который включает в себя различные и разнообразные типы наборов данных [5]. Характеристики больших данных определяются 6V [6, 7].

- Velocity – Скорость передачи данных;
- Volume – Объем данных;
- Variety – Разнообразие данных;
- Veracity – Достоверность данных;
- Vocabulary – Данные о данных;
- Value – Полезность данных.

Скорость относится к скорости обработки и создания данных. Объем - это объем данных. Разнообразие указывает на типы данных. Достоверность указывает на достоверность данных. Словарь включает в себя схемы, модели и онтологии, которые описывают структуру данных. Значение относится к пониманию и стоимости.

Поскольку традиционные методы не могут справиться с характеристиками больших данных, анализ больших данных приобретает все большее значение. Анализ больших данных – это набор хорошо зарекомендовавших себя инструментов и методов для поиска полезной скрытой информации внутри необработанных данных [8]. Следовательно, модели Big Data являются более быстрыми, масштабируемыми и отказоустойчивыми, чем традиционные подходы.

Угроза или попытка вторжения относится к созданию аномалии как несанкционированная попытка получить доступ к системе, изменить информацию или сделать систему непригодной для использования [9]. Методы обнаружения аномалий используются во многих приложениях, таких как обнаружение вторжений, обнаружение мошенничества и предотвращение утечки данных [10]. Сетевое обнаружение вторжений предназначено для обнаружения необычных моделей поведения пользователей сети, а

высокая скорость работы интерфейсов требует анализа Big Data для этого процесса как естественного результата разработки.

При изучении темы с точки зрения обнаружения аномалий больших сетей (таблица 1) представляется, что анализ сетей с Big Data-ой в основном осуществляется традиционными методами на относительно больших объемах данных для выявления атак с помощью контролируемых методов. Кроме того, начали внедряться решения для работы с большими данными для снижения ложноположительной и ложноотрицательной скорости, а также для обработки огромных и потоковых данных.

Таблица 1 – Сравнение для литературы

Назначение	Аномалии	Данные	Методы и технологии	Результаты
Модель, основанная на Big Data, которая может избежать влияния, от ложноотрицательной скорости и повысить точность обнаружения регулировкой распределения сетевого трафика	Dos, U2R, R2L, Probe	KDD CUP99	k-means, KNN, decision tree, random forest	Detection rates: 95.4% on normal data, 98.6% on DoS attack, 93.9% onProbe attack, 56.1% on U2R attack, and 77.2% on R2L attack
Реализация метода обнаружения DDoS в кластере Apache Spark	DDoS	2000 DARPA LLDOS 1.0 and generated normal traffic data	ANN, Spark	Accuracy: 94%
Модель обнаружения аномалий, которая объединяет облачные вычисления с машинным обучением на основе Hadoop	Bad connections	KDD CUP 9	HDFS, MapReduce, Weka, naïve bayes , detection tree	Выше 90% точности
Гибридная система обнаружения вторжений в реальном времени с использованием apache storm	DDos	ISCX 2012	Storm, CC4 нейронные сети Многослойный персептрон	Средняя точность: 89 %

			нейронные сети	
Обнаружение вторжений на основе аномалий на разных уровнях TCP/IP (сети / приложения)	Несанкционированный доступ в интернет, систематическая загрузка и DDoS-атаки	Журналы прокси-сервера локальной сети кампуса и трассировки пограничного маршрутизатора	Машинное обучение, анализ временных рядов, анализ паттернов	-
Обнаружение P2P ботнетов с использованием случайных лесов в квазиреальном времени	Бот-атак (conficker, kelihoshlux, zeus, storm)	Сетевой трафик CAIDA и кампуса	Hive, Tshark, Mahout, Random Forest	Точность: 99,7%

2. Предлагаемый подход

NetFlow-это сетевой протокол, который собирает информацию о трафике, такую как сетевые пользователи, сетевые приложения и трафик маршрутизации [26]. Эти данные широко используются для исследований обнаружения сетевых аномалий, поскольку вредоносная информация о трафике может быть идентифицирована с помощью анализа NetFlow.Обнаружение сетевых аномалий может быть выполнено с помощью дистанционных, плотностных и машинных методов обучения или программных вычислений [27]. Предлагаемый в данном исследовании метод является кластеризованным с точки зрения машинного обучения. Кластеризация является широко используемым методом обнаружения аномалий, так как она не требует маркированных наборов данных и предопределенных классов [27].

Этапы предлагаемого подхода поясняются ниже:

a) Чистые потоки делятся на интервалы.

- Большинство действий показывают подобное поведение в течение нескольких минут (поведение временной локализации [28]);

b) Чистые потоки агрегируются в соответствии с IP-адресами источников.

- Размер данных уменьшается для обработки;
- Агрегированные данные могут показать новые модели для обнаружения поведения.

c) Полученные данные стандартизированы по нулевой шкале, как в (1),

$$z = \frac{x - \mu}{\sigma}, \tag{1}$$

где μ-среднее, а σ-стандартное отклонение.

- Эта процедура выравнивает изменчивость данных;
- Стандартизированные данные в меньшей степени подвержены влиянию выбросов.

d) Агрегированные чистые потоки кластеризуются на основе алгоритма k-средних как распределенные.

- Неконтролируемые методы, обученные с немаркированными данными, обладают способностью обнаруживать незнакомые атаки [29];
- Предполагается, что кластеры будут возникать в соответствии с нормальным или ненормальным поведением трафика.

e) Вычисляется Евклидово расстояние элементов кластера до центра кластера.

- Элементы в кластере должны быть близки к центру для хорошей кластеризации;
- Элементы могут быть аномально удалены от центра по любой причине, и центроиды могут быть использованы для обнаружения выбросов;
- Гистограмма используется для понимания распределения расстояния элементов от центра;
- Элементы, удаленные от сосредоточенной области на гистограмме, считаются аномальными.

f) Фактические нормальные и ненормальные числа потоков определяются по временным интервалам на этапах 4 и 5. Наконец, оценивается критерий успеха.

3. Исследование

Предлагаемый подход был реализован на общедоступном кластере NetFlow data on Apache Spark в Azure HDInsight с использованием языка программирования python. Применяя этот подход к тематическому исследованию, был получен коэффициент точности 0,96. Кроме того, полученные результаты были визуализированы в 3D путем уменьшения размеров.

Набор данных CTU-13 использовался для анализа трафика ботнета. Эти данные были получены университетом CTU в Чешской Республике в 2011 году [30]. Набор данных состоит из 13 сценариев, имеющих различные образцы атак. В этом исследовании 10-й сценарий был выбран из-за размера набора данных и количества атак ботнета. Набор данных имеет 4,75 часа записей и 1309791 потоков, охватывающих 106352 UDP DDoS потоков.

```
StartTime,Dur,Proto,SrcAddr,Sport,Dir,DstAddr,Dport,State,sTos,dTos,TotPkts,TotBytes,SrcBytes,Label
2011/08/18 09:56:29.146150,2752.656250,udp,71.222.124.71,60621,  <->,147.32.84.59,63550,CON,0,0,3,435,290,flow=Background-Established-cmpgw-CVUT
2011/08/18 09:56:42.630892,1849.315552,udp,78.234.54.245,51413,  <->,147.32.84.59,63550,CON,0,0,3,417,272,flow=Background-Established-cmpgw-CVUT
2011/08/18 09:56:44.640650,2001.747314,udp,31.147.120.139,63195,  <->,147.32.84.59,63550,CON,0,0,2,290,145,flow=Background-Established-cmpgw-CVUT
2011/08/18 10:10:52.782230,1535.769409,udp,118.5.35.64,39110,  <->,147.32.84.59,63550,CON,0,0,2,290,145,flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:13.328372,0.002636,tcp,147.32.86.166,33426,  <?>,212.24.150.110,25443,FRPA_FPA,0,0,6,490,321,flow=Background
2011/08/18 10:19:13.328670,72.436790,udp,82.39.2.249,41915,  <->,147.32.84.59,43087,CON,0,0,23849,24298138,509912,flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:13.330765,3599.473633,tcp,147.32.86.166,42020,  <?>,147.32.192.34,993,PA_PA,0,0,543,98018,33640,flow=Background
2011/08/18 10:19:13.333772,28.152548,tcp,115.184.37.24,49190,  <?>,147.32.84.2,80,A_FPA,0,0,222,191281,6610,flow=Background
2011/08/18 10:19:13.335316,632.001648,tcp,80.78.79.156,51287,  <?>,147.32.86.24,31002,FPA_FPA,0,0,15347,2542390,1237911,flow=Background
2011/08/18 10:19:13.335512,628.915222,udp,147.32.86.24,31002,  <->,151.41.188.39,49621,CON,0,0,9464,2024974,2022958,flow=Background-UDP-Established
2011/08/18 10:19:13.336134,0.000177,udp,82.73.244.56,39051,  ->,147.32.84.118,1153,INT,0,,1,145,145,flow=Background-UDP-Attempt
2011/08/18 10:19:13.336311,0.000000,icmp,147.32.84.118,0x0303,  ->,82.73.244.56,0x8104,URP,0,,1,173,173,flow=Background
2011/08/18 10:19:13.337361,1315.114136,tcp,188.95.61.42,53389,  <?>,147.32.86.110,48190,RPA_FPA,0,0,59405,24973123,21487780,flow=Background
2011/08/18 10:19:13.341725,450.406830,tcp,192.221.106.126,80,  <?>,147.32.84.59,2774,FPA_FA,0,0,85347,97405130,96357830,flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:13.344200,123.438812,tcp,212.111.2.151,8000,  <?>,147.32.86.135,3978,PA_FRA,0,0,4238,4189542,4104702,flow=Background
```

Рис. 1 – сценарий набора данных CTU-13

Этапы внедрения и результаты были объяснены ниже:

a) NetFlows в необработанных данных (рисунок 1) были разделены на интервалы в 1 минуту;

- 1 минуты было достаточно для захвата аномалий и интервалов не содержащих слишком много потоков.

b) Чистые потоки были агрегированы в соответствии с исходным IP-адресом.

- Агрегирование проводилось по количеству уникальных портов источника, количеству уникальных IP-адресов назначения, количеству уникальных портов назначения, количеству сетевых потоков, количеству байт и количеству пакетов;
- Число потоков было уменьшено до 1309791 с 294374.

c) Полученные данные были стандартизированы по нулевой шкале в соответствии с их средними и стандартными значениями отклонения

d) Агрегированные чистые потоки были сгруппированы.

- Алгоритм был выполнен с использованием 2 кластеров и не более 1000 итераций.
- После процесса кластеризации в первом кластере было 294351 член, а во втором-23 члена.
- Многие потоки из многих портов в несколько пунктов назначения можно рассматриваются как поведение ботнета. Во втором кластере средние уникальные IP-адреса назначения и средние уникальные порты назначения были найдены очень маленькими, хотя средние порты источника Unique и количество сетевых потоков были очень большими. По этой причине второй кластер был помечен как аномалия были очень большими. По этой причине второй кластер был помечен как аномалия

e) Хотя различие было сделано путем кластеризации, аномалии также могут быть найдены в нормально классифицированном кластере.

- Рассчитано расстояние от первых элементов кластера до первого центра кластера и 5-ковшовая гистограмма кластера.
- Удаленные от центра скопления элементы рассматривались как аномалии.

f) Хотя различие было сделано путем кластеризации, аномалии также могут быть найдены в нормально классифицированном кластере.

- Для того, чтобы найти показатель успеха, IP-адреса, которые атаковали ботнет в сценарии и "ботнет" в метке потока, были оценены как аномалии.
- Было установлено, что кластер, идентифицированный как аномалия на этапе 4, на самом деле является аномальным. Однако ни один из элементов кластера, идентифицированных как аномалия на этапе 5, не был аномальным. Это отклонение может быть выбросом по любой причине.
- Количество вычислений агрегированных потоков в исходных данных. Это соответственно 76954 и 15458 в шаге 4 и 5.
- В результате анализа была получена матрица аномалий (таблица 2).

Таблица 2 – Матрица аномалий

	Actually Botnet	Actually Not Botnet
Detected Botnet	TP-76954	FP-15458
Detected Not Botnet	FN-29398	TN-1187981

- Согласно матрице аномалий, точность (2) метода обнаружения неконтролируемых аномалий составляет 0,96.

$$\text{Точность} = \frac{TP + TN}{TP + TN + FP + FN} \qquad (2)$$

• Помимо точности, чтобы легко сделать исследование и визуализировать 6-мерные данные были сведены к 3-мерным с помощью PCA. Красные треугольники представляют трафик ботнета, а синие круги-обычный трафик в сети. Предложенный метод позволил успешно выявлять аномалии, отличающиеся от нормальных. Однако не удается обнаружить аномалии, которые были похожи на нормальный трафик. Каким-то образом группа данных, которая имела отличающийся от нормального паттерна, была обнаружена неправильно как ненормальная на рисунке 2.

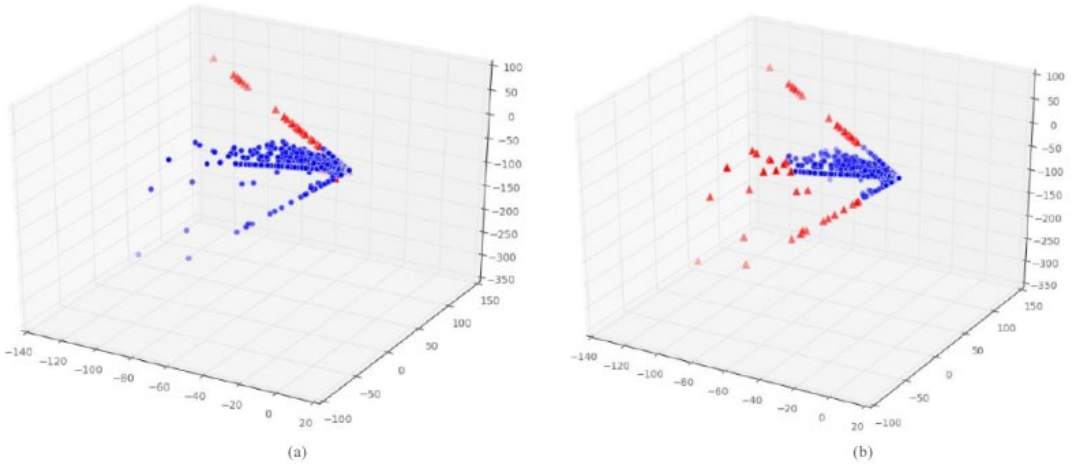


Рис. 2 – (а) аномалии в данных, (б) аномалии обнаружены предложенным методом

Заключение

В этой работе были проанализированы публичные данные с помощью нового бесконтрольного подхода обнаружения аномалий в кластере Apache Spark в Azure HDInsight с точностью 96%. Полученные результаты были визуализированы в виде 3D путем уменьшения размеров с помощью PCA. Таким образом, подозрительные или вредоносные потоки трафика, выбросы, скомпрометированные устройства и нарушения политики были легко обнаружены. Результаты и литература ясно указывают на то, что своевременное и эффективное обнаружение аномалий необходимо для повышения безопасности сети. Выявленные аномалии могут обеспечить лучшее восприятие для различения, анализа и понимания. Высокая точность обнаружения аномалий обеспечивает высокое качество услуг и связи даже при увеличении сложности атак и процесса анализа. В сетевом трафике большинство потоков являются нормальными. Аномалии, такие как атаки и выбросы, естественно, редки. Это ситуация, которая негативно влияет на обнаружение аномалий и показатели успеха. По этой причине в будущих исследованиях, содержащих больше данных и аномалий, инновационных алгоритмов и платформ, могут быть достигнуты более высокие результаты. Считается, что эти вопросы будут рассмотрены в будущих исследованиях.

Список литературы

1. Budget-in-Brief Fiscal Year 2016, US Department of Homeland Security, Editor. 2016.
2. 2016 Norton Cyber Security Insights Report. 2016.

3. Big Data Working Group, Big Data Analytics for Security Intelligence.2013, Cloud Security Alliance.
4. Cisco Public, Network as a Security Sensor Threat Defense with Full NetFlow. 2016. 1-19.
5. Elarabi, T., et al. Big data analytics concepts and management techniques. in 2016 International Conference on Inventive Computation Technologies (ICICT). 2016.
6. Lakshen, G.A., S. Vraneš, and V. Janev. Big data and quality: A literature review. in 2016 24th Telecommunications Forum (TELFOR).2016.
7. Tsai, C.-W., et al., Big data analytics: a survey. Journal of Big Data, 2015. 2(1): p. 21.
8. Sanjay, M. and B.H. Alamma. An insight into big data analytics; Methods and application, 2016 International Conference on Inventive Computation Technologies (ICICT). 2016.
9. Bhuyan, M.H., D.K. Bhattacharyya, and J.K. Kalita, Network Anomaly Detection: Methods, Systems and Tools. IEEE Communications Surveys & Tutorials, 2014. 16(1): p. 303-336.
10. Goldstein, M. and S. Uchida, A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data.PLOS ONE, 2016. 11(4): p. e0152173
11. He, W., G. Hu, and Y. Zhou, Large-scale IP network behavior anomaly detection and identification using substructure-based approach and multivariate time series mining. Telecommunication Systems, 2012. 50(1): p. 1-13.
12. Liu, D., et al. Network Traffic Anomaly Detection Using Adaptive Density-Based Fuzzy Clustering. in 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. 2014.
13. Xie, Y., et al., Resisting Web Proxy-Based HTTP Attacks by Temporal and Spatial Locality Behavior. IEEE Transactions on Parallel and Distributed Systems, 2013. 24(7): p. 1401-1410.
14. Gogoi, P., B. Borah, and D.K. Bhattacharyya, Anomaly detection analysis of intrusion data using supervised & unsupervised approach.Journal of Convergence Information Technology, 2010. 5(1): p. 95-110.
15. García, S., et al., An empirical comparison of botnet detection methods.Computers & Security, 2014. 45: p. 100-121

МОДЕЛИ НАРУШИТЕЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Отар Е.Х., Турдиева Г.Т.
e-mail: Otarov_erlan@mail.ru
Академия КНБ Республики Казахстан

Аннотация: *Повсеместное использование, хранение, обработка и передача информации приводят к повышению актуальности вопросов, связанных с защитой информации. Одной из видов защиты информации является криптографическая защита. В данной статье рассматривается один из возможных способов определения*

моделей нарушителя. Применение представленного метода позволит учитывать мотивацию, знания, финансовые и технические возможности потенциальных противников и современные достижения информационных технологий.

Для защиты информации от несанкционированного доступа при ее хранении, обработке и передаче используются средства криптографической защиты информации (далее – СКЗИ). Основным документом для оценки качества СКЗИ отечественного и зарубежного производства, используемых в РК, является Стандарт Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» (далее – Стандарт), который был принят в 2007 году. Анализ введенных в других странах стандартов по криптозащите информации показал, что модель нарушителя является важной частью в обеспечении информационной безопасности, поэтому при определении уровней безопасности СКЗИ учитываются возможности нарушителей.

Возникновение проблемы отсутствия модели нарушителя криптографической защиты информации в Республике Казахстан является естественным этапом при внедрении повсеместного использования автоматизированных систем для хранения, обработки и передачи информации.

Например, минимальная длина используемых ключей симметричных алгоритмов в Стандарте была не менее 60 бит, в настоящее время специализированная машина «Deep crack» в состоянии перебрать такие ключи за три дня.

Разработка моделей нарушителя позволит корректно определить (вычислить) безопасные пороги для вычислительной сложности известных алгоритмов вскрытия криптографической защиты информации, что в свою очередь, обеспечит надлежащий выбор и рациональное использование СКЗИ.

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал являются основной причиной и движущей силой нарушений и преступлений. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы, это и есть модель нарушителя. Модель нарушителя является важной частью в обеспечении информационной безопасности. Важно понимать, что игнорирование или недобросовестное построение модели может серьезно отразиться на сохранности защищаемой информации и привести к ее потере.

Так как за прошедшее время криптография получила новое развитие, а также выросли квалификация и технические возможности потенциальных нарушителей, положения и параметры Стандарта вычислены вне зависимости от моделей нарушителей и не соответствуют современному развитию информационных технологий. В связи с этим, авторами статьи проводится разработка собственных моделей нарушителей криптографической защиты информации.

Авторами поставлена цель – построить собственные модели нарушителя криптографической защиты информации и вычислить максимальные возможности каждой из них.

В различных источниках даются разные определения нарушителя информационной безопасности. Нарушитель безопасности информации (attacker) – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами [1].

Нарушитель информационной безопасности – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов или ради игры или удовольствия, с целью самоутверждения и т.п.) и использующие для этого различные возможности, методы и средства [2].

В любом случае, однозначно определено, что нарушитель – это некое лицо, обладающее теоретическими и практическими возможностями, априорными знаниями и располагающие временем для выполнения своих задач. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках разработки и анализа модели нарушителя.

Под моделью нарушителя, согласно [3], понимается абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа. Модель нарушителя позволяет выявлять и специфицировать возможные атаки, описывать их сценарии и формулировать возможные цели нарушителя. Модель будет также способствовать оценке конкретных атак с точки зрения их выполнимости, а также потребления ресурсов, которые нарушителю необходимо затратить для успешного проведения атаки [4].

Подходы к построению модели нарушителя у разных авторов различны, хотя и имеются общие классификационные признаки. При построении модели нарушителя используются следующие критерии: выделяют внутренних и внешних нарушителей, учитывают уровень профессиональной подготовки нарушителей, учитывают уровень знаний нарушителей об объектах атак, учитывают преследуемые цели нарушителей, учитывают наличие доступа и полномочий, учитывают возможность использования нарушителями различных средств для проведения атак, учитывается возможный сговор нарушителей разных категорий.

При проведении анализа уязвимостей и оценки эффективности интегрированных систем безопасности выделяют три типа нарушителей [5]: технологическая, оперативная и проектная.

Согласно приказу ФСБ России от 10 июля 2014 года №378, регламентирующему применение криптографических средств защиты информации и персональных данных, определены шесть классов потенциальных нарушителей: КС1, КС2, КС3, КВ1, КВ2, КА1.

В методических рекомендациях по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 года №149/54-144 приведены 6 основных типов нарушителей: Н1, Н2, Н3, Н4, Н5, Н6.

В Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК России и утвержденной Указом Президента Российской Федерации от 16 августа 2004 г. №1085 приведены 11 видов нарушителя и их возможных целей (мотивации) реализации угроз безопасности информации.

В литературе также встречается классификация из 3 видов нарушителей: с базовым (низким) потенциалом, с базовым повышенным (средним) потенциалом, с высоким потенциалом [6].

В связи с ростом квалификации и вычислительных возможностей потенциальных нарушителей в 2017 году были предложены 4 модели нарушителя криптографической защиты информации [7].

Под моделью нарушителя понимаем абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа, где нарушитель – это некое лицо, обладающее теоретическими и практическими возможностями, априорными знаниями и располагающее временем для выполнения своих задач [4].

Известно, что затрачиваемые ресурсы являются одними из параметров применяемых криптографических алгоритмов и выбор алгоритма вскрытия криптозащиты напрямую зависит от имеющихся технических возможностей нарушителя. Поэтому важно понимать, что разработка моделей нарушителя будет также способствовать оценке конкретных атак с точки зрения их выполнимости, а также потребления ресурсов, которые нарушителю необходимо затратить для успешного проведения атаки [5].

По определению, СКЗИ используются для обеспечения всесторонней защиты данных, которые передаются по линиям связи. Для этого необходимо соблюсти авторизацию и защиту электронной подписи, аутентификацию сообщающихся сторон с использованием протоколов передачи данных, а также защиту самого канала связи при необходимости. Существуют следующие механизмы применения СКЗИ для информационной защиты [6]:

1. Защита конфиденциальности хранимой или предаваемой информации.
2. При установлении связи обеспечивается идентификация.
3. Защита от навязывания (проникновение в связь со стороны) или повтора информации.
4. Контроль достоверности используемых ключей.
5. Обеспечение целостности информации.
6. Определение авторства документа.
7. Прочая защита – против закладок, вирусов, модификаций операционной системы.

Реализация данных механизмов зависит от возможностей нарушителя, что еще раз доказывает необходимость учета моделей при выборе алгоритма шифрования и уровня безопасности. Важным моментом является определение оптимального количества моделей нарушителя, так как его увеличение приведет к тому, что пользователям станет легче определять уровень безопасности СКЗИ, при этом увеличится и объем выполняемой ими работы. Модель нарушителя позволяет выявлять и специфицировать возможные атаки, описывать их сценарии и формулировать возможные цели нарушителя.

Авторами были рассмотрены разные шкалы моделей нарушителя с разными градациями. Учитывалось, что уровни моделей должны отличаться на равные значения рассматриваемых параметров, уровни должны быть стабильными по отношению к развитию информационных технологий и не зависеть от изменений политического характера или от количества жителей планеты и т.д.

При проведении исследования проведен анализ крупнейших предприятий мира (The World’s Largest Public Companies) для определения максимальных ресурсов потенциальных нарушителей [8].

В ходе работы были исследованы компьютеры различных производителей, однако в списке лидеров по соотношению «цена-качество» остались только два производителя: AMD и Intel. Другие поставщики компьютеров или используют процессора указанных

производителей или уступают по техническим характеристикам. Так процессоры фирмы VIA Technologies (Китай) стоят дешевле, но соответствуют по характеристикам более дешевым аналогам (начальный и средний уровни) процессоров Intel. Например, по тестам VIA Technologies, процессоры KX-5640 (4 ядра, 4 потока, 2,0 ГГц, 4 МБ кэш-памяти L2) и KX-U5680 (8 ядер, 8 потоков, 1,8 ГГц, 8 МБ кэш-памяти L2) по производительности находятся примерно на уровне Intel Atom C2750 (8 ядра, 8 потока, 2,4 ГГц, 4 МБ кэш-памяти L2) [9]. Цены на процессоры были взяты с официальных сайтов самих производителей, в случае отсутствия таковых была взята средняя цена поставщиков.

За основу выбора деления на 8 моделей был взят Предпринимательский кодекс РК от 29 октября 2015 года №375, в котором среднегодовой доход вычислен с 30-кратным шагом:

субъекты малого предпринимательства – среднегодовая численность работников не более ста человек и среднегодовой доход не свыше трехсоттысячекратного МРП;

субъекты крупного предпринимательства – среднегодовая численность работников более двухсот пятидесяти человек и (или) среднегодовой доход свыше трехмиллионнократного МРП.

На основании проведенного изучения и анализа возможностей нарушителей построены 8 моделей с шагом $\sqrt{1000}\approx 30$: Обыватель, Специалист, Малое предприятие, Предприятие, Крупное предприятие, Корпорация, Государство и Империя.

Все возможные противники авторами отнесены к одной из категорий нарушителей, описаны их финансовые, технические и человеческие (научные) ресурсы, мотивы и выгода нарушений.

1. Модель нарушителя "Обыватель"

К категории "Обыватель" будем относить большую часть населения Земли, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 30 МРП – это примерно 2,5 минимальных размеров заработной платы (в 2018 году МРЗП = 28284 тенге), около 0,44 среднемесячных заработных плат (в 2018 году СЗП = 162751 тенге). Так как по ВВП на душу населения Казахстана соответствует среднемировому уровню (в 2017 году – 8837,46 и 10038 USD соответственно, 74 место из 186 стран), то в эту же категорию попадает и большинство населения развивающихся стран мира [10].

В отношении нарушителя-обывателя будем полагать следующее: до 50% имеющихся финансовых средств нарушитель данной категории израсходует на оплату электроэнергии за работу персональных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 4 года. В среднем производительность компьютеров 4 миллиарда 64-разрядных операций в секунду. При использовании таких процессоров нарушитель может эксплуатировать в течение 4 лет несколько ЭВМ с общим количеством ядер до 4, на которых решать задачи с вычислительной сложностью до 4 (ядер) $\times 4\times 10^9$ (операций/с/ядро) $\times$ 3600 (с/час) $\times$ 24 (час/сутки) $\times$ 365,25 (сутки/год) $\times$ 4 (года) $\approx 2^2 \times 2^{32} \times 2^{25} \times 2^2 = 2^{61}$. Обыватель работает в фоновом режиме, так как вскрыть шифрограмму не главная его задача. В таком случае, число 2^{61} необходимо разделить на 2, так как 50% времени уходит на другие дела, в итоге вычислительная сложность получается 2^{60}. Обыватель может иметь в своем распоряжении персональную ЭВМ незначительной производительности, достаточной для работы текстовых редакторов, электронных таблиц и простейших игр, для которой сам обыватель или его

знакомые могут разработать прикладное программное обеспечение, реализовав криптографический алгоритм из случайно попавшей к ним книге по криптографии.

Таким образом, для защиты от нарушителя-обывателя вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{60}. Если ущерб законного владельца информации от такого вскрытия и, соответственно, потенциальный выигрыш нарушителя не превышают 30 МРП, то есть 10-кратно меньше затраченных им средств, то это сделает заведомо экономически невыгодным вскрытие криптографической защиты даже в условиях, когда нарушитель располагает существенно большими материальными и финансовыми средствами, объединяет свои усилия с другими нарушителями-специалистами, использует малобюджетные или уцененные средства вычислительной техники или приступает к вскрытию криптографической защиты через 5 лет с учетом роста производительности средств вычислительной техники.

Однако тенденцией является повсеместное повышение компьютерной и криптографической грамотности, доступность персональных ЭВМ с существенно возросшей вычислительной мощностью, появление в широком доступе в Интернете значительного количества программ и методик для вскрытия криптографической защиты, а также иного вредоносного программного обеспечения. Изменилась и мотивация нарушителей из-за повсеместной коммерциализации и, как следствие, криминализации общества.

2. Модель нарушителя "Специалист"

К категории "Специалист" будем относить специалистов в информационных технологиях, индивидуальных предпринимателей, преступников и иных физических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1000 МРП – это около 85 МРЗП. В эту же категорию попадает большинство населения экономически развитых стран [10]. То есть большинству специалистов и других физических лиц придется накапливать финансовые средства в течение нескольких лет, чтобы собрать указанную сумму. Таким образом, верхняя оценка в 1000 МРП для модели нарушителя "Специалист" является оправданной.

В отношении нарушителя-специалиста будем полагать следующее: до 50% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – персональных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 4 года, а остальные финансовые средства уйдут на оплату электроэнергии. Стоимость процессоров может достигать половины от стоимости персональной ЭВМ, то есть до $1000 \times 0{,}5 \times 0{,}5 = 250$ МРП. При использовании процессоров последнего поколения нарушитель может эксплуатировать в течение 4 лет несколько ЭВМ с общим количеством ядер до 25-32, на которых решать задачи с вычислительной сложностью до 32 (ядер) $\times$ 4×10^9 (операций/с/ядро) $\times$ 3600 (с/час) $\times$ 24 (час/сутки) $\times$ 365,25 (сутки/год) $\times$ 4 (года) $\approx 2^5 \times 2^{32} \times 2^{25} \times 2^2 = 2^{64}$.

Таким образом, для защиты от нарушителя-специалиста вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{64}.

3. Модель нарушителя "Малое предприятие"

К категории "малое предприятие" будем относить группы специалистов в информационных технологиях и криптографии, предприятия, организованные преступные группы и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 30 тыс. МРП. Например, в эту категорию попадает значительная часть казахстанских субъектов малого предпринимательства, то есть предприятия со среднегодовой численностью до 100 человек и со среднегодовым доходом до 300 тыс. МРП.

В отношении нарушителя-малого предприятия будем полагать следующее: до 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – серверных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 8 лет, а остальные финансовые средства уйдут на зарплату работников, приобретение или аренду помещений, оплату электроэнергии и других коммунальных услуг. Стоимость процессоров, в том числе сопроцессоров, может составлять до 90% от стоимости многопроцессорных серверных ЭВМ, то есть до 30 тыс. ×0,9×0,9 = 24 тыс. МРП. Согласно данным основных производителей процессоров для серверных ЭВМ, часть из которых приведены в таблице 2, условная стоимость одного ядра большинства процессоров составит 8-10 МРП при нормировании на производительность в 4 миллиарда 64-разрядных операций в секунду [10]. Однако более эффективную категорию серверных сопроцессоров составляют многоядерные вычислительные ускорители типа Tesla, для которых условная стоимость одного ядра составит 0,15-0,30 МРП, а при аналогичном нормировании всего 0,5-1,0 МРП. При использовании таких ускорителей нарушитель может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 24 тыс.: 0,15 = 160 тыс., на которых решать задачи с вычислительной сложностью до 160×10^3 (ядер) × $1{,}4\times10^9$ (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) ×4 (лет) ≈ $2^{17,5} \times 2^{30,5} \times 2^{25} \times 2^2 = 2^{75}$.

Таким образом, для защиты от нарушителя-малого предприятия, в том числе в случае попытки вскрытия им криптографической защиты через 5-10 лет, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{75} \times 2^{10:2} \times 1000 \approx 2^{90}$.

4. Модель нарушителя "Предприятие"

К категории "предприятие" будем относить группы специалистов в информационных технологиях и криптографии, предприятия, организованные преступные группы и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 млн. МРП.

Например, в эту категорию попадают практически все казахстанские субъекты среднего предпринимательства, то есть предприятия со среднегодовой численностью до 250 работников и со среднегодовым доходом до 3 млн. МРП соответственно.

В отношении нарушителя-предприятия будем полагать следующее: до 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – серверных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 8 лет, а остальные финансовые средства уйдут на зарплату работников, приобретение или аренду помещений, оплату электроэнергии и других коммунальных услуг. Стоимость процессоров, в том числе сопроцессоров, может составлять до 90% от стоимости многопроцессорных серверных ЭВМ, то есть до 1 млн.

×0,9×0,9 = 810 тыс. МРП. При использовании ускорителей типа Tesla нарушитель может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 810 тыс.: 0,15 = 5,4 млн., на которых решать задачи с вычислительной сложностью до $5{,}4\times10^6$ (ядер) × $1{,}4\times10^9$ (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) ×8 (лет) ≈ $2^{22,5} \times 2^{30,5} \times 2^{25} \times 2^3 = 2^{81}$.

Таким образом, для защиты от нарушителя-предприятия, в том числе в случае попытки вскрытия им криптографической защиты через 5-10 лет, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{81} \times 2^{10:2} \times 1000 \approx 2^{96}$.

5. Модель нарушителя "Крупное предприятие"

К категории "крупное предприятие" будем относить большие корпорации, специальные службы, преступные сообщества и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 30 млн. МРП. В эту категорию попадают практически все крупные предприятия Казахстана.

В отношении нарушителя-крупное предприятие будем полагать следующее: до 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – супер-ЭВМ, в том числе из списка TOP500, которые будут работать 24часа/7дней/8лет, а остальные финансовые средства уйдут на зарплату работников, приобретение или аренду помещений, оплату электроэнергии и других коммунальных услуг. Стоимость процессоров, в том числе сопроцессоров, может составлять до 90% от стоимости многопроцессорных супер-ЭВМ, то есть до 30 млн.×0,9×0,9 = 24 млн. МРП. При использовании многоядерных вычислительных ускорителей, ранее рассмотренных в модели нарушителя "Предприятие", нарушитель-корпорация может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 24 млн.: 0,15 = 160 млн., на которых решать задачи с вычислительной сложностью до 160×10^6 (ядер) × $1{,}4\times10^9$ (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) × 8 (лет) ≈ $2^{27,5} \times 2^{30,5} \times 2^{25} \times 2^3 = 2^{86}$.

Таким образом, для защиты от нарушителя-корпорации, в том числе в случае попытки вскрытия криптографической защиты через 10-20 лет и со 100-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{91} \times 2^{20:2} \times 10^6 \times 100 \approx 2^{128}$.

6. Модель нарушителя "Корпорация"

К категории "корпорация" будем относить транснациональные корпорации, специальные службы, преступные сообщества и иные компании, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 млрд. МРП.

В открытом доступе достоверные сведения о бюджетах спецслужб и преступных сообществ, как правило, отсутствуют. Опираясь на отрывочные сведения из Интернета, Агентство национальной безопасности США (годовой бюджет от 5 до 50 млрд. USD), Министерство государственной безопасности КНР (4-5 млрд. USD), Штаб-квартира правительственной связи Великобритании (около 1 млрд, фунтов стерлингов), Федеральная служба безопасности России (около 60 млрд, рублей), БНД ФРГ (552 млн. евро) и другие специальные службы для вскрытия криптографической защиты

конкретной системы не располагают средствами свыше 1 млрд. МРП, что примерно соответствует их квартальному (только АНБ США), годовому (МГБ КНР, ШКПС Великобритании, ФСБ России) или даже десятилетнему бюджету (БНД ФРГ и др.). Аналогичными средствами располагают наиболее сильные транснациональные преступные сообщества, в частности, сицилийская Коза Ностра, неапольская Каморра и другие преступные организации итальянской мафии (суммарный годовой доход всех организаций итальянской мафии около 200 млрд. евро).

В категорию "корпорация" заведомо попадают около 50 стран мира, имевшие в 2016 году ВВП не более 1 млрд. МРП, в том числе Таджикистан (6,9 млрд. USD, 143 место из 191 оцененной страны), Молдова (6,8 млрд., 144 место), Косово (6,7 млрд., 145 место), Кыргызстан (6,6 млрд., 146 место). Кроме того, представляется маловероятным, что даже в военное время страна на вскрытие криптографической защиты системы противника в состоянии потратить более 10% своего ВВП. Поэтому к этой же категории нарушителей целесообразно отнести более широкий перечень стран, включая Кению (68,9 млрд. USD, 70 место), Гватемалу (68,2 млрд., 71 место), Узбекистан (66,5 млрд., 72 место) и многие другие [8].

В отношении нарушителя-корпорации будем полагать следующее: до 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – супер-ЭВМ, в том числе из списка TOP500, которые будут работать 24часа/7дней/8лет, а остальные финансовые средства уйдут на зарплату работников, помещения, оплату коммунальных услуг. При использовании многоядерных вычислительных ускорителей, ранее рассмотренных в модели нарушителя "Предприятие", нарушитель-корпорация может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 810 млн.: 0,15 = 5,4 млрд., на которых решать задачи с вычислительной сложностью до $5{,}4\times10^9$ (ядер) × $1{,}4\times10^9$ (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) × 8 (лет) ≈ $2^{32,5} \times 2^{30,5} \times 2^{25} \times 2^3 = 2^{91}$.

Таким образом, для защиты от нарушителя-корпорации, в том числе в случае попытки вскрытия криптографической защиты через 10-20 лет и со 100-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{91} \times 2^{20:2} \times 10^6 \times 100 \approx 2^{128}$.

7. Модель нарушителя "Государство"

К категории "государство" будем относить развитые страны мира и иных юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 30 млрд. МРП.

Например, в эту категорию попадают Япония (4,9 трлн., 3 место), ФРГ (3,5 трлн., 4 место), Великобритания (2,6 трлн., 5 место) и другие развитые страны [8].

В отношении нарушителя-государства будем полагать следующее: практически все имеющиеся финансовые средства нарушитель израсходует на разработку, производство или приобретение средств вычислительной техники – супер-ЭВМ с доминантой передовых процессоров и сопроцессоров, которые будут работать 24часа/7дней/8лет. При государственном подходе издержки на производство гигантской партии вычислительной техники и, в частности, вычислительных ускорителей нарушитель сможет снизить до 0,01 МРП на ядро, то есть в 15-25 раз по сравнению с ценами вычислительных ускорителей, ранее рассмотренных в модели нарушителя

"Предприятие", а производительность каждого ядра повысится до 5 GFLOPS. В результате, нарушитель-империя может эксплуатировать в течение 8 лет значительное количество ЭВМ с общим количеством ядер до 30 млрд.: 0,01 = 3 трлн., на которых решать задачи с вычислительной сложностью до 3×10^{12} (ядер) × 5×10^{9} (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) × 8 (лет) ≈ $2^{41,5} \times 2^{32,5} \times 2^{25} \times 2^{3} = 2^{102}$.

Таким образом, для защиты от нарушителя-империи, в том числе в случае попытки вскрытия криптографической защиты через 15-30 лет и со 250-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{102} \times 2^{30:2} \times 30\times10^{6} \times 200 \approx 2^{150}$.

8. Модель нарушителя "Империя"

К категории "империя" будем относить ведущие страны мира и иных юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 трлн. МРП.

Например, в эту категорию попадают США (18,6 трлн. USD ВВП в 2016 году, 1 место в мире), КНР (11,2 трлн., 2 место), и другие ведущие страны, а также НАТО (892 млрд. USD бюджет 2016 года) [7].

В отношении нарушителя-империи будем полагать следующее: практически все имеющиеся финансовые средства нарушитель израсходует на разработку, производство или приобретение средств вычислительной техники – супер-ЭВМ с доминантой передовых процессоров и сопроцессоров, которые будут работать 24часа/7дней/8лет. Нарушитель-империя может эксплуатировать в течение 8 лет значительное количество ЭВМ с общим количеством ядер до 1 трлн.: 0,01 = 100 трлн., на которых решать задачи с вычислительной сложностью до 100×10^{12} (ядер) × 5×10^{9} (операций/с/ядро) × 3600 (с/час) × 24 (час/сутки) × 365,25 (сутки/год) × 8 (лет) ≈ $2^{46,5} \times 2^{32,5} \times 2^{25} \times 2^{3} = 2^{107}$.

Для защиты от нарушителя-империи, в том числе в случае попытки вскрытия криптографической защиты через 15-30 лет и со 250-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{107} \times 2^{30:2} \times 10^{9} \times 250 \approx 2^{160}$.

В ходе научного исследования авторами предложен метод вычисления параметров криптографических преобразований с примерно 30-кратным шагом на основе 8 моделей нарушителя.

Параметры криптографических преобразований нами вычислены как математические функции от возможностей потенциальных нарушителей, т.е. напрямую зависят от того сколько финансов, времени и человеческих ресурсов может потратить каждый. Некоторые полученные результаты вычислений совпадают с теми параметрами, которые были вычислены ранее в 2017 году [9], и это связано с отсутствием за последние 2 года резкого прорыва в развитии компьютерных технологий и криптографии,

Считаем, что использование данных моделей нарушителя позволит более эффективно определять уровень безопасности используемых СКЗИ и точно вычислять возможный ущерб от разглашения, навязывания и несанкционированного изменения защищаемой информации.

Полученные результаты рекомендуем учесть при последующей переработке Стандарта в целях обеспечения его соответствия современному мировому уровню развития технологий.

Литература

1. ГОСТ Р 53114-2008: Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.– URL: http://pqm-online.com>files>lib>std/ (дата обращения 29.11.2019).

2. Постановление Правительства РК от 20 октября 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». – URL: http://adilet.kz (дата обращения 20.11.2019).

3. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения. – URL: http://adilet.kz/ (дата обращения 20.11.2019).

4. Десницкий В.А., Чеулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами // Технические науки - от теории к практике: сб. ст. по матер. XXXIX междунар. науч.-практ. конф. № 39. – Новосибирск: СибАК, 2014- С.16-17.

5. Ахлюстин С.Б. Модель нарушителя в задачах анализа надежности интегрированных систем безопасности. – URL: https://cyberleninka.ru/article/v/ (дата обращения 20.11.2019).

6. Информационная безопасность банковских безналичных платежей. – URL: http://m.habr.com/ru/post/351326/ (дата обращения 20.02.2019).

7. Абдрахманов. А.Е. Модели нарушителя криптографической защиты и стандарт СТ РК 1073-2007. – URL: http://nblib.library.kz/elib/library.kz/jurnal/ (дата обращения 20.02.2019).

8. Global 2000 - The World’s Largest Public Companies 2018 – Forbes. – URL: http://www.forbes/com>global2000/ (дата обращения 20.02.2019).

9. Процессоры. – Санта-Клара: Intel, 2018. – URL: http://ark.intel.com/ru/ (дата обращения 20.02.2019).

10. ВВП стран мира на душу населения. – URL: http://visasam.ru/emigration/vybor/ (дата обращения 20.02.2019).

ВНЕДРЕНИЕ ОБРАЗОВАТЕЛЬНЫХ ОНЛАЙН ПЛАТФОРМ В УЧЕБНЫЙ ПРОЦЕСС СТУДЕНТА

Ризабек А.Д.
e-mail: arman.rizabek@narxoz.kz
АО Университет «Нархоз»,Казахстан

Аннотация. *Основные преимущества внедрения современного метода обучения. Обзор самых популярных образовательных платформ на актуальное время. Анализ основных инструментов в освоении учебного материала. Выявление необходимых компонентов образовательной платформы. Рассмотрены основные организационные формы педагогической деятельности, используемые для реализации совместных образовательных программ дистанционного обучения студентов в наукоемкой образовательной деятельности.*

В сфере образования уже давно началось время технологического и информационного прорыва: теперь с развитием высоких технологий и интернета, образование уже перестало быть таким стандартизированным как его помнят наши родители. Лекции мировых профессоров любых университетов в наши дни можно послушать, сидя дома. Всё чаще представители нового поколения осознанно выбирают дистанционное образование, используя различные курсы и вебинары, онлайн-платформы. Такие возможности нам дают целый ряд онлайн-платформ. Обучение доступно каждому, нужно лишь иметь подключение к интернету. Обозрим самые лучшие стороны такого метода обучения для освоения нужных нам учебных материалов. В настоящее время в сфере образования в нашей республике очень актуален вопрос об интегрировании онлайн-платформ в учебный процесс, так как современное электронное обучение, как это доказывает практика, располагает значительным потенциалом.

Как считают сами студенты по результатам опросов, инновационный подход к онлайн-обучению адаптирован под механику мышления более современных людей, которые хотят расширить каналы информации, нуждаются в том, чтобы повысить уровень конкретных навыков.

В наших реалиях уже рассматриваются основные этапы становления дистанционных образовательных технологий и информационно-коммуникационных средств, послужившие непрерывным источником создания и внедрения инноваций в образование и обучение. На данный момент представлены основные этапы эволюции информационно-коммуникационных технологий в обучении студентов. Первые этапы характеризуются развитием компьютерных коммуникаций и попытками внедрения их в образовательный процесс. Следующие этапы характеризуются бурным развитием информационно-коммуникационных технологий, появлением термина «дистанционное обучение», происходит признание технологий дистанционного обучения на уровне государства. Современные этапы характеризуются обилием систем дистанционного обучения и систем контроля знаний, эволюция технологий изменила как методики обучения, так и содержание образования. Происходит активное использование ресурсов веб 2.0, развитие технологий общения в сети, их ориентация на социальные потребности людей, использование их для обеспечения профессионально-ориентированного диалога в мировом информационном пространстве. Учебный процесс при дистанционном обучении студента включает в себя все основные формы традиционной организации учебного процесса.

Для реализации различных форм задач онлайн платформа предлагает виртуальный инструментарий, так называемые tools или инструменты. Виртуальный инструментарий включает в себя такие инструменты как «Форум», «Вики», «Глоссарий», «Банк данных», «Задания», «Чат» и другие, а также определённый набор административных инструментов для контроля и оценки заданий.

Далее мы рассмотрим самые популярны онлайн платформы для обучения по разным отраслям. Одними из самых интересных олнай платформ является Udacity – этот сервис будет интересен тем казахстанцам, кто расположен к точным наукам. Тут собраны курсы, посвященные языкам программирования, криптографии, робототехнике, физике. Примечательно, что здесь работают не только университетские профессоры, но и специалисты из ведущих компаний, в том числе Google и Microsoft. Что особенно приятно в работе с этим ресурсом, так это то, что пользователи не привязаны к наличию интернета. Так, отправляясь в дорогу, можно просто загрузить несколько уроков и не терять время в пути даром.

К числу нужных онлайн платформ так же относится проект Coursera в сфере массового онлайн-образования. Проект был запущен в 2012 году. Coursera основана профессорами информатики Стэнфордского университета Эндрю Ыном и Дафной Коллер. На базе сотрудничества с большим спектром университетов, онлайн-платформа создает образовательные материалы, сформированные в систему курсов, которые проходят студенты. На сайте Coursera проводятся тесты и экзамены. Также имеется официальное мобильное приложение для iPhone и Android что выгодно отличает от других платформ. В проекте представлены полноценные курсы по физике, инженерным дисциплинам, гуманитарным наукам, искусству, медицине, биологии, математике, информатике, экономике и бизнесу. Продолжительность курсов варьируется от шести до десяти недель, куда входят видео-лекции, презентации, домашние задания и тексты. Предусмотрены чаты с сокурсниками, где можно обсуждать идеи и помогать с решением задач. Курсы можно пройти как на английском, так и на русском языке, зачастую с субтитрами. Coursera сотрудничает с университетами Стэнфорда, Принстона, Мичигана, Пенсильвании и многими другими. По окончанию обучения студенты получают соответствующие сертификаты и дипломы. Это может быть степень бакалавра или магистра. По последним данным, Coursera насчитывает более 25 миллионов пользователей, 149 университетов-партнёров, около 2000 тысяч различных курсов по 180 специализациям. Большая часть курсов основана на платной основе, но есть и набор семинаров, лекций, доступных бесплатно.

Microsoft Virtual Academy - задача этого онлайн-ресурса состоит в том, чтобы обучить пользователей основам программирования, в максимально доступном формате. Все курсы проходят бесплатно, используя знания экспертов компании Microsoft. В списке образовательных программ числятся: изучение HTML5, CSS3 и JavaScript, разработка игр, приложений, визуализация серверов и многое другое. Курсы предусмотрены для разных уровней подготовки, от начинающих до продвинутых программистов. Новые курсы появляются на сайте каждую неделю. Учебный план пользователь может создавать самостоятельно, согласно тем навыкам, которые он хочет развить. Продвинутая система отслеживания прогресса позволяет проходить тестирования, а в дальнейшем получить сертификат Microsoft Virtual Academy.

К числу интересных онлайн платформ можно отнести также HTML Academy. Этот образовательный ресурс обладает всем необходимым, для тех, кто начинает свой путь в сфере IT. Портал выбрал для себя одно чёткое направление – Frontend. Пользователи обучаются основам HTML, CSS и JavaScript. Курсы выстроены максимально интерактивно, с практическим уклоном. Программы обучения состоят из многочисленных упражнений, в ходе которых ученику необходимо изменять HTML и CSS код в онлайн-редакторах, следуя указаниям системы. Учебная программа состоит из восьми детальных тем. По итогам обучения, пользователи получают задания сверстать макет сайта или написать код. Усвоив базовые знания, есть возможность пройти интенсивный курс, где под руководством личного наставника пользователи научаться создавать современные сайты и веб-приложения по критериям качества, принятым в веб-индустрии. На сайте представлено около 1200 различных заданий и испытаний. Обучение можно пройти бесплатно или по подписке.

Обозревая все эти онлайн платформы для обучения можно выявить специфику различных образовательных порталов. Образование дают в разных местах: в детских садах, школах, колледжах, ВУЗах, на курсах и т.д. Для каждой аудитории характерны особые черты, которые нужно учитывать при создании платформы. Образовательная

онлайн платформа может стать практически полноценным учебным заведением, расположенным в сети. Благодаря современным технологиям на таком ресурсе может быть размещена любая образовательная программа. И каждый желающий получить знания может в любое время получить к ним доступ. Создание образовательного портала обычно занимает огромное количество времени и требует огромных финансовых затрат.

В наших реалиях хорошо продуманная обучающая онлайн платформа должна использовать весь спектр возможностей, которые предоставляет нам интернет. К числу возможностей нельзя исключать видео курсы с конкретными заданиями и рекомендациями. Образовательная онлайн платформа в арсенале университета будет большим хранилищем и генератором огромной базы знаний, которая безусловна облегчит и ускорит освоения знаний студентам ВУЗов.

В заключении необходимо подчеркнуть, что использование метода онлайн платформ при преподавании теоретических предметов в ВУЗах способствует наилучшему усвоению учебного материала, развивает умение студентов самостоятельно осваивать теоретический и практический материал, приучает высказывать свою точку зрения по проблемам, предложенным на платформе. Интерактивные задания в союзе с традиционным учебником дают не только хорошие результаты, но повышают степень индивидуализации обучения на уроке, стимулируют студентов к активному получению знаний. Следовательно, закрытые учебные онлайн-платформы обладают весомым методическим потенциалом, открывают широкие возможности в сфере обучения и способствуют интенсификации учебного процесса

Список использованных источников:

1. Туракулова С. Т. «К вопросу о возможности использования онлайн платформ для интенсификации обучения в вузах» № 20 (154) / 2017 497с.
2. Онлайн-платформы.–https://the-steppe.com/gorod/10-onlayn-platform-kotorye-prokachayut-vash-mozg (10.11.2019).

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА МОНИТОРИНГА КАЧЕСТВА ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ БАКАЛАВРОВ

Сансей А.Ш.
e-mail: adil.sansei@narxoz.kz
АО «Университет «Нархоз», студент 2-курса магистратуры специальности «Информационные системы»,
научный руководитель: к.э.н., ассоц. проф. Алдажаров К.С.,
Казахстан

Аннотация. *В статье рассматриваются организационно-педагогические условия мониторинга качества подготовки бакалавров в образовательном учреждении высшего образования. Выявлены факторы, влияющие на выбор условий мониторинга. В работе определены показатели мониторинга качества подготовки бакалавров: сформированные у них на необходимом уровне общекультурные и профессиональные*

компетенции с учетом требований работодателей как основных заказчиков образовательных услуг и профессионального стандарта.

Мониторинг качества подготовки бакалавров как единство его содержательной, процессуальной и результативной сторон будет эффективен только при определенных организационно-педагогических условиях. Понятие «условия» является общенаучным, под ними понимаются определенная совокупность причин, обстоятельств, влияющих на функционирование и развитие объекта.

Организационно-педагогические условия рассматриваются учеными как «совокупность объективных возможностей, обеспечивающая успешное решение поставленных задач, обстоятельства взаимодействия субъектов образовательного процесса, являющиеся результатом целенаправленного планируемого отбора, конструирования и применения элементов содержания, методов (приемов) для достижения цели педагогической деятельности, совокупность возможностей содержания, форм, методов целостного образовательного процесса».

Успешность выделения условий зависит от того, насколько четко определена структура мониторинга качества подготовки бакалавров в вузе и соответствует ли она ожидаемым результатам. К тому же эффективность мониторинга, как правило, достигается за счет реализации целого комплекса условий.

В результате изучения научной литературы по данной теме было выявлено, что выбор комплекса условий мониторинга качества подготовки бакалавров обеспечивается влиянием некоторых факторов: государственного заказа на компетентного специалиста, конкурентоспособного в определенной сфере деятельности; образовательной среды, в которой реализуется мониторинг качества; процессуальной и результативной составляющих мониторинга качества подготовки бакалавров; компонентов мониторинга качества: целевого, теоретико-методологического, содержа-тельного, технологического, оценочно-результативного; оценки качества на основе принципа согласованности действий всех заказчиков образовательных услуг (вуза, обучающихся, работодателей); комплекса личностных качество субъектов мониторинга [3], [6].

Кроме того, анализ опыта вузов позволил выделить некоторые тенденции реализации мониторинга качества подготовки бакалавров, которые могут способствовать определению условий его проведения: мониторинг дает возможность реконструировать систему образования, чтобы соответствовать потребностям общества и развитию индивидуальных возможностей обучающихся; выстраивать новые отношения между обществом и образовательными учреждениями; согласованность требований субъектов мониторинга качества на разных уровнях приводит к развитию пространства выбора направлений, видов и форм мониторинговой деятельности; выстраивание системы работы вуза с работодателями как основными заказчиками образовательных услуг; рост востребованности научного консультирования работодателей представителями академического сообщества вуза по вопросам интеграционного взаимодействия с целью повышения качества образования; разработка контрольно-измерительных материалов, диагностического инструментария, критериев и показателей мониторинга качества подготовки бакалавров.

Реализация данного мониторинга возможна при учете двух основных аспектов: организационного (организация образовательного процесса в рамках мониторинга) и личностного (взаимодействие всех его субъектов).

В связи с этим мы можем говорить об организационно-педагогических условиях, создаваемых в образовательном процессе. Их реализация обеспечивает наиболее эффективное протекание процессов, в основании которых лежит педагогическая деятельность [6].

В качестве методологического ориентира при определении структуры данного вида мониторинга использовались основные положения компетентностного подхода. Как показывает анализ понятия «компетенции», в настоящее время не существует общепринятого определения данной категории. Общим является понимание ее как способности личности справляться с самыми различными задачами (Ю.И.Алюшина, В.С. Безрукова, С.Г. Воровщиков, В.А. Ситаров, В.М. Шепель). Понятие включает различные стороны деятельности: мотивационную, операционально-технологическую. Компетенции/компетентности могут интерпретироваться как единый согласованный язык для описания академических и профессиональных профилей и уровней высшего образования (Ю.Г. Татур). В России реализация компетентностного подхода будет способствовать поддержанию единого образовательного, профессионально-и культурно-ценностного пространства. Под компетентностным подходом к проектированию ФГОС ВО В.И. Байденко предлагает понимать метод моделирования результатов образования как норм его качества [4].

Определение структуры мониторинга качества подготовки бакалавров в вузе для выявления организационно-педагогических условий, считают исследователи, необходимо осуществлять через анализ его функций [1], [3], [6]. Поскольку мониторинг тесно связан со всеми функциями управления (такими как целеполагание, информация, контроль, анализ, координация, принятие управленческих решений), то выделяют следующие функции мониторинга: анализа, мотивации и стимулирования, контроля, принятия управленческих решений. В связи с этим мониторинг качества подготовки бакалавров в вузе можно рассматривать как систему непрерывного слежения за функционированием и развитием образовательного процесса с целью диагностики формирования общекультурных и профессиональных компетенций выпускников, педагогического прогнозирования и управленческих решений по коррекции образовательного процесса [5].

С точки зрения компетентностного подхода с учетом функций мониторинга, указанных ранее показателями качества подготовки бакалавров, могут служить сформированные у них общекультурные и профессиональные компетенции учитывающие требования работодателей как основных заказчиков образовательных услуг и профессионального стандарта.

Структуру мониторинга качества удобно представить в виде модели. Мы приняли во внимание теоретико-методологические подходы моделирования и разработали модель мониторинга качества подготовки бакалавров в вузе, включающую структуру компетенций выпускника и состоящую из пяти взаимосвязанных блоков (компонентов): целевого, теоретико-методологического, содержательного, технологического, оценочно-результативного (рисунок №1).

Целевой компонент дает представление об объективной цели реализации мониторинга качества подготовки бакалавров в вузе. Теоретико-методологический блок определяет цель мониторинга, раскрывает исходные положения и принципы его организации, выявляет возможности и условия мониторинговой деятельности. К структурным компонентам содержательного блока относятся содержание и особенности проведения мониторинга качества. Здесь отражены исходные психолого-педагогические

положения, взаимодействие всех субъектов мониторинга, его организационно-педагогические условия, а также образовательный результат –освоенные выпускниками-бакалаврами общекультурные и профессиональные компетенции с учетом требований работодателей.

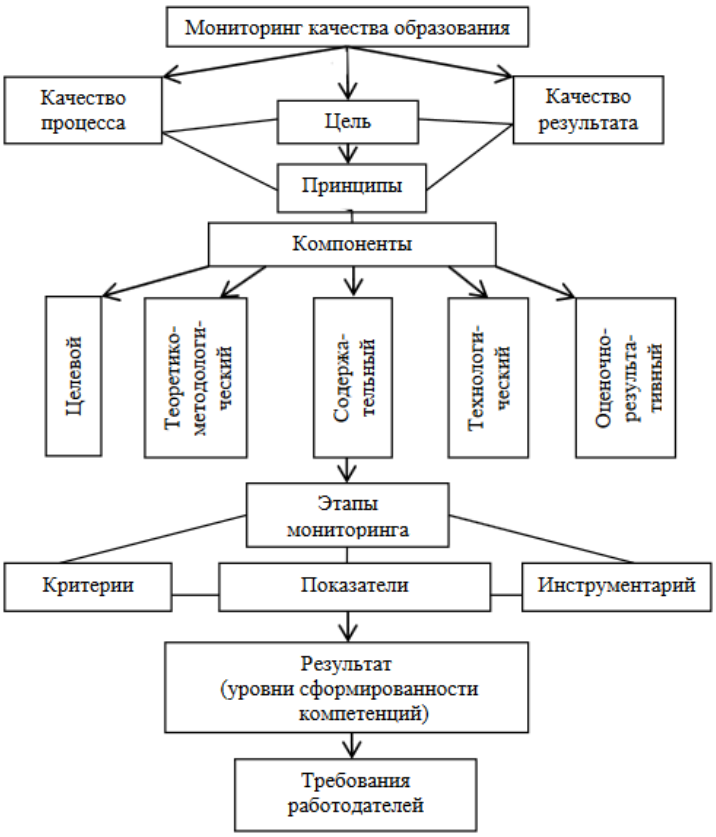


Рис. 1 Модель мониторинга качества подготовки бакалавров

Литература

1. Абрамов С. М., Пронина И. И. Мониторинг качества подготовки бакалавров с двумя профилями // Университетский комплекс как региональный центр образования, науки и культуры: сборник научных трудов по материалам Всероссийской научно-методической конференции. – Оренбург: Оренбургский государственный университет, 2017. –С. 2716–2718.

2. Белоцерковский А. В. О «качестве» и «количестве» образования // Высшее образование в России. –2011. –No 4. –С. 3–9.

3. Белоцерковский А. В., Кравцова Л. А., Дождиков А. В. Независимая внешняя оценка качества подготовки бакалавров// Высшее образование в России. –2013. –No 5. –С. 3–12.

4. Болонский процесс: Результаты обучения и компетентностный подход / под редакцией В. И. Байденко. –Москва: Исследовательский центр проблем качества подготовки специалистов, 2009. –536 с.

5. Вискова Т. А. Мониторинг качества подготовки специалистов в вузе // Парадигмы университетской истории и перспективы университетологии (к 50-летию Чувашского государственного университета им. И. Н. Ульянова): сборник статей в 2 томах. –Чебоксары: Издательский дом «Среда», 2017. –Т. 2. –С. 204–206.

6. Коннова З. И., Гладкова О. Д. Организационно-педагогические условия эффективного мониторинга качества профессиональной языковой подготовки студентов в условиях информационной методической среды кафедры // Фундаментальные исследования. –2011. –No 11. –С. 121–129.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ В КОНТЕКСТЕ БОЛЬШИХ ДАННЫХ

Сейдалиев Ш.А.
email: shake.seyd@bk.ru
Академия Комитета национальной безопасности РК,
Казахстан

Аннотация: *В эпоху больших данных образ жизни людей, их повседневные привычки и образ мышления претерпели колоссальные изменения. Большие данные стали важной темой для исследований в промышленности и научных кругах. Но большие данные-это палка о двух концах. Технология приносит удобство людям и несет определенные риски. В процессе сбора, хранения и использования данных это может легко привести к утечке личной информации, а также к тому, что данные могут быть модифицированы. На современном этапе исследований одним из самых острых вопросов стало, как обеспечить безопасность больших данных и защиту конфиденциальности. Статья описывает технологию больших данных, анализирует проблемы безопасности больших данных и предлагает стратегии защиты для обеспечения безопасности и конфиденциальности.*

Ключевые слова: *Большие данные, big data, безопасность, конфиденциальность, приватность, информационное воздействие, манипуляции.*

В эпоху больших данных люди получают выгоду от интернет-технологий. В настоящее время предприятиям приходится работать с большими объемами информации, которая часто обновляется и приходит из разных источников. В сущности, понятие big data предполагает работу с информацией большого объема и разнообразного состава, обновляемой очень часто и находящейся в разных источниках. Как правило, большие данные поступают из трех источников это: Интернет (СМИ, социальные сети, блоги, форумы и другие сайты); архивы корпоративных документов т.е. базы данных; показания приборов, датчиков и других устройств. С помощью технологий Big Data организации могут анализировать огромные массивы данных и выявлять полезные закономерности, дающие им конкурентные преимущества. Но как бы эта технология не была полезной, так же существуют и определенные проблемы безопасности. Есть два основных аспекта, которые должны быть рассмотрены при обсуждении проблем безопасности больших данных. Первый аспект - как государственные органы, организации и квазигосударственные учреждения, могут обезопасить колоссальные объемы генерируемой информации о пользователях их систем? Второй аспект - состоит в определении способов, в которых аналитика больших данных может быть применена для роста уровня безопасности. В первом случае проблема начинается с классификации

и идентификации данных. Необходимо находить возможности правильно идентифицировать как данные, так и источники, которые ее генерируют и обрабатывают, и, соответственно, необходимо классифицировать информацию (происхождение, структура, типология и т.д.). Таким образом, можно спроектировать организованную среду больших данных, над которой намного легче вести контроль. Это означает слияние облачной вычислительной среды с системами хранения и возможностями обработки данных, которые потребуют новых конкретных мер безопасности. В конечном счете, правильная классификация данных будет одним из шагов в создании, зашифрованной на основе атрибутов среды, что приведет к построению более безопасной среды больших данных. Затрагивая второй аспект, можно прийти к выводу, что существует много эффективных способов применения технологии big data для повышения уровня безопасности, а выбор наиболее приемлемого из них будет полностью зависеть от систем и направлений деятельности. Например, потоки огромных структурированных и неструктурированных данных могут быть использованы для создания моделей прогнозирования, которые позволят организациям прогнозировать атаки, поведение пользователей и др. Аналитика технологий big data позволяет моментально извлекать необходимую информацию из различных источников, что дает возможность компаниям получить максимально подробную информацию, собираемую из логов, в режиме реального времени. Хорошим примером этого могут служить высокоэффективная защита, достигаемая с помощью SIEM и IDS - систем, которые используют передовые методы машинного обучения и большие данные, чтобы мгновенно узнать о потенциально опасном поведении и его источниках[1].

Основываясь на этом, во времена развития технологии больших данных, необходимо найти решение как уладить проблемы безопасности и конфиденциальности в контексте больших данных.

Информационное пространство, как объект технологии больших данных, является инструментом, предоставляющим максимально-доступный объем данных за минимальное время «по желанию» субъекта. Использование различных технологий с применением ресурсов предоставляемых посредством интернет-среды, открывает новые горизонты манипулирования обществом на уровне государств, союзов, стран, расположенных в любой точке географического пространства. Направленность ресурсов, их подача, освещение по отношению к одной и той же проблеме может являться диаметральной от позитивной для одного слоя, общества, региона, государства до негативной для другого. От созидания, до разрушения. В тоже время при необходимости цели фокусируются адресно, точно, выверено, на которые обрушивается скоординированный совокупный ресурс.

Воздействие на общество и личность осуществляется с помощью преднамеренного целенаправленного воздействия с учетом личности, социальных слоев и интересов. Примером может являться распространение идей экстремизма, избранности, использование «двойных стандартов» в современном мире. Горизонты манипулирования постепенно расширялись с совершенствованием технических возможностей интернет-ресурсов. Масштабы манипуляции общественными институтами, в котором подавляющая часть населения доверяет источникам информации и без особого труда поддается влиянию, значительно расширились [2].

Искусная обработка информации делает возможности манипулирования обществом практически безграничными, так как в подавляющей части оно не имеет сформированного собственного мнения. Информационное воздействие на общество

способно привести к смене проводимой политики, изменению правительства, государственного строя. При этом общество даже не ощущает, что воздействие навязано извне. Это опасно для любого государства, не обладающего соответствующим иммунитетом. Информационные воздействия могут стимулировать поведение каждой личности; использоваться для достижения конкретных целей для изменения состояния, структуры общества, быть конструктивными, нейтральными, деструктивными. В обиход входят понятия «кибербезопасность», «кибергигиена», «информационный суверенитет», «кибернетические войны», «кибернетический солдат», «боты» и т.д.

Для противодействия негативным информационным воздействиям надо сформировать матрицу основных угроз. В дальнейшем на основе сформированной матрицы основных угроз осуществлять мониторинг СМИ, социальных сетей и других площадок, не зависимо от форм собственности, способов распространения. Основная задача, которой выявление методов манипулирования с целью принятия блокирующих мер.

Государственные органы в своей деятельности работают с большими объемами данных. К ним могут относиться статистические показатели, базы данных. Часто именно они становятся целью злоумышленников. Кроме того, нарушения в области неприкосновенности частной жизни заключаются в извлечении, распространении или использовании приватной информации. Так, в частности, не каждый пользователь захочет, чтобы кто-то знал, какие сайты он посещает, какими продуктами интересовался. В других случаях это касается сбора приватной информации пользователя информационных ресурсов через средства мобильной связи и прочие «умные» гаджеты составляя портрет потребителя, основываясь на личных данных *(например, пол, возраст)* и поисковых запросах.

В нынешнее время, информация распространяется чрезвычайно быстрыми темпами. В тоже время при передаче информации, из-за слабого контроля над информацией в данных, отсутствии технической поддержки, несовершенной системы контроля, может произойти утечка данных, что вызовет множество негативных и отрицательных последствий для отдельных лиц, предприятий и даже общества, что приведет к большим политическим и экономическим потерям. Так, в нынешнем году персональные данные 11 млн. казахстанцев оказались в свободном доступе, любой желающий мог свободно получать доступ к системе или полностью загрузить ее к себе локально. При анализе данных содержащихся в базе было обнаружено, что информация свежая и актуализирована около половины года назад, персональная информация была проиндексирована поисковыми системами Google и Yandex [3].

Так же в июле 2019 года в Казахстане произошла утечка медицинской информации сотен тысяч пациентов сети клиник Damumed. Виной утечки стала элементарная ошибка - неавторизованный доступ к медицинским документам организации, т.е. инцидент передачи третьим лицам информации, содержащей конфиденциальные данные, произошел от лица, имеющего легальный авторизованный пользовательский доступ в медицинскую информационную систему Damumed [4].

Чрезвычайно важным является повышение контроля и мониторинга различных информационных площадок на наличие недостоверной информации. Во-вторых, осуществлять надзор и управление социальной информацией, чтобы гарантировать безопасность, что личная информация не будет использована преступниками, что приведет к большим потерям. Кроме того, повышать осведомленность пользователей о мерах предосторожности и свести к минимуму заполнение личной важной

(конфиденциальной) информации. Так же, уведомлять об ответственности и повышать знания государственных служащих имеющих прямой доступ к персональной информации граждан, т.к. согласно Закону Республики Казахстан «О персональных данных и их защите» п.1 ст.11 «Лица, которым стали известны персональные данные ограниченного доступа в связи с профессиональной, служебной необходимостью, а также трудовыми отношениями, обязаны обеспечивать их конфиденциальность» [5]. Необходимо ужесточить наказание за уголовные правонарушения в сфере информатизации и связи.

Также, одним из предложений является создание агентства по защите конфиденциальности. В большинстве западных стран созданы специальные агентства по защите конфиденциальности для защиты частной информации. Создав в Республике Казахстан агентство по защите конфиденциальности, стало бы возможно решать задачи по защите персональных данных, эффективно пресекать посягательства на частную жизнь наших граждан.

Список литературы

1. Безопасность данных в эпоху Больших данных. - https://www.securitylab.ru/blog/company/PandaSecurityRus/343466.php (18.12.2019 г.)
2. Фрейд З. Психология масс и анализ человеческого "Я". М.: Азбука, 2014 - 192с.
3. Персональные данные казахстанцев оказались в свободном доступе - https://profit.kz/news/53462/Personalnie-dannie-kazahstancev-okazalis-v-svobodnom-dostupe (19.12.2019 г.)
4. Утечка данных пациентов - https://www.zakon.kz/4976956-utechka-dannyh-patsientov-minzdrav-rk.html (19.12.2019 г.)
5. Закон Республики Казахстан «О персональных данных и их защите» от 21.05.2013 N 94-V.

УМНОЖИТЕЛЬ ЧИСЕЛ ПО МОДУЛЮ С АНАЛИЗОМ ДВУХ СТАРШИХ РАЗРЯДОВ МНОЖИТЕЛЯ ЗА ШАГ

Тынымбаев С.Т.[1], Айтхожаева Е.Ж.[2], Бердибаев Р.Ш.[1], Абильда Б.Г.[3]
e-mail: ait_djam@mail.ru
[1] Алматинский Университет Энергетики и Связи имени Г. Даукеева,
[2] Казахский Национальный Технический Университет имени К.И. Сатпаева,
[3] Евразийский Национальный Университет имени Л. Гумилева,
Казахстан

Аннотация. *В работе рассматривается быстродействующий умножитель чисел по модулю, который является базовым устройством для криптосистем с открытым ключом. В умножителе аппаратными средствами на каждом шаге умножения анализируются два разряда множителя, начиная со старших разрядов, и формируются частичные произведения, что в два раза ускоряет процесс умножения по модулю. При этом, параллельно с умножением, в блоках формирования частичных*

остатковумножителя выполняется операция приведения по модулю получаемых частичных произведений, что позволяет исключить временные затраты на приведение по модулю многоразрядного произведения. Ускорение умножения достигается за счет дополнительных аппаратных затрат.

Введение. Умножение чисел по модулю является актуальной задачей асимметричной криптографии [1, 2]. В данной работе рассматривается умножитель по модулю с анализом двух разрядов множителя за шаг (начиная со старших разрядов), который позволяет уменьшить количество шагов умножения в два раза. А чтобы избежать ресурсозатратной по времени операции приведения по модулю многоразрядного произведения, необходимо выполнять приведение по модулю частичных произведений параллельно процессу их получения.

Умножение по модулю с анализом двух старших разрядов множителя и приведение по модулю частичных произведений во время их получения позволяют ускорить процесс умножения по модулю за счет дополнительных аппаратных затрат.

Учитывая, что используется позиционная двоичная система счисления, и представив B в виде полинома с использованием основания двоичной системы счисления, произведение двух целых чисел A и B можно представить в следующем виде:

$A \cdot B = A \cdot (b_{n-1}2^{n-1} + b_{n-2}2^{n-2} \ldots + b_1 2 + b_0) = A \cdot (b_{n-1} \cdot 2^{n-1}) + A \cdot (b_{n-2}2^{n-2}) + \ldots + A \cdot b_1 2 + A \cdot b_0 = [A \cdot 2^{n-1}(b_{n-1}) + A \cdot 2^{n-2}(b_{n-2})] + [\ldots] + [A \cdot 2(b_1) + A \cdot (b_0)]$.

На каждом шаге умножения выполняется получение и приведение по модулю двух слагаемых этого полинома. Умножение на 2 реализуется путем сдвига влево на один разряд.

Основная часть. Функциональная схема быстродействующего умножителя по модулю приведена на рисунке 1. В состав умножителя входят: регистр RgA для приема и хранения множимого A, сдвигающий регистр RgB для хранения и сдвига множителя B, регистр RgP для приема и хранения модуля P, формирователи частичных остатков PRF1 и PRF2, а также регистр RgPRF для временного хранения остатков, блок синхронизации БСИНХ (SynU на рисунке 1), который состоит из триггера, счетчика импульсов Count, схемы И1, блока схем И2 и элементов задержки DL.1÷ DL.3. На входы БСИНХ подается сигнал START, тактовые сигналы Clock и двоичный код числа сдвигов К-1. В состав умножителя также входят блоки схем И3÷И9.

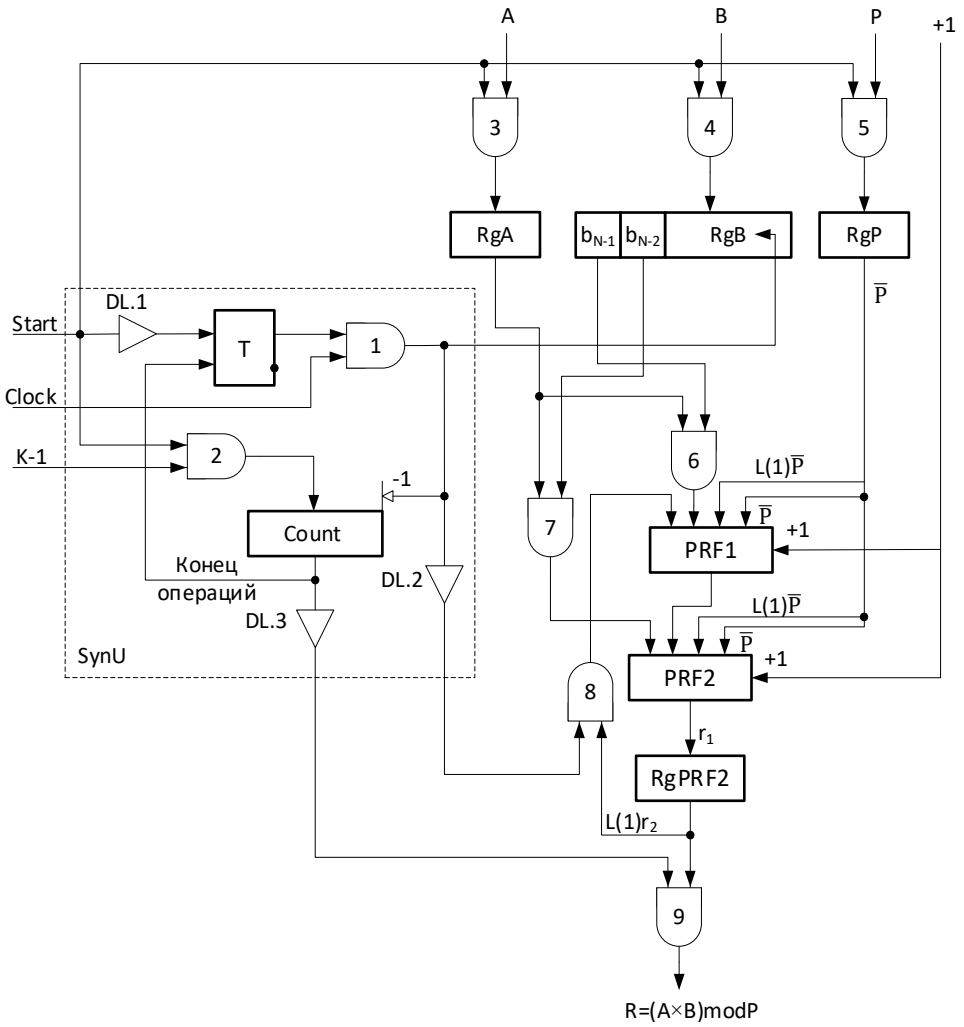


Рис. 1. Функциональная схема умножителя чисел по модулю с анализом двух старших разрядов множителя

Центральными блоками умножителя являются формирователи частичных остатков PRF1 и PRF2. На рисунке 2 приведена функциональная схема формирователя частичных остатков PRF. PRF служит для формирования частичного остатка r_i путем приведения числа C_i по модулю P, т.е. $r_i = (2r_{i-1}+A \cdot bj) \ modP$ (j=N-i+1).

PRF состоит из сумматора Add1, где суммируются удвоенный предыдущий частичный остаток $2r_{i-1}$ с множимым A (при b_j=1), в результате которого вычисляется значение $C_i = 2r_{i-1}+A \cdot b_j$. Сумматоры Add2, Add3 и блоки схем И1÷И3, ИЛИ1 служат для формирования частичного остатка r_i. Значение C_i подается на левые входы Add2 и Add3. На правые входы Add2 подается $\overline{P}$ со сдвигом влево на один разряд, т.е. $2\overline{P}$. На правые входы Add3 подается обратный код модуля $\overline{P}$. На входы младших разрядов Add2 и Add3 подается уровень +1, что позволяет обратные коды $2\overline{P}$ и $\overline{P}$ перевести в дополнительный код. Это дает возможность заменить операцию вычитания операцией сложения.

Конкретные значения частичного остатка r_i можно вычислить путем анализа соотношений значений C_i, 2P и P. В таблице 1 приведены условия формирования остатка C_i.

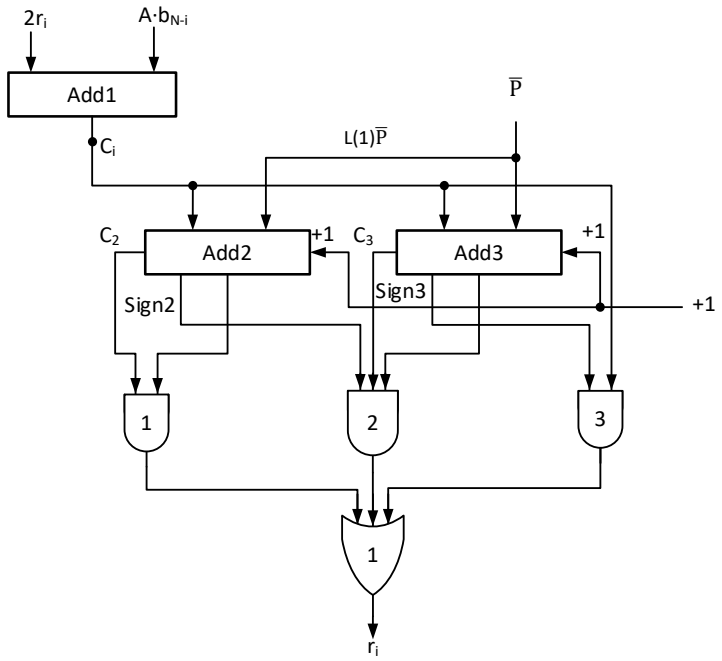


Рис. 2. Функциональная схема формирователя частичных остатков PRF

Таблица 1. Условия формирования частичного остатка r_i

Условия	*Вычисление r_i*
$C_i<P$	$r_i= C_i$
$P\leq C_i<2P$	$r_i= C_i-P$
$2P\leq C_i$	$r_i= C_i-2P$

Для вычисления r_i в сумматоре Add2 выполняется операция C_i-2P, что соответствует операции сложения в дополнительном коде $C_i+2\overline{P}+1$. В сумматоре Add3 выполняется операция C_i-P, что соответствует операции сложения в дополнительном коде $C_i+\overline{P}+1$. При условии C_i <P значение r_i соответствует C_i.

Операции сложения в сумматоре Add2 и Add3 выполняются одновременно и одновременно вырабатываются переносы из знаковых разрядов C_2 и C_3 и знаки операций Sign2 и Sign3 на соответствующих выходах сумматоров Add2 и Add3.

В таблице 2 приведены условий формирования наименьшего остатка r_i в зависимости от значений переносов C_2 и C_3 и знаков Sign2 и Sign3.

Таблица 2. Условия формирования наименьшего положительного остатка на выходах сумматоров Add2 и Add3

№	*C_2*	*Sign2*	*C_3*	*Sign3*	*Выходы сумматоров*		*C_i*
					Add2	*Add3*	
1	*1*	*0*	*1*	*0*	r_i	–	–
2	*0*	*1*	*1*	*0*	–	r_i	–
3	*0*	*1*	*0*	*1*	–	–	$r_i=C_i$

Из таблицы 2 видно, что при $C_2=C_3=1$ и Sign2=Sign3=0 наименьший положительный остаток r_i определяется разницей C_i-2P с выходов сумматора Add2, значение которого передается на выходы схем И1 с уровнем $C_2=1$ одновременно.

При значениях $C_2=0$ и $C_3=1$ остаток $r_i=C_i-P$ формируется на выходах сумматора Add3. Уровнями Sign2=Sign3=0 блокируется передача кодов на выходы блоков схем И2 и И3. При этом выходы сумматора Add2 сигналом $C_2=0$ блокируются, их прохождение на вход блока схем И1 не происходит. Сигналом Sign3=0 блокируется прохождение значений C_i на выход схемы И3.

При $C_2=C_3=0$ блокируются выходы Add2 и Add3. Сигналом Sign3=1 значение C_i схемой И3 передается на выход умножителя в качестве остатка ($r_i=C_i$).

Работа умножителя начинается с подачи на вход БСИНХ сигнала START. По этому сигналу в регистр RgB принимается множитель B, в регистр RgA принимается множимое A и модуль P принимается в регистр RgP.

Сигналом START в счетчик Count записывается двоичный код числа необходимых сдвигов через блок схем И2. После приема множителя B в RgB, в его старших разрядах фиксируются биты b_{N-1} и b_{N-2}. Старший разряд множителя b_{N-1} связан с управляющим входом блока схем И6, а разряд множителя b_{N-2} связан с управляющим входом блока схем И7. На информационные входы блоков схем И6 и И7 подаются разряды множимого из регистра RgA.

Выходы блока схем И6 связаны с входами формирователя PRF1. На входы PRF1 также подаются модули $2\overline{P}$ и $\overline{P}$ и удвоенное значение предыдущего частичного остатка $2r_{i-1}$, а на входы младших разрядов сумматоров PRF1 подается уровень +1. Поскольку во время действия сигнала START $2r_{i-1}=0$ и если $b_{N-1}=1$, то на входы PRF1 подается $C_0=A\cdot b_{N-1}=A$. Так как значение C_0 при этом меньше 2P и P, то на выходе PRF1 формируется $r_0=A$. Далее со сдвигом на один разряд в сторону старшего разряда r_0 передается на входы PRF2. На другие входы подаются $A\cdot b_{N-2}$ и значение $2\overline{P}$, $\overline{P}$ и +1. В PRF2 выполняется операция по формированию $r_i=(2r_0+A\cdot b_{N-2})\text{mod}P$, который запоминается в регистре RgPRF2. Таким образом, за время действия сигнала START формируется частичный остаток r_0, затем формирователем PRF2 вычисляется частичный остаток r_1, который запоминается в регистре RgPRF2. После окончания формирования r_1 сигнал START с выхода элемента задержки DL.1 подается на единичный вход триггера T и переводит его в состояние «1», что разрешает прохождение первого импульса Clock.1 на выход схемы И1, который осуществляет сдвиг RgB на два разряда влево. После сдвига в старших разрядах фиксируются значения b_{N-3} и b_{N-4}, которые подаются, соответственно, на входы блоков схем И6 и И7. Импульс Clock.1 подается на счетчик Count, уменьшая его значение на единицу.

Сигнал Clock.1, задержанный на DL.2 на время сдвига регистра RgB, подается на управляющий вход блока схем И8, на информационные входы схем И8 подано значение r_1, сдвинутое на один разряд влево. Под действием импульса Clock.1 значение с выхода блока схем И8 подается на входы PRF1, на другие входы подаются значения $A\cdot b_{N-3}$ и $2\overline{P}$ и $\overline{P}$. На выходе PRF1 формируется частичный остаток $r_2=(2r_1+A\cdot b_{N-3})\text{mod}P$.

Далее частичный остаток со сдвигом на один разряд влево подается на вход PRF2, а на другие входы подаются $A\cdot b_{N-4}$, $2\overline{P}$ и $\overline{P}$. На выходах PRF2 формируется частичный остаток $r_3=(2r_2+A\cdot b_{N-4})\text{mod}P$. Значение r_3 запоминается в регистре RgPRF2.

Аналогично формируется частичный остаток r_4 и r_5 под воздействием следующего импульса Clock.2. После подачи последнего тактового сигнала регистр RgB сдвигается на 2 разряда влево и в старших разрядах фиксируются b_1 и b_0. Формирователи PRF1 и PRF2 вырабатывают частичные остатки r_{N-2} и r_{N-1}. Частичный остаток r_{N-1} фиксируется в регистре RgPRF2. Сигнал «Конец операций», с задержкой на элементе DL.3 на время

формирования остатка r_{N-2} и r_{N-1}, подается на вход блока схем И9 и выдает r_{N-1} как результат.

Рассмотрим пример умножения чисел по модулю с анализом двух старших разрядов множителя за шаг.

Множимое $A=22_{10}$, множитель $B=39_{10}=100111_2$, модуль $P=45_{10}$, $2P=90_{10}$.

В таблице 3 приведена последовательность выполнения операций, где для наглядности все вычисления производятся в десятичной системе счисления.

Проверка: (A·B) mod45=858 mod45=3.

Таблица 3. Последовательность выполнения операций

	START	*Clock.1*	*Clock.2*
b_i, b_{i-1}	$b_5=1, b_4=0$	$b_3=0, b_2=1$	$b_1=1, b_0=1$
PRF1	$r_0=(0+A\cdot b_5)\ modP = =22\ mod45=22$	$r_2=(2r_1+A\cdot b_3)\ modP = =88\ mod45=43$	$r_4=(2r_3+A\cdot b_1)\ modP= =(36+22)\ mod45=13$
PRF2	$r_1=(2\cdot r_0+A\cdot b_2)\ modP = =44 mod45=44$	$r_3=(2\cdot 43+A\cdot b_2)\ modP = =108-2P=108-90=18$	$r_5=(2\cdot r_4+22\cdot b_0)\ modP= =48\ mod45=3$
RgPRF2	$r_1=44$	$r_3=18$	$r_5=3$

Выводы. Быстродействие разработанного умножителя определяется быстродействием используемых схем. В рассматриваемом умножителе в процессе вычислений используются комбинационные схемы, которые, как известно, отличаются высоким быстродействием по сравнению с последовательностными схемами, независимо от метода синтеза, базиса и архитектуры реализации. Анализ выполнения операции умножения по модулю показывает, что при разрядности множителя N, количество требуемых для умножения тактовых импульсов K=(N/2) -1.

Представленные результаты были получены в ходе проведения научных исследований в рамках выполнения государственного заказа на реализацию научной программы по бюджетной программе «Развитие науки», подпрограмме «Программно-целевое финансирование субъектов научной и/или научно-технической деятельности», по научно-технической программе: BR053236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения».

Литература

1. Kalimoldayev, M., Tynymbaev, S., Magzom, M., Ibraimov, M., Khokhlov, S., Abisheva, A., Sydorenko, V. Polynomials Multiplier under Irreducible Polynomial Module for High-Performance Cryptographic Hardware Tools / M. Kalimoldayev // Proceedings of 15th International Conference on ICT in Education, Research and Industrial Applications Integration, Harmonization and Knowledge Transfer. Volume II: Workshops Kherson, Ukraine, June 12-15, 2019. - P. 729-737.

2. Aitkhozhayeva, Y. Zh., Tynymbayev, S., Seilova, N. A., Tereikovska, L. A., Imanbayev, A. Zh. Method and Devices for Modulus Reduction / Y. Zh. Aitkhozhayeva // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. - Алматы: Наука, 2019. - Vol. 378, N. 2 - P. 220-225.

КЛИЕНТ-СЕРВЕРНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Усатова О.А.
e-mail: uoa-olga@mail.ru
Институт информационных и вычислительных технологий КН МОН РК
Казахский Национальный Университет им. аль-Фараби,
Казахстан

Аннотация. *Предлагается система двухфакторной аутентификации для контроля целостности данных, хранящихся в базе данных информационной системы. В данной работе предложен алгоритм и программная реализация метода двухфакторной аутентификации на основе программы - аутентификатора и мобильного приложения.*

В настоящее время Интернет превратился в основной метод связи нашей современной жизни. Интернет является основным инструментом для осуществления покупки и других финансовых операций. Появление этих технологий создало сопутствующей спрос на методы аутентификации, основанные не только на традиционных криптографических способах (шифрование, хеширование, цифровая подпись), но и методах, основанныхна использовании нескольких факторов обеспечения подлинности. Двухфакторная система безопасности базируется на том, что пользователь, кроме пароля доступа к определенному имени пользователя – логину, владеет и инструментом для получения соответствующего ему ключа доступа. Последним может служить сохраненный на компьютере электронный ключ безопасности либо пришедший на личный телефон СМС с кодом подтверждения, а так же биометрические данные, снятые при помощи считывающих электронных устройств. Механизмы двухфакторной аутентификации используют два независимых канала передачи конфиденциальных данных, соединенные данные позволяют сгенерировать аутентификатор и подтвердить личность уполномоченного пользователя.

Типичным примером двухфакторной аутентификации является работа банковских систем. При успешном вводе логина и пароля для доступа запрашивается второй фактор аутентификации - код подтверждения, который приходит на личный телефон в виде СМС либо при помощи сканирования биометрических данных.

Сегодня существует большая проблема с обеспечением безопасности информационных систем. Пользователи используют легкие пароли и переиспользуют их на других ресурсах [1]. Метод двухфакторной защиты работает в информационных системах аналогично работе банковской системы. Возможно использование логина и пароля для доступа к онлайн аккаунтам. Однако, после успешного ввода пароля, информационная система не предоставляет доступ к вашей учётной записи, а запрашивает второй фактор аутентификации, проверочный код. В основе механизмов обеспечения криптостойкости формируемого аутентификатора в протоколах двухфакторной аутентификации, как правило, используются криптографические алгоритмы формирования псевдослучайных последовательностей [2].

Существующие системы аутентификации базируются на предъявлении пользователем компьютеру статической пары идентификатор/пароль. Однако в таком случае пары могут быть скомпрометированы из-за халатности пользователей или

возможности подбора паролей злоумышленником. Значительные интервалы времени, в течение которых пароль и идентификатор остаются неизменными, позволяют применить различные методы их перехвата и подбора. Для повышения защищенности информационной системы администраторы ограничивают срок действия паролей, но в типичном случае этот срок составляет недели и месяцы, что вполне достаточно для злоумышленника. Радикальным решением является применение двухфакторной аутентификации, когда система просит пользователя предоставить одноразовый код подтверждения с коротким сроком действия.

Целью работы является разработка системы защиты информации для обеспечения целостности электронных документов при их хранении и обмене в базах данных информационных систем с использованием аутентификации пользователя на основе второго фактора.

Новизна предложенной системы заключается в разработке модифицированного алгоритма формирования одноразового кода, реализованного при помощи программы-аутентификатора и мобильного телефона [3]. В данном алгоритме формирования используется хэш-функция, основанная на входных данных, таких как логин, пароль, текущий момент времени/дата и секретное слово. Секретное слово не формируется пользователем, оно случайным образом генерируется из массива символов. Для реализации этого алгоритма используется хэш функция SHA256. После формирования хэш-функции на основании ее значения определяются индексы тригонометрической функции и переменные из соответствующего блока, которые выбранная функция будет использовать для расчета результата. Из результата выполнения функции формируется одноразовый код, который отображается только в мобильном приложении пользователя, привязанном к логину on-line системы. Для успешной авторизации в системе пользователю необходимо ввести полученный одноразовый код после попытки авторизации с корректными данными по запросу.

Для реализации рассмотренного алгоритма разработана система, состоящая из трех компонент [4]:

– Пользователь, выполняющий взаимодействие с сервером и мобильным приложением;
– Мобильное приложение, являющееся аутентификатором;
– Серверная часть, взаимодействующаяс клиентом и мобильным приложением.

Внешняя архитектура системы представлена на рисунке 1.

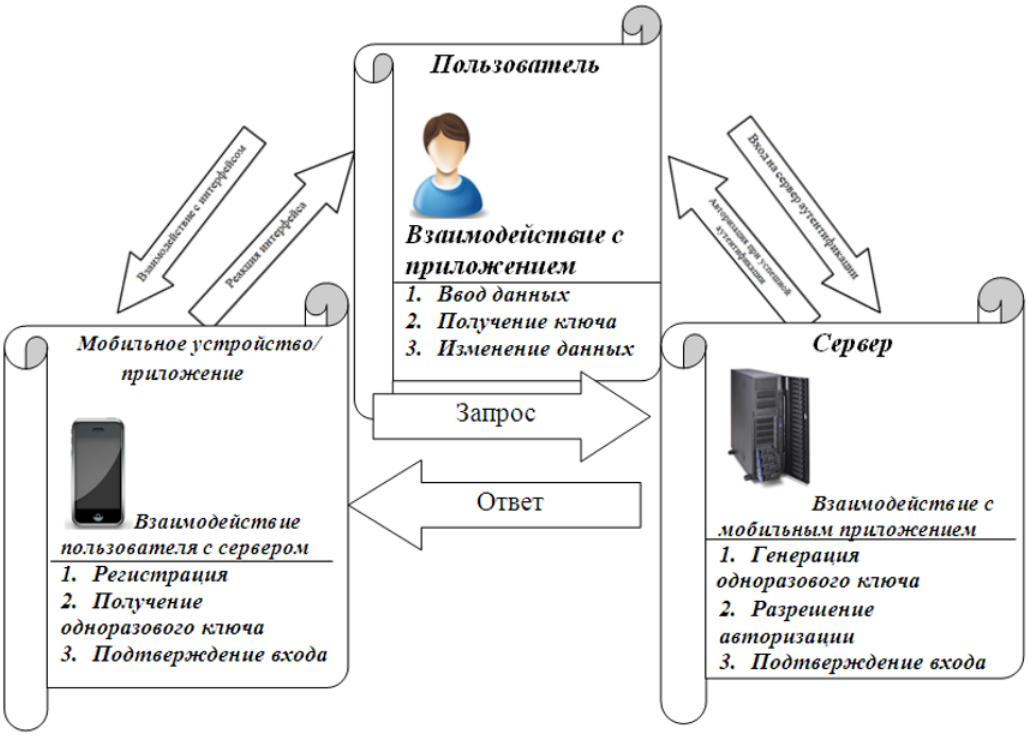


Рис.1 – Внешняя архитектура системы

Пользователь при входе в информационную систему должен пройти регистрацию для осуществления дальнейшего взаимодействия с сервисом. При регистрации необходимо создать логин и пароль, пароль желательно создать сильный, следуя рекомендуемым стандартам.

При входе в информационную систему пользователь авторизуется, вводя свои учетные данные и одноразовый пароль. Для получения одноразового пароля пользователь должен иметь мобильный телефон и установленное на него приложение.

Мобильное приложение – клиентская часть защиты информационной системы с использованием двухфакторной аутентификации. Оно позволяет взаимодействовать пользователю с системой путем регистрации собственных информационных ресурсов или выбора одного из доступных и генерации одноразового временного пароля для входа.

Мобильное приложение состоит из следующих основных файлов:

– App.js – начальный файл, в котором происходит настройка маршрутизации приложения;

– AccountScreen.js – страница авторизованного профиля подключенного информационного ресурса. Из этой страницы открывается доступ к просмотру APIсерверной части разработанной системы;

– UserAccountScreen.js – страница авторизированного аккаунта пользователя, из которой открывается доступ к выбору подключенных ресурсов и генерации секретного кода;

– ConnectScreen.js – страница подключения информационного ресурса к своему аккаунту;

– CreateCode.js – страница для осуществления генерации временного пароля и его отображения пользователю;

– LoginScreen.js – страница авторизации профиля подключенного информационного ресурса;

– UserLoginScreent.js – станица авторизации пользовательского аккаунта;

– MainScreen.js – начальная страница с навигационными кнопками;

– RegistrationScreen.js – страница для осуществления регистрации профиля и подключения информационного ресурса;

– UserRegistrationScreen.js – страница регистрации пользовательского аккаунта;

– ResourcesListScreen.js – страница, содержащая список доступных информационных ресурсов, в которых осуществлена защищенная авторизация с помощью разработанной системы двухфакторной аутентификации. С этой страницы при выборе одного из ресурсов открывается доступ к странице генерации одноразового пароля.

Для реализации мобильного приложения используются фреймворки и библиотеки:

– React – фреймворк для разработки клиентской части webприложений;

– Expo – клиентская оболочка, позволяющая проводить компиляцию кода написанного на ReactNative в полноценной мобильное приложение. Также используется для отладки программы во время разработки;

– ReactNative–фреймворк для разработки мобильного приложения на основе JavaScript коде с использованием фреймворка React;

– Axios – подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером.

Серверная часть является основополагающим модулем в работе проекта. В ней реализован алгоритм генерации временного пароля для осуществления защищенного входа в подключенные информационные ресурсы. Для безопасного хранения информации используется алгоритм защиты баз данных base64 и стандартные средства защиты, такие как подключение к базе данных с помощью логина и пароля администратора.

Серверная часть состоит из следующих файлов:

– index.js – основной файл, в котором происходит подключение базы данных, настройка сессий и обработка защищенного входа для подключенных информационных ресурсов;

– generators.js – файл, содержащий генератор слов и генератор тригонометрических функций.

Используемые фреймворки и библиотеки для реализации серверной части:

– Express – фреймворк для Node.js, упрощающий ведение разработки;

– Mongo-db – библиотека для подключения MongoDB;

– Nodemon – библиотека, позволяющая следить за обновлениями кода и перезагружать сервер после появления таковых;

– Request и Request-promise – библиотеки, осуществляют отправку запросов напрямую с сервера на сервер.

– Crypto-js – данная библиотека позволяет использовать модуль шифрации SHA 256;

– Body-parser – библиотека, позволяющая обрабатывать данные, приходящие на сервер в виде POST-запросов.

Программная реализация рассмотренного алгоритма и архитектуры системы представлена на рисунке 2.

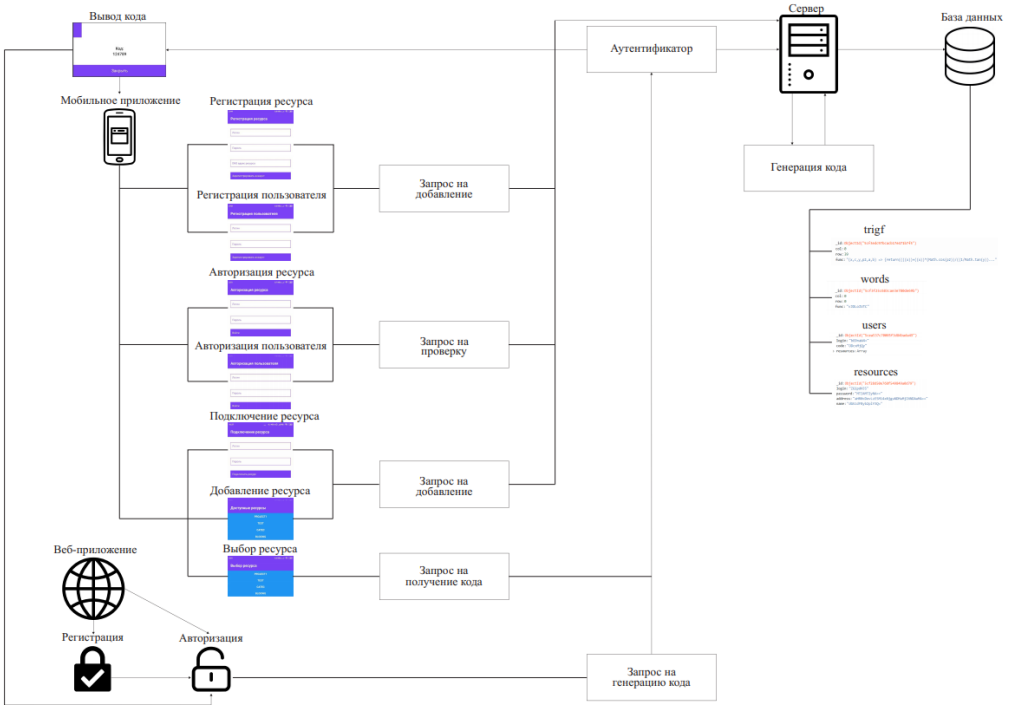


Рис. 2– Модель защиты информационных систем на основе предложенной двухфакторной аутентификации

Для запуска мобильного приложения необходимо выполнить следующие действия:

– установить приложение на телефон с помощью установочного apk файла;

– запустить приложение.

Данный алгоритм реализуется на стороне сервера. Со стороны клиента необходимо лишь взаимодействие с API приложением. Для реализации клиентской части приложения была выбрана платформа для разработки мобильных приложений – ReactNative. Она позволяет использовать ряд веб-технологий, привычных для разработки веб-приложений и ставит расчет на использование компонентов для написания универсальных мобильных приложений.

Разработанная система двухфакторной аутентификации соответствует всем требованиям надежности для обеспечения целостности хранящихся данных. Новизна разработанной системы двухфакторной аутентификации основана на генерации и последующем обновлении блоков тригонометрических функций и секретных слов, реализованных на стороне сервера.

Проведенные исследования показывают, что использование метода двухфакторной аутентификации на основе программы - аутентификатора и мобильного приложения является оптимальным решением.

Использование описанной системы имеет ряд преимуществ, таких как:

- отсутствие необходимости в использовании SMS-сервиса;

- нужно только соединение с сервером, чтобы открыть сессию;
- экономия времени и денег;
- не требуется дополнительных ресурсов или затрат на обслуживание.

Многие компании отказываются от использования SMS для обработки второго фактора из-за небезопасности данного метода. Сотовые сети используют «SignalSystem 7» для взаимодействия между собой. Но в этой системе обнаружены серьезные уязвимости, позволяющие перехватывать входящие вызовы и SMS абонентов.

Предложенная система идентификации пользователя на основе двухфакторной аутентификации для защиты информации разработана и находится на стадии тестирования.

Литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Комплексное противодействие атакам на информационные ресурсы.– М.: АСТ, 2016- 87с.
2. Аутентификация – значение https://sendpulse.com/ru/support/glossary/ authentication (Дата обращения 10.09.2019).
3. S. Nyssanbayeva, W. Wojcik, O. Ussatova «Algorithm for generating temporary password based on the two- factor authentication model» // Przegląd Elektrotechniczny, Poland, № 5, 2019 г.,ISSN 0033-2097, R. 95, - P. 101 – 106.
4. O. Ussatova, S. Nyssanbayeva, W. Wojcik «Two-factor authentication algorithm implementation with additional security parameter based on mobile application» // International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019), Guilin, China, 2019. - P.–84-86.

АНАЛИЗ НОВОСТНЫХ ТЕМАТИЧЕСКИХ ТРЕНДОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Якунин К., Красовицкий А.М., Уалиева И.М., Мейрамбеккызы Ж., Мусабаев Р.Р.
e-mail: rmusab@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Рассмотрен метод автоматизированного текстового анализа динамики современных новостных трендов в сфере информационной безопасности на основе вероятностного тематического моделирования. Выявлены наиболее обсуждаемые в социуме тренды в сфере ИБ, проведен прогноз резонансности и продолжительности темы.*

Введение

Сфера информационной безопасности (ИБ) стремительно и бурно развивается в соответствии с потребностями современного общества. Появление новых технологий и систем – это одна из сторон информатизации и глобализации в стране. Поэтому отслеживание актуальных, динамически изменяющихся трендов в сфере ИБ является

важной и востребованной задачей для широкого круга заинтересованных лиц. Отслеживание ключевых нововведений и изменений в данной сфере может служить для повышения конкурентоспособности многих субъектов, напрямую или косвенно связанных с ИБ, а также других видов деятельности связанных с принятием стратегических решений. Привлечение *автоматических* средств для анализа динамики современных тематических трендов ИБ позволяет не только открывать скрытые закономерности в данных, ускорить процесс анализа огромного потока информации (больших данных), но также вывести аналитику, связанную с актуальными трендами на качественно новый уровень.

Публикации в открытых СМИ служат “лакмусовой бумагой” для представления текущих трендов медиа пространства и интересов социума. Новости затрагивают злободневные события в мире информационных технологий, некоторые из которых имеют резонансный характер. В литературе [1] представлены методы выявления угроз ИБ, основанные на анализе новостных ресурсов. Здесь, как и во многих аналогичных работах, используется метод вероятностного тематического моделирования (ТМ) для извлечения информации из неструктурированных и слабо структурированных текстовых данных [2]. Существуют методы, на основе ТМ, которые используются для поиска конкретных событий, либо инфоповодов. При помощи ТМ также было возможно провести сравнительный анализ активности мировых трендов в отношении ИБ по значительным временным промежуткам [3]. В статье [4] собраны результаты анализа трендов 15-ти европейских стран по материалам корпоративных отчетов, затрагивающих социально-экономические вопросы. При помощи ТМ ищут ответы на вопросы: 'какие тематики наиболее часто появляются в заголовках', 'что изменилось (со временем)', 'какие различия для разных секторов (экономики)'. Ответы на данные вопросы позволяют провести сравнительный анализ (временной, региональный, относительный) для любого отдельно взятого тренда. ТМ на текстовой технической информации был использован для автоматизированного анализа уязвимости программного обеспечения и выявления трендов ИБ [5].

Нами предлагается комплексный подход ТМ для выявления динамики активности тем (и, в частном случае, интересуемых трендов) в среде ИБ с учетом тональности для русскоязычного медиапространства Казахстана. Объектом нашего исследования является новостной корпус СМИ РК, глубиной два года. Были использованы только текстовые материалы находящийся в открытом доступе. Инструментами для данного анализа послужили программные библиотеки для ТМ больших текстовых данных BigARTM [6]. Данная система представляет собой комплекс оптимизационных методов вероятностного тематического моделирования на основе аддитивной регуляризации [7,8]. Это, в свою очередь, позволяет применять методы автоматизированного текстового анализа динамики современных трендов в сфере ИБ.

Тематическое моделирование

Используется понятие *темы* как базовой единицы в ТМ. Каждая тематика определяется своим словарем, т.е. конечным множеством слов, полученных из исходного текстового корпуса. При этом часть тем является фоновыми, т.е. с большой вероятностью присутствуют во всех текстах, либо скрытыми, т.е. теми, которые не имеет явного осмысленного значения. Тематическое моделирование – это процесс с одной стороны определения тем, а с другой определения принадлежности текстов к данной теме.

Наиболее известным инструментом ТМ является латентное размещение Дирихле (LDA) [1]. Нами используется программный инструментарий BigARTM в основе которого лежит аддитивная регуляризация тематических моделей, более общая модель чем LDA, однако требующая дополнительной настройки параметров. Проводимые настройки данной системы приняты близкими к настройкам по умолчанию, с изменениями, направленными на максимизацию разреженности тем [8].

Для анализа значимости и адекватности тем были привлечены асессоры для разметки и ранжирования тем по соответствии области ИБ. Заметим, что данная разметка необходима для проведения только один раз. Это сделано для минимального вовлечения человеческого фактора в процесс выделения тем.

Нами проводилось двойное ТМ. Сначала выделялись темы, имеющие прямое отношение к информационным технологиям. Затем проводилось повторное ТМ уже для новостей, относящихся к ИБ.

Корпус

Для тематического моделировании использовался открытый новостной корпус СМИ РК глубиной до двух лет. Общее число публикаций для построения тематической модели составляет около 645 тыс публикаций, с заданием числа тем равным 200. Из них отобраны семь тем верхнего уровня Таблица 1 для проведения повторного ТМ в области ИБ. На этом этапе получено 25 тем (ТМ второго уровня) Таблица 2 для сферы ИБ. Далее анализ ТМ проводится только на данных 25 темах. Каждая публикация содержит название источника публикации, ссылку на источник, заголовок публикации, имена авторов (при наличии), дату публикации и непосредственно текст. Каждой публикации присвоен свой идентификатор. Все документы представлены в формате json.

На этапе предварительной обработки из текстов были удалены стоп-слова, URL-адреса, редко встречаемые слова, проведена лемматизация текста.

Результаты

Ниже приведены результаты ТМ. Представлены иерархические двухуровневые темы: семь тем верхнего уровня (из двухсот для информационных технологий) в Таблице 1; двадцать пять тем второго уровня с позитивной и негативной тональностью Таблицы 2-4 выделенные непосредственно для анализа ИБ.

Таблица 1. Темы верхнего уровня всей сферы информационных технологий.

	Тема	**Мощность**	**Удельный вес**
1	Услуга, Электронный, Гражданин, Портал, Правительство	4588	0,955
2	Информация, Telegram, Сайт, Сертификат, Мессенджер	3005	0,604
3	Безопасность, Казахстан, Узбекистан, Страна, Республика	2489	0,449
4	Цифровой, Еаэс, Евразийский, Союз, Страна	2154	0,404
5	Криптовалюта, Блокчейн, Валюта, Атака, Биткоин	1373	0,262
6	Право, Закон, Власть, Вопрос, Правительство	1485	0,236
7	Технология, Информация, Использование, Система, Корея	617	0,086

1 тема включает в себя следующие темы: «Услуга, Электронный, Гражданин, Портал, Правительство». В данной группе преобладает темы цифровизации, портал eGov.kz, адресные справки, цифровой и миграционный ЦОНы, т.е. темы, не относящиеся к информационной безопасности напрямую, но входят в сферу информационных

технологий. Как видно на Рис.1, данные темы отражаются в СМИ в основном касательно Казахстана

2 тема «Информация, Telegram, Сайт, Сертификат, Мессенджер» В данной группе собраны новости, которые описывают события блокировки Telegram в России. Основные новости относятся к информационной безопасности России, упоминается также Иран, где также был заблокирован Telegram. Примеры заголовков новостей: *Суд заблокировал Telegram в России, Павел Дуров не собирается отдавать ключи шифрования Федеральной службе* безопасности России. Встречаются новости, касающиеся сертификата безопасности, к примеру, *О блокировке казахстанского "сертификата безопасности" в Safari заявила Apple.* Из всех 7 тем, данная тема больше всего относится к сектору ИБ.

3 тема «Безопасность, Казахстан, Узбекистан, Страна, Республика». В данной группе новостей в основном тема военной безопасности, армии ОДКБ. Практически отсутствуют новости об информационной безопасности. На графике Казахстан отражен выше, чем другие страны.

4 тема «Цифровой, Еаэс, Евразийский, Союз, Страна». Как видно на графике Казахстан и другие страны примерно на одном уровне, поскольку темы новостей в данной группе в основном относятся к евразийскому союзу, цифровизации в странах-участников. Однако новости касательно именно информационной безопасности практически не встречаются.

5 тема «Криптовалюта, Блокчейн, Валюта, Атака, Биткоин». Основные новости касаются криптовалюты, блокчейна, без относительной связи со странами. К примеру, новость *PayPal разрабатывает систему криптоплатежей* безотносительна к странам в целом. Как видно на графике, в СМИ по данной теме события в Казахстане отражаются меньше, чем в других странах.

6 тема «Право, Закон, Власть, Вопрос, Правительство». В данной группе преобладают новости, относящиеся к Казахстану и практически нет новостей касательно информационной безопасности.

7 тема «Технология, Информация, Использование, Система, Корея» Данная тема является обширной областью, в которой встречаются самые разные события в информационных технологиях.

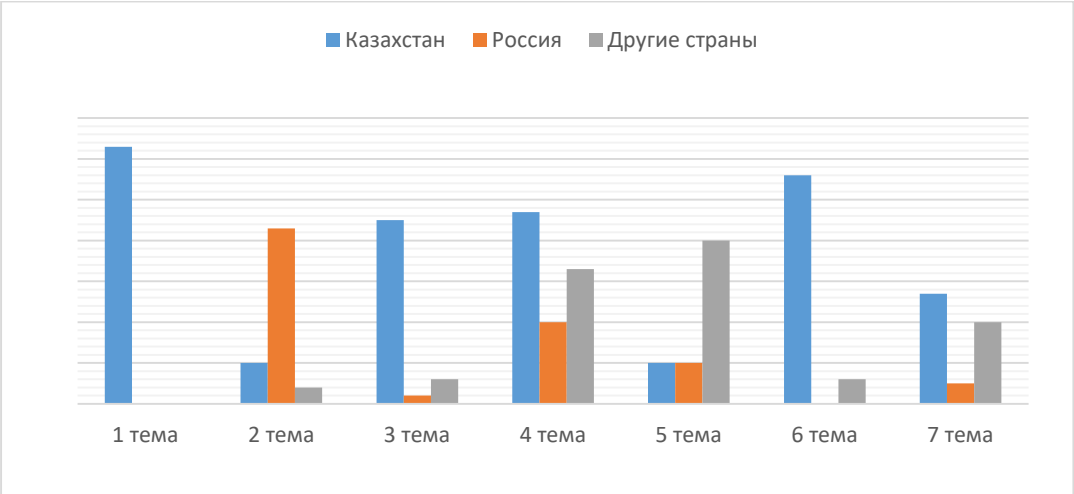


Рис.1. Объем новости ИБ для Казахстанского сектора. К группе других стран относятся только те, которые встречаются в корпусе новостей. Основные страны: Узбекистан, Иран, Южная Корея, Китай.

Таблица 2. Три темы ИБ с наибольшим удельным весом ТМ второго уровня.

Тема	**Топ 25 слов**	**Мощность**	**Удельный вес**
Казахстан, Информационный, Безопасность, Национальный, Страна	Казахстан (1,00); Информационный (0,69); Безопасность (0,63); Национальный (0,42); Страна (0,42); Государственный (0,37); Республика (0,36); Министерство (0,36); Развитие (0,27); Работа (0,27); Технология (0,26); Интернет (0,23); Система (0,23); Международный (0,22); Кибербезопасность (0,21); Сайт (0,21); Сфера (0,19); Центр (0,18); Цифровой (0,17); Место (0,16); Комитет (0,16); Промышленность (0,16); Обеспечение (0,16); Организация (0,15); Правительство (0,15);	727	1,000
Telegram, Мессенджер, Россия, Блокировка, Роскомнадзор	Telegram (1,00); Мессенджер (0,65); Россия (0,39); Блокировка (0,39); Роскомнадзор (0,36); Суд (0,36); Пользователь (0,27); Дуров (0,26); Компания (0,24); Решение (0,23); Апрель (0,22); Фсб (0,21); Российский (0,19); Сервис (0,19); Доступ (0,19); Заблокировать (0,19); Павел (0,18); Ключ (0,17); Иран (0,16); Сообщение (0,15); Иск (0,15); Требование (0,14); Переписка (0,13); Заявить (0,12); Сайт (0,11);	592	0,900
Казахстан, Информация, Доступ, Блокировка, Материал	Казахстан (1,00); Информация (0,38); Доступ (0,38); Блокировка (0,36); Материал (0,36); Сайт (0,35); Sputnik (0,31); Двк (0,29); Мессенджер (0,28); Министерство (0,28); Территория (0,26); Telegram (0,26); Запретить (0,25); Заблокировать (0,24); Ресурс (0,23); Администрация (0,23); Коммуникация (0,23); Пользователь (0,22); Республика (0,22); Экстремистский (0,21); Сеть (0,20); Решение (0,20); Группа (0,20); Сообщить (0,19); Абай (0,17);	487	0,762

Таблица 3. Темы с позитивной тональностью

№	**Тема**	**Вес**	**Прогнозируемая резонансность**	**Прогнозируемая продолжительность в днях**	**Фаза роста**
П1	Казахстан, информационный, безопасность, национальный, страна	1,000	**0,768**	106,8	0,111
П2	Безопасность, информационный, обеспечение, требование, государство	0,624	*	*	*
П3	Безопасность, доступ, сертификат, персональный	0,373	**2,553**	127	**-2,226**

П4	Система, электронный, образование, школа	0,335	-0,577	123	0,740
П5	Сертификат, пользователь, безопасность, whatsapp, сообщение	0,264	**1,220**	160	**1,580**
П6	Доллар, компания, facebook, криптовалюта, сша	0,261	-0,035	91,3	0,465
П7	Компания, страна, безопасность, технология, цифровой	0,239	-0,598	61,4	0,471
П8	Система, казахстан, товар, продукция, министерство	0,179	*	*	*
П9	Комитет, вопрос, новость, информация, facebook	0,176	-0,653	85,3	**-4,578**

* - обозначены темы, о которых регулярно пишут в публикациях новостных сайтов

Таблица 4. Темы с негативной тональностью

№	**Тема**	**Вес**	**Прогнозируемая резонансность**	**Прогнозируемая продолжительность в днях**	**Фаза роста**
Н1	Пользователь, приложение, устройство, атака, компания	1,000	-0,036	85,7 дней (Score: -0,508)	**-6,552**
Н2	Telegram, мессенджер, россия, блокировка, роскомнадзор	0,948	**3,149**	98,5 дней (Score: 0,000)	0,166
Н3	Информация, сообщение, распространять	0,875	**1,120**	106,5 дней (Score: 0,317)	0,280
Н4	Информация, сеть, суд, уголовный, статья	0,694	0,133	109,3 дней (Score: 0,426)	0,908
Н5	Сайт, сеть, суд, фото, материал	0,669	-0,417	104,8 дней (Score: 0,247)	2,802
Н6	Сеть, социальный, facebook, интернет, выбор	0,552	0,000	67,8 дней (Score: -1,215)	**-15,823**
Н7	Казахстан, информация, доступ, блокировка, материал	0,504	0,851	72,0 дней (Score: -1,049)	**-3,314**
Н8	Компания, google, информация, сотрудник	0,407	0,577	78,3 дней (Score: -0,802)	**-4,363**
Н9	Информация, закон, министерство, орган	0,371	-0,257	**141,7 дней (Score: 1,709)**	0,243
Н10	Атака, безопасность, казахстан, информационный, компания	0,347	0,642	**118,3 дней (Score: 0,785)**	**-1,826**

Показательные характеристики для каждой темы определены как резонансность, продолжительность и фаза роста.

Вес показывает частоту появления публикаций, принадлежащих к заданной теме на новостных порталах в заданный период времени. Прогнозируемая резонансность показывает прогноз степени интереса СМИ к публикациям определенной темы. Как

долго публикация темы будет еще обсуждаться в СМИ, показывает прогнозируемая продолжительность темы. Фаза роста показывает резкие, монотонные нарастающие либо убывающие темы. Иными словами фаза — это то, куда направлены рост либо падение веса.

Для расчета резонансности и продолжительности для каждой темы вычислялось статистическое распределение пиков максимальной активности по времени. Иными словами, для временной последовательности весов данной темы выделены все локальные максимумы. Затем их отношения к среднеквадратичному отклонению данного распределения рассматривались как показатели соответствующих характеристик.

Как видно из таблиц, такие крупные компании как *telegram, facebook, whatsapp, google* имеют непосредственное отношение к вопросам информационной безопасности. Публикации, связанные с социальными сетями *facebook* (П9, Н6) и мессенджером *telegram* (Н2), *whatsapp* (П5) наиболее обсуждаемые, с высокой степенью прогнозируемой резонансности и фазами роста или падения. Причем следует отметить, что обсуждение мессенджера *telegram* проходит только в негативной тональности и входит в одну тему со словами *Россия, блокировка, роскомнадзор*. Вопросы национальной безопасности РК (П1) также часто обсуждаемые, вошли в тему публикаций с позитивной тональностью, что говорит о том, что в прессе часто публикуются официальные правительственные отчеты по вопросам информационной безопасности. Еще одна тема с негативной тональностью, это тема блокировки доступа к информации (Н7). Как видно из значения фазы, то интерес к этой теме снижается (фаза роста = -3.314), а прогноз резонансности довольно низкий (0,851). Тема, связанная с сертификатом доступа пользователей (П5), имеет довольно высокий прогнозируемый уровень резонансности, а количество публикаций растет (фаза роста = 1,580). Тема (Н1), в которую вошли слова *приложение, устройство, атака, компания* не резонансная, но часто обсуждаемая, хотя наблюдается резкое снижение публикаций на эту тему (фаза роста= -6,552)

Анализ также показал, что публикации, которые вошли в темы по информационной безопасности носят, в основном, негативный характер Рис 2.

Рис.2. Отношение объемов позитивных и негативных публикаций по темам ИБ за период 2 года. Пунктирная линия позитив, сплошная негатив.

Заключение

Авторы применили ТМ на текстовых неструктурированных данных для автоматического выявления трендов в сфере информационной безопасности. Наши исследования показали возможности использования данного метода для выделения и анализа наиболее востребованных социумом трендов в сфере ИБ.

В дальнейшем предполагаем продолжить исследование в области анализа зависимостей и интерпретации получаемых результатов среди выделенных трендов. А

также представляется интересным провести анализ тематик, которые могут иметь зависимости типа иерархии.

Литература

1. Alghamdi, R., Alfalqi, K. A Survey of Topic Modeling in Text Mining. International Journal of Advanced Computer Science and Applications, 2015. 6. 10.14569/IJACSA.2015.060121.

2. Neuhaus, S., Zimmermann, T. Security Trend Analysis with CVE Topic Models, 2010. 111. 111 - 120. 10.1109/ISSRE.2010.53.

3. Tang, X., Yang, C. TUT: A statistical model for detecting trends, topics and user interests in social media. ACM International Conference Proceeding Series, 2012. 10.1145/2396761.2396884.

4. Goloshchapova, I., Poon, Ser-H. & Pritchard, M., Reed, P. Corporate social responsibility reports: topic analysis and big data approach. The European Journal of Finance, 2019. 1-18. 10.1080/1351847X.2019.1572637.

5. Al Moubayed, N., Wall, D., Mcgough, A. Identifying Changes in the Cybersecurity Threat Landscape Using the LDA-Web Topic Modelling Data Search Engine, 2017. 287-295. 10.1007/978-3-319-58460-7_19.

6. BigARTM: State-of-the-art Topic Modeling. website: https://bigartm.org/ (просмотрен 15.12.2019)

7. Vorontsov, K., Potapenko, A., Plavin, A. Additive Regularization of Topic Models for Topic Selection and Sparse Factorization, 2015, 193-20210.1007/978-3-319-17091-6_14.

8. Vorontsov, K., Potapenko, A. Additive regularization of topic models. Machine Learning, 2014. 101. 1-21. 10.1007/s10994-014-5476-6.

Содержание

МАТЕРИАЛЫ

Международной научно-практической конференции
"Актуальные проблемы информационной безопасности в Казахстане",

15 января 2020, Алматы, Казахстан

Под редакцией М.Н. Калимолдаева

Компьютерная верстка
Шокишалов Ж.М.

Подписано в печать 10.01.2020 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 30,03.
Тираж 100 экз. Заказ № 00331.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125