SECURITY CONTROL SYSTEM FOR INFORMATION EXCHANGE IN TELECOMMUNICATION NETWORKS

Elvin Abaszade[1], Zafar İsmayilov[1], Almaz Mehdiyeva[2], Huseyn Qasimov[3]
•
[1]Azerbaijan Technical University, Huseyn Javid Ave. 25, Az1073, Baku
[2]Azerbaijan State Oil and Industry University, Azadliq Avenue 20, AZ1010, Baku
[3]Nakhchivan State University, University campus, AZ7012, Azerbaijan
elvinabaszadaphd@gmail.com, zafar.ismayilov@aztu.edu.az, almaz.mehdiyeva@asoiu.edu.az,
huseynqasimov@ndu.edu.az

Abstract

The principles of information security and the problems faced were investigated. Cyber security issues are explored. Also, technical requirements for ensuring information security and means ensuring the security of Information systems were studied. Based on Visual Studio and MySQL programs, the issue of web page security and user data protection has been resolved. In this application, Users can access their personal cabinet by typing username and password on the web page. If a user is not registered on this page, then that user will encounter a problem, which means that the database does not have that user's information. The proposed method ensures security.

Keywords: Information security, telecommunication networks, cyber security, MySQL programs, information system, information exchange.

I. Introduction

Information system (IS) is a formal, socio-technical, organizational system designed to collect, process, store and distribute information. From a socio-technical point of view, information systems consist of four components: task, people, structure (or roles), and technology. Information systems can be defined as the integration of components for the collection, storage and processing of data, from which data are used to provide information, contribute to knowledge, as well as digital products that facilitate decision making.

A computer information system is a system consisting of humans and computers that process or interpret information. The term is also sometimes used to refer simply to a computer system on which software is installed.

"Information systems" is also the academic field study of the information-specific systems and complementary networks of computer hardware and software that people and organizations use to collect, filter, process, create, and disseminate information. Emphasis is placed on an information system that has a defined boundary, users, processors, memory, inputs, outputs, and the aforementioned communication networks.

In many organizations, the department or unit responsible for information systems and data processing is known as "information services" [1-5].

Any specific information system aims to support operations, management and decision making. An information system is the information and communication technology (ICT) used by an organization, as well as how people interact with this technology to support business processes [6, 7].

Some authors make a clear distinction between information systems, computer systems and business processes. Information systems usually include an ICT component, but are not concerned with ICT alone, instead focusing on the end use of information technology. Information systems are also different from business processes. Information systems help control the execution of business processes [8, 9].

Alter advocates the advantages of viewing an information system as a specific business system. A work system is a system in which people or machines perform processes and activities using resources to produce specific products or services for customers. An information system is a business system whose activity is dedicated to capturing, transmitting, storing, retrieving, manipulating and displaying information [10-15].

Thus, information systems interact with information systems on the one hand, and activity systems on the other. An information system is a form of communication system in which information is represented and processed as a form of social memory. An information system can also be considered a semi-formal language that supports human decision-making and actions.

Information security, sometimes abbreviated to InfoSec, is the practice of protecting information by reducing information risks. It is part of information risk management. This typically involves preventing or mitigating unauthorized/inappropriate access or illegal use of information, disclosure, disruption, deletion, corruption, alteration, verification, recording or impairment of information. It also includes measures to reduce the negative effects of such events. Protected information can be in any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge)) is balanced protection. This is mainly achieved through a structured risk management process that includes:

identification of information and related assets, plus potential threats, vulnerabilities and impacts;

- risk assessment;
- deciding how to address or treat risks ie. avoid, reduce, share or accept them;
- selecting or designing appropriate security controls and implementing them when risk mitigation is required;
- monitoring activities, making corrections, changes and improvements as necessary to solve any problems.

In order to standardize this discipline, scholars and professionals are working on passwords, antivirus software, firewalls, encryption software, legal liability, security awareness and training, etc. collaborate to offer guidelines, policies, and industry standards for the application of any standards and guidelines within may have limited impact.

The CIA's triad of privacy, integrity, and availability is the foundation of information security. interchangeably.) However, this CIA triad emphasizes the relationship between accessibility and privacy, as well as security and privacy [16, 17]. Debate continues as to whether it is sufficient to meet rapidly changing technology and business requirements, with recommendations to consider scaling up. Sometimes other principles have been proposed, such as “responsibility”; It has been pointed out that issues such as non-denial do not correspond to the three basic concepts. It appears that the triad was mentioned in a 1977 NIST publication [18-22].

In 1992 and revised in 2002, the OECD Guidelines for the Security of Information Systems and Networks proposed nine generally accepted principles: awareness, responsibility, responsiveness, ethics, democracy, risk assessment, security design and implementation, security management and re-evaluation [23]. Based on these, in 2004 NIST's Engineering Principles for Information Technology Security He proposed 33 principles. It is derived from each of these guidelines and practices.

In 1998, Donn Parker proposed an alternative model to the classic CIA triad, which he called the six atomic elements of information. The elements are privacy, ownership, integrity, authenticity, accessibility, and utility. The merits of the Parkerian Hex are a matter of debate among security experts.

II. Technical requirements for ensuring information security

IT security standards or cybersecurity standards are generally methods described in published materials that attempt to protect a user's or organization's cyber environment. This environment includes the users themselves, networks, devices, all software, processes, data in storage or transit, applications, services and systems that can be directly or indirectly connected to networks [24].

The main objective is to reduce risks, including preventing or mitigating cyber-attacks. These published materials include tools, policies, security concepts, security safeguards, guidelines, risk management approaches, measures, training, best practices, security and technologies.

Cybersecurity standards have existed for several decades, as users and providers have collaborated in many domestic and international forums to implement the necessary capabilities, policies, and practices - generally originating in the 1990s with work at the Stanford Consortium for Research on Information Security and Policy.

A 2016 U.S. security framework adoption study reported that 70% of surveyed organizations recognized the NIST Cybersecurity Framework as the most popular best practice for information technology (IT) computer security, but many considered it a significant investment. states that it requires Cross-border, cyber-exfiltration Law enforcement operations against international criminal activities on the dark web raise complex jurisdictional questions that remain to some extent unanswered. Tensions between domestic law enforcement efforts to conduct cross-border cyber-exfiltration operations and international jurisdiction are likely to continue. provides improved cyber security norms. The following subsections detail international standards related to cybersecurity.

III. Principles of building information protection systems

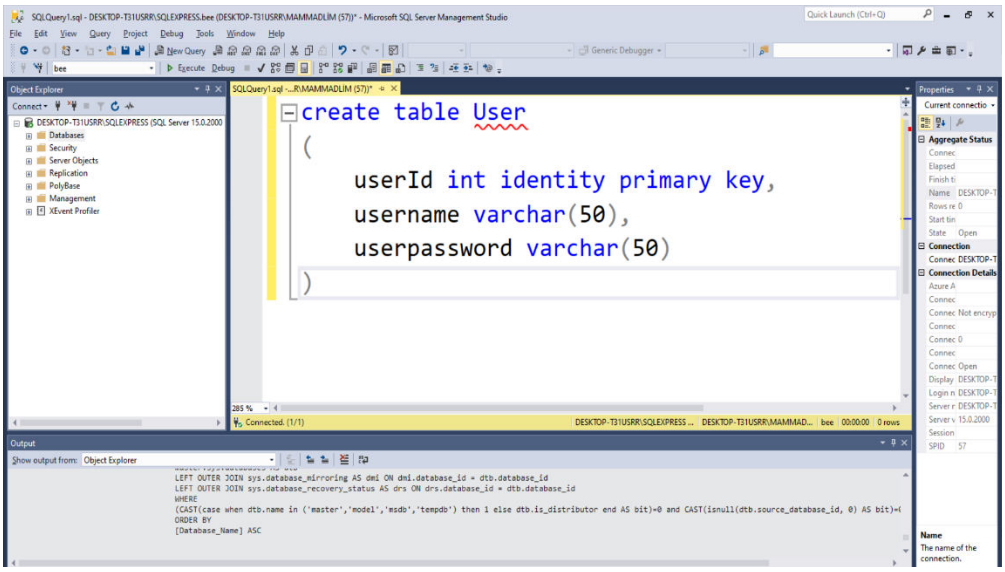
In our modern era, information protection systems are used on web pages. Programs are used to build these systems. Now, for the information protection we will look at, it is required to use visual studio and mysql programs.

Visual Studio IDE (integrated development environment) is software for developers to write and edit their code. Its user interface is used for software development to edit, debug, and build code. Visual Studio includes a code editor that supports IntelliSense (a code completion component), as well as code refactoring. The integrated debugger works as both a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, a designer for building GUI applications, a web designer, a class designer, and a database schema designer [25].

MySQL is a relational database management system (RDBMS) developed by Oracle and based on structured query language (SQL).

A database is a structured collection of data. This can be anything from a simple shopping list to an image gallery or a place to store large amounts of data on a corporate network [26]. Specifically, a relational database is a digital store that collects data and organizes it according to a relational model. In this model, tables consist of rows and columns, and the relationships between data elements all follow a strict logical structure. An RDBMS is simply a set of software tools used to implement, manage, and query such a database [27-29].

A new database is created in MySQL and this database will contain username and userpassword (Figure 1, 2).

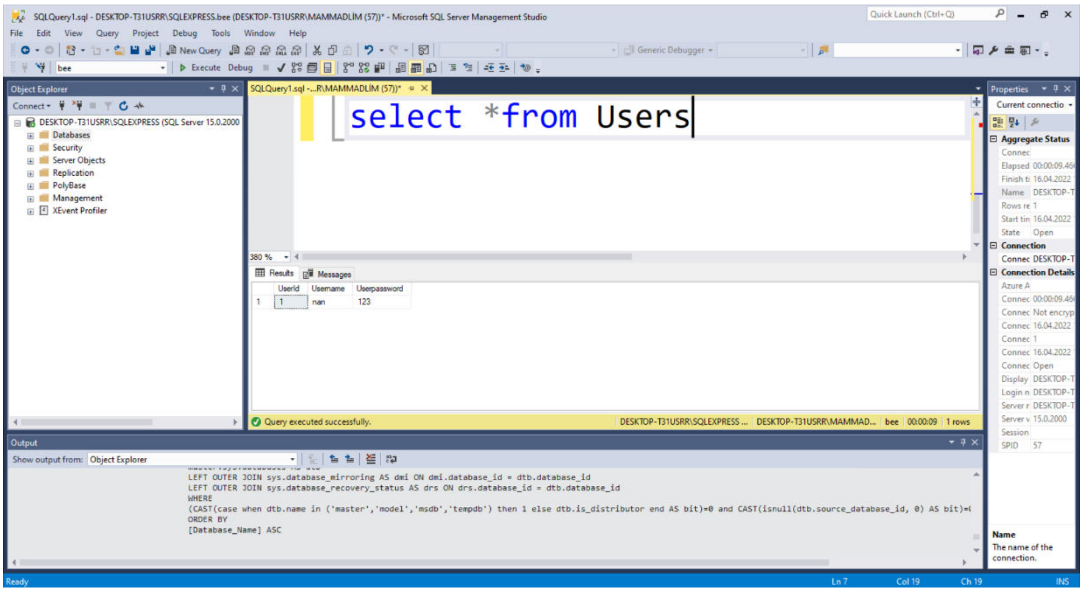


```
create table User
(
    userId int identity primary key,
    username varchar(50),
    userpassword varchar(50)
)
```

Connected. (1/1) | DESKTOP-T31USRR\SQLEXPRESS ... | DESKTOP-T31USRR\MAMMAD... | bee | 00:00:00 | 0 rows

```
LEFT OUTER JOIN sys.database_mirroring AS dmi ON dmi.database_id = dtb.database_id
LEFT OUTER JOIN sys.database_recovery_status AS drs ON drs.database_id = dtb.database_id
WHERE
(CAST(case when dtb.name in ('master','model','msdb','tempdb') then 1 else dtb.is_distributor end AS bit)=0 and CAST(isnull(dtb.source_database_id, 0) AS bit)=(
ORDER BY
[Database_Name] ASC
```

Figure 1: *User data*



```
select *from Users
```

	UserId	Username	Userpassword
1	1	nan	123

Query executed successfully. | DESKTOP-T31USRR\SQLEXPRESS ... | DESKTOP-T31USRR\MAMMAD... | bee | 00:00:09 | 1 rows

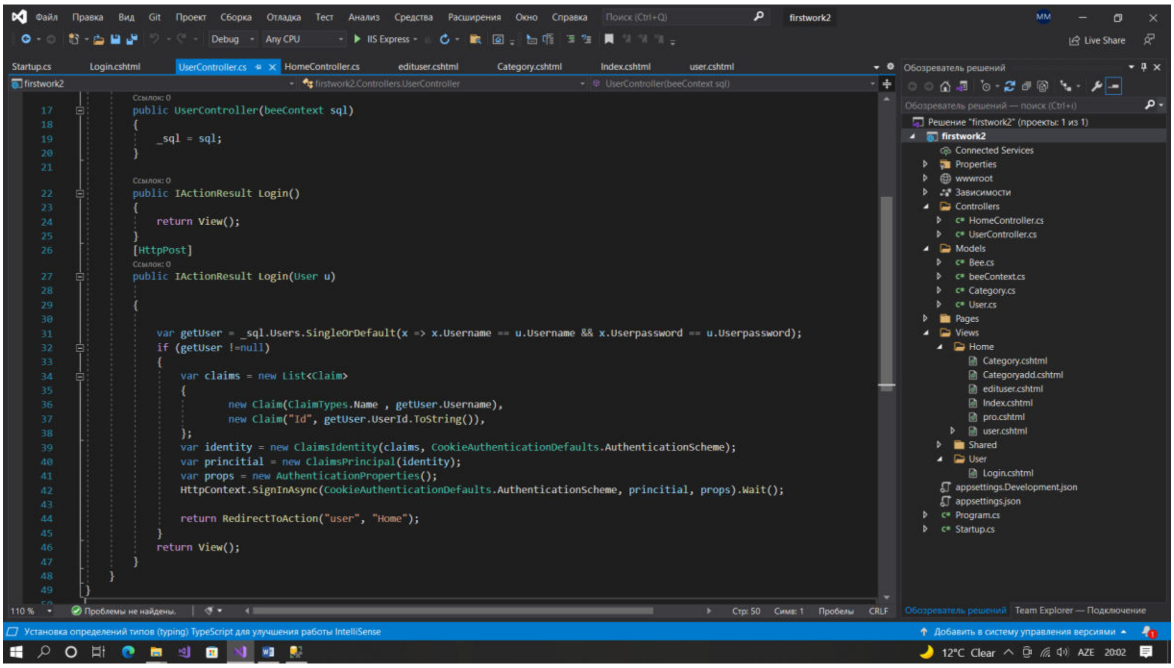
```
LEFT OUTER JOIN sys.database_mirroring AS dmi ON dmi.database_id = dtb.database_id
LEFT OUTER JOIN sys.database_recovery_status AS drs ON drs.database_id = dtb.database_id
WHERE
(CAST(case when dtb.name in ('master','model','msdb','tempdb') then 1 else dtb.is_distributor end AS bit)=0 and CAST(isnull(dtb.source_database_id, 0) AS bit)=(
ORDER BY
[Database_Name] ASC
```

Figure 2: *User table*

At the next stage, we connect with visual studio and create a login in visual studio. With the connection we write in Visual Studio, we can get the information directly from MySQL.

IV. Ensuring security in information exchange

We provide security on web pages through the Visual Studio program and create security walls with the help of special codes. We receive a request from the database we have created under certain conditions, and this request is evaluated by the Visual Studio side. If the request is correct, then the user using our web page is redirected to the desired address, otherwise, if the user's request - user data is incorrect, then he will not be able to access the Web page (Figure 3).

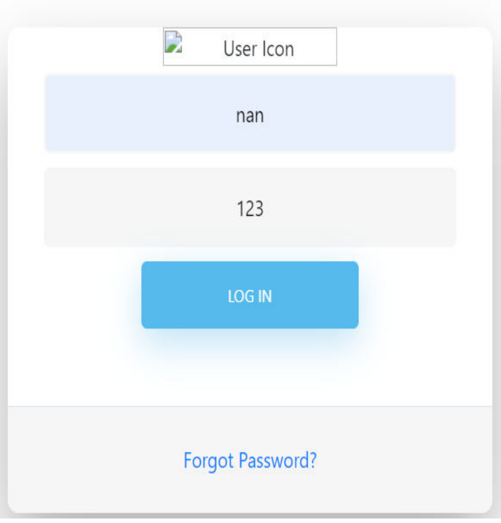


```
public UserController(beeContext sql)
{
    _sql = sql;
}

public IActionResult Login()
{
    return View();
}
[HttpPost]
public IActionResult Login(User u)

{

    var getUser = _sql.Users.SingleOrDefault(x => x.Username == u.Username && x.Userpassword == u.Userpassword);
    if (getUser !=null)
    {
        var claims = new List<Claim>
        {
                new Claim(ClaimTypes.Name , getUser.Username),
                new Claim("Id", getUser.UserId.ToString()),
        };
        var identity = new ClaimsIdentity(claims, CookieAuthenticationDefaults.AuthenticationScheme);
        var principial = new ClaimsPrincipal(identity);
        var props = new AuthenticationProperties();
        HttpContext.SignInAsync(CookieAuthenticationDefaults.AuthenticationScheme, principial, props).Wait();

        return RedirectToAction("user", "Home");
    }
    return View();
}
```

Figure 3: *Security codes*

V. Results and discussion

On our login page (Figure 2), enter your username and password, and enter your username and password for testing. Clicking on the sign in button here will redirect us to the user's personal page.



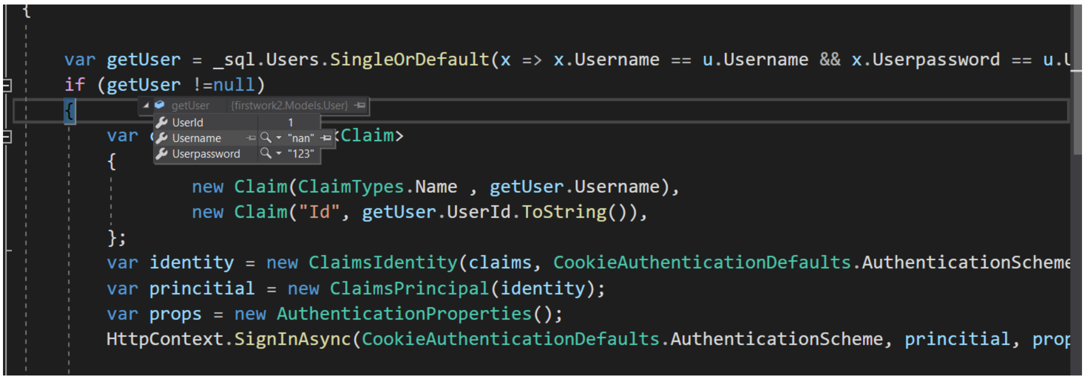
User Icon

nan

123

Figure 4: *Login*

The next stage is related to whether the user sent the information correctly or not. For this, we should look at the getuser code and Figure 5 was shown. The user will be redirected to the correct address as the information is already in the system.



```
{

    var getUser = _sql.Users.SingleOrDefault(x => x.Username == u.Username && x.Userpassword == u.U
    if (getUser !=null)
    {
        var (                 <Claim>
        {
                new Claim(ClaimTypes.Name , getUser.Username),
                new Claim("Id", getUser.UserId.ToString()),
        };
        var identity = new ClaimsIdentity(claims, CookieAuthenticationDefaults.AuthenticationScheme
        var princitial = new ClaimsPrincipal(identity);
        var props = new AuthenticationProperties();
        HttpContext.SignInAsync(CookieAuthenticationDefaults.AuthenticationScheme, princitial, prop
```

```
getUser        {firstwork2.Models.User}
  UserId          1
  Username        "nan"
  Userpassword    "123"
```

Figure 5: *Security check*

VI. Conclusion

The following results were obtained from the conducted research: Security control systems are used in information exchange, and these systems are also used in web pages. Firewalls are created on web pages and attacks are prevented by the software we use. From these pages, there is a registration page for users, and after registration, they can log into their personal accounts with the unique username and password provided to them.

References

[1] Kerstin., Fink (2004). Knowledge Potential Measurement and Uncertainty. Deutscher Universitätsverlag. ISBN 978-3-322-81240-7. OCLC 851734708.

[2] Keyser, Tobias (2018-04-19), "Security policy", The Information Governance Toolkit, CRC Press, pp. 57–62, doi:10.1201/9781315385488-13, ISBN 978-1-315-38548-8, retrieved 2021-05-28

[3] Ibrahimov B.G. Research and analysis of the efficiency of multiservice communication networks using the NGN architectural concept / B.G. Ibragimov, S.R. Ismaylova // T- Comm, Telecommunications and transport, - Moscow: - 2014. Vol. 8, No. 8, - pp. 47 - 50.

[4] Ibrahimov B.G., Ismaylova S.R. On one approach to assessing the quality of functioning of a signaling network link // All-Russian Scientific and Technical Conference "Information and Telecommunication Technologies and Mathematical Modeling of High-Tech Systems", section - "Theory of Teletraffic", - Moscow: RUDN, - 2012, - pp. 38 - 40.

[5] Ibrahimov B.G., Mehdiyeva A.M., Bakhtiyarov I.N. Study of throughput indicators of corporate multiservice networks // Bulletin of Computer and Information Technologies, No. 5, Moscow, 2020. pp. 38 - 44.

[6] Ibrahimov B.G., Mehdiyeva A.M., Bakhtiyarov I.N. Mathematical model for assessing the level of noise immunity of the paths of systems for transmitting, processing and receiving packet messages // Proceedings of the XII International Scientific-Practical Conference. New Informational and Computer Technologies in Education and Science - IES-2020, – Ukraine, Vinnytsia: 2020, p .77–79.

[7] Tanenbaum E., Computer networks, Peter, 2003, pp. 361-370.

[8] Andreev R.N. Theory of electrical communication / R.N. Andreev, R.P. Krasnov, M. Hotline Telekom, 2014. 230 p.

[9] Sheluhin O.I. Modeling of information systems. O.I. Sheluhin. - Moscow: Hotline - Telekom, 2018. 516 p.

[10] Andreev R.N. Theory of electrical communication. Textbook for students / R.N. Andreev, R.P. Krasnov, M.Yu. Chepelev Hotline Telekom, 2014. 230 p.

[11] Michael P.F. Fundamentals of Communications Systems. Communications Engineering. New York: McGraw-Hill Companies, 2007. 436 p.

[12] Andreev R.N. Theory of electrical communication. Textbook for students / R.N. Andreev, R.P. Krasnov, M.Yu. Chepelev Hotline Telekom, 2014. 230 p.

[13] Bitner.V.I. Networks of the new generation-NGN. / V.I. Bitner, Ts.Ts. Mikhailova - Moscow: Hotline-Telecom. 2011. 228 p..

[14] Vasiliev K.K. Mathematical modeling of information communication systems. Moscow: Hotline Telekom. 2018. 236 p.

[15] Mehdiyeva A.M., Zeynalova, R.R., Safarova, A.A., Takhumova O.V., Nikolaevc P.P., Mozgovoy A.I. Development of an adaptive control system for the quality parameter in the lack of information. Proceedings of SPIE - The International Society for Optical Engineering, 12637, 1263707. doi: 10.1117/12.2681371, 2023, Fergana, Uzbekistan.

[16] Mehdiyeva A.M., Bakhtiyarov I.N., Bakhshaliyeva S.V. Increasing the Immunity of Information Transmission and Fault Tolerance of the Path. Lecture Notes on Data Engineering and Communications Technologies. Volume 166. Mobile Computing and Sustainable Informatics. Proceedings of ICMCSI 2023, 11-12 January 2023. Tribhuvan University, Nepal. pp. 775 784. http://icmcsi.com/2023.

[17] ISO/IEC 27000:2009 (E). (2009). Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC.

Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

[18] Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.

[19] McDermott, E., & Geer, D. (2001). Information security is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms NSPW ‘01, (pp. 97 – 104). ACM. doi:10.1145/508171.508187

[20] Anderson, J. M. (2003). "Why we need a new definition of information security". Computers & Security. 22 (4): 308–313. doi:10.1016/S0167-4048(03)00407-3.

[21] Michael P.F. Fundamentals of Communications Systems. Communications Engineering. New York: McGraw-Hill Companies, 2007. 436 p.

[22] Andreev R.N. Theory of electrical communication. Textbook for students / R.N. Andreev, R.P. Krasnov, M.Yu. Chepelev Hotline Telekom, 2014. 230 p.

[23] Bitner.V.I. Networks of the new generation-NGN. / V.I. Bitner, Ts.Ts. Mikhailova - Moscow: Hotline-Telecom. 2011. 228 p.

[24] Vasiliev K.K. Mathematical modeling of information communication systems. Moscow: Hotline Telekom. 2018. 236 p.

[25] Velichko V.V. Models and methods of increasing the durability of modern communication systems. Moscow: Hotline–Telekom 2016. 270 p.

[26] Velichko V.V. Models and methods of increasing the durability of modern communication systems. /V.V. Velichko, G.V. Popkov, V.K. Popkov. Moscow: Hotline.Telecom 2016. 270 p.

[27] Sheluhin O.I. Modeling of information systems. Teaching manual for universities. Moscow: Hotline – Telekom. 2018. 516 p.

[28] Sheluhin O.I. Modeling of information systems. Study guide for students. Moscow: Hotline Telecom. 2018. 516 p.