Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Video-Conferencing Integration into the Univercity Information Security System

Dmitry Tarov[1], Sergey Roshchupkin[1], Lyudmila Alexandrova[1]
[1]*Bunin Yelets State University, Yelets, Russia*

Abstract:- The article explores ways to increase the security of a modern university information system and use the capabilities of a video conferencing service as one of such methods. The authors assume that the centralized and hierarchical organizational structure of a Russian university is in many ways reminiscent of a corporate structure and the structure of an industrial enterprise. This, in turn, allows, during the development, construction and operation of a university information system, to rely on the standards, methods and methodology used in the construction of similar corporate systems. Ensuring information security of a university information system is understood as protecting confidential and personal data, maintaining a sufficient level of accessibility, taking into account the differentiation of the rights of various user groups, as well as data integrity. The article describes the information system of the Federal State Budgetary Educational Institution of Higher Education YSU named after. I.A. Bunin, the features of its use and the types of network attacks to which it is subjected are indicated, methods of integration into its structure are proposed, and some elements of configuration and operation are proposed in order to increase the security of the university information system.

Keywords*:information security, network threats, information system, automated university information system, video-conferencing service.*

1. Introduction

In the process of digitalization of Russian education, which is a structural element of the Russian economy, one of the sources of competitive advantage is the systematic introduction of IT technologies both in the educational process and in the administration of an educational institution. In a modern university, this is the development and deployment of its information environment, based on the university's information system and hosted both on its own hardware resources and based on external integration, for example, with online libraries, payment systems, online cards, etc. As we said earlier [1], the organizational structure of a Russian university, being centralized and hierarchical [2], is in many ways reminiscent of a corporate structure, the structure of an industrial enterprise, which, in turn, allows the development, construction and operation of a university information system to rely on standards, methods and methodology to be used when building similar corporate systems. On this basis, it can be argued that when developing, building and operating an information security system for a modern university as a structural element of its information system, one can and should proceed from the same position and use the same approaches and methodologies as in the development, construction, operation, as well as assessing the effectiveness of the information security system of an industrial enterprise or corporation [3].

Various aspects of ensuring the information security of modern educational institutions have recently received increased attention: methods for assessing network threats to which their information infrastructure is exposed are modeled [4; 5], ways to protect data obtained as a result of research [6]. At the same time, on the basis of Russian legislation [7], sets of measures are being developed to organize the work of specialists to ensure the information security of educational institutions [8].

The information system of a modern Russian university is a hardware-software system for ensuring the automation of most functions of an educational institution, including not only means of supporting educational activities, but also means of supporting document flow, coordinating the work of structural divisions and elements of an expert

system, as well as digital means of supporting scientific research. Such a complicated, distributed structure is subject to increased risks of complex information threats [1].

2. Methods

By ensuring information security of a university information system, we will traditionally understand ensuring the protection of confidential, including personal, data, maintaining a sufficient level of accessibility, taking into account the delimitation of the rights of various user groups, as well as data integrity. Confidentiality of stored information is ensured through segmentation of the information system and differentiation of access rights, including for information system administrators, data encryption, authentication and authorization methods, including through smartphones [1]. Maintaining an acceptable level of availability is achieved through the distribution of information system elements in order to ensure adequate throughput and request processing time. Data integrity is achieved through systematic backup, including the use of RAID arrays [9], data hashing, and the use of digital signatures and certificates [10]. It should be noted the extensiveness of the above-mentioned methods, implying additional costs for their implementation.

We will indicate a number of behavioral features of users of the university information system that must be taken into account when maintaining an appropriate level of counteraction to complex information threats. These include:

1. A significant number of users, among them fairly qualified ones, which include teachers and students who use computerized scientific and educational laboratories and have access to the university's network infrastructure from the inside. In addition, many users inevitably generate a significant number of requests for certain resources and, thus, the task of establishing request priorities and forming queues becomes urgent [11].

2. The university's organizational structure assumes that it is distributed among buildings, often located in different parts of the locality. In addition, it may include branches located in other localities. Because of this, the university information system assumes the diversity and distribution of individual segments, the presence of several access points to the external network, so part of the information system traffic will have to be transmitted using external networks [12].

3. Due to the diversity and distribution of the components of the information system and the presence of several access points to external networks, as well as the need to dynamically connect new components to the network structure and connect to the system via mobile communications (smartphones, tablets, laptops, etc.) the university information system has significant openness. This must be taken into account when developing, building and operating an information security system.

4. As practice shows, university hardware and software systems on which information systems are based are built on the basis of heterogeneous, often outdated, components. This negatively affects the throughput of communication channels, as well as the integration of information system components, and integration with external resources, which, in turn, reduces the availability of the information system, and the use of outdated software increases the vulnerability of the system as a whole.

5. The reliability of incoming information is determined in a spatial and temporal context, since information is verified in some context, and not on its own, for example, as data from a scientific laboratory or an accounting request. Thus, the nature of the request or transmitted information is associated with the time of the event, with the network segment and the metadata contained in the information, since without taking into account these factors there is a risk of erroneous assessment of the information, which may affect the accuracy of identifying its source.

Here are the most typical, from our point of view, examples of information threats that a university information system may encounter:

1. Random destructive impact on the university information system due to multiple simultaneous user requests that cannot be processed by the information system in an acceptable time. At the same time, the source of such influence are completely legitimate users of the system. An example is the mass access to an electronic library,

the data transmission channel capacity of which turned out to be insufficient due to a miscalculation in the design of the system.

2. Erroneous interpretation of incoming requests by information system components. Such a destructive impact can occur when an information system is integrated with speech and biometrics recognition services and so on. In addition, such threats can arise due to errors occurring during client-server interaction of software or failures during API integration with both internal and external network resources. The source of threats in this case is errors and failures of software or network infrastructure.

3. Targeted external and internal information attacks on the digital infrastructure of the university through incorrect data, when the source of impact can be either an attacker or a fully authorized user or network segment. As an example, we can point out DoS and DDoS attacks, which are quite common today. These attacks target the university's computer network infrastructure to cause a distributed denial of service to authorized users. Moreover, the source of an information attack can be not only targeted actions on the part of external botnets, but also software errors made during the development of software integrated into the information system.

Experience has shown that attacks on a university's digital infrastructure are most often tracked by the resulting anomalies in network traffic [13], the source of which can be associated with destructive actions from the outside, errors of authorized users, as well as software and hardware failures. In addition, when ensuring information security of a university information system, it is necessary to take into account the dynamic conditions of the system's functioning, dictated by frequent changes in the composition of users due to the completion of studies by some students and the arrival of new ones, as well as the replacement of hardware components and software updates, the connection of new network segments, as well as the dynamics network threats and their sources, which requires the information system to be adaptable to information security tools.

Thus, we come to the conclusion that in order to ensure a sufficient level of information security of the university information system and ensure an appropriate level of its accessibility to users, it is necessary to develop and put into operation a system of its adaptive protection against complex information threats, taking into account the peculiarities of the functioning of the university as an organizational structure, which dictates the need identifying these conditions.

3. Research results and discussion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Orci a scelerisque purus semper eget duis at tellus at. Quisque egestas diam in arcu cursus. Pulvinar mattis nunc sed blandit. Tempus iaculis urna id volutpat lacus laoreet non curabitur. Morbi tincidunt ornare massa eget egestas purus viverra accumsan in. Vehicula ipsum a arcu cursus. Sapien et ligula ullamcorper malesuada proin. Ut diam quam nulla porttitor. Tincidunt dui ut ornare lectus sit. Neque ornare aenean euismod elementum nisi quis eleifend. Mus mauris vitae ultricies leo integer. In nulla posuere sollicitudin aliquam ultrices. Eget duis at tellus at urna condimentum mattis. Tellus molestie nunc non blandit. Quam quisque id diam vel quam elementum pulvinar. Integer quis auctor elit sed vulputate mi. Pellentesque elit eget gravida cum sociis natoque penatibus et. Aliquet risus feugiat in ante. Commodo ullamcorper a lacus vestibulum sed.

Congue nisi vitae suscipit tellus mauris a diam maecenas. Aliquet nec ullamcorper sit amet risus. Pulvinar sapien et ligula ullamcorper malesuada proin libero nunc consequat. Non consectetur a erat nam at lectus urna duis convallis. Purus viverra accumsan in nisl nisi scelerisque eu. Netus et malesuada fames ac turpis egestas maecenas pharetra convallis. Sed turpis tincidunt id aliquet. Et malesuada fames ac turpis egestas sed tempus urna et. In dictum non consectetur a erat nam at. Nulla aliquet porttitor lacus luctus accumsan tortor posuere. Nunc consequat interdum varius sit amet mattis vulputate enim nulla. Cras tincidunt lobortis feugiat vivamus. Venenatis a condimentum vitae sapien pellentesque habitant morbi. Suscipit adipiscing bibendum est ultricies integer. Et ultrices neque ornare aenean. Ut porttitor leo a diam sollicitudin tempor id eu. Lorem ipsum dolor sit amet consectetur adipiscing elit. Morbi tincidunt ornare massa eget egestas purus viverra accumsan in. Sit amet consectetur adipiscing elit duis tristique.

Ipsum dolor sit amet consectetur adipiscing. Arcu felis bibendum ut tristique. Lectus sit amet est placerat in egestas. In massa tempor nec feugiat nisl pretium. Vel pharetra vel turpis nunc eget lorem dolor. Ornare aenean euismod elementum nisi quis eleifend quam. Tellus id interdum velit laoreet id donec. Eget arcu dictum varius duis at consectetur lorem donec massa. Amet facilisis magna etiam tempor orci eu lobortis. Consectetur adipiscing elit duis tristique sollicitudin. Pellentesque dignissim enim sit amet venenatis urna cursus eget.

Pellentesque adipiscing commodo elit at imperdiet. Lectus proin nibh nisl condimentum id venenatis. Dignissim diam quis enim lobortis scelerisque fermentum dui faucibus in. Volutpat diam ut venenatis tellus. Vehicula ipsum a arcu cursus vitae. Volutpat maecenas volutpat blandit aliquam etiam. Sed id semper risus in. Eget nulla facilisi etiam dignissim diam quis enim lobortis scelerisque. Tellus in hac habitasse platea dictumst. Non enim praesent elementum facilisis leo. A cras semper auctor neque vitae tempus quam pellentesque. Dolor magna eget est lorem ipsum dolor sit amet consectetur.

Neque laoreet suspendisse interdum consectetur libero id faucibus. Ac turpis egestas maecenas pharetra convallis. Sagittis aliquam malesuada bibendum arcu vitae elementum curabitur vitae nunc. Nulla facilisi cras fermentum odio eu feugiat pretium nibh. Tortor at auctor urna nunc id cursus. Bibendum enim facilisis gravida neque convallis a cras semper auctor. Feugiat vivamus at augue eget arcu. Et netus et malesuada fames ac turpis egestas. Quisque id diam vel quam elementum. Amet est placerat in egestas erat. Egestas maecenas pharetra convallis posuere morbi leo. Sagittis aliquam malesuada bibendum arcu vitae. Ultricies lacus sed turpis tincidunt id aliquet risus. Ipsum dolor sit amet consectetur adipiscing elit. Cursus sit amet dictum sit amet justo donec.

4. Results

Using as an example the information system of the Federal State Budgetary Educational Institution of Higher Education Yelets State University named after I.A. Bunin, we will examine the conditions that make it possible to effectively protect it from complex information threats. The university information system is built on a service-oriented architecture and is segmented in order to isolate critical nodes from external interference, i.e. it contains loosely coupled services, the transfer of data streams between which is supported based on web sockets, which support opening and connecting using standard data transfer protocols. Their use of websockets was chosen because they, unlike the REST architecture, make it possible to keep the connection active for a fairly long time, which is certainly important when opening and maintaining a secure connection based on the HTTPs and TLS protocol. Unlike the transmission of JSON messages, the process of generating keys when creating a logical channel is a longer process, so using web sockets instead of REST architecture when building a university information system allows us, firstly, to effectively control connection statuses, and secondly, to quickly restore services and network segments after software and hardware failures and, thirdly, significantly reduces the cost of its development, construction and operation.

Let us list the system and application services, as well as network segments implemented in the information system of the Federal State Budgetary Educational Institution of Higher Education YSU named after. I.A. Bunin. Services and segments are described in detail by the formats for interaction with each other, their implementations and interfaces through which user access is provided are indicated.

Table 1. Services and segments of the information system of the Bunin Yelets State University.

Services and Segments	Description
System	
Identification, Authentication and Authorization System	Identification, authentication and authorization of users, provision and control of access rights to services and network segments to the content of the information system.
Database of Services and System Segments	Storing and issuing upon request information about the components of the university information system, their current status and access methods.
Administration System	Interface for online administration of the information system.

Group Policy Enforcement System	Implementation of group policy, granting and controlling access rights to users of the information system.
The Event Log	Publication and storage by services and network segments of information about states and events necessary for the functioning of other services and segments of the university information system.
Applied	
Educational Portal	A highly accessible online resource containing curricula, educational and work programs, as well as educational content prepared by teaching staff.
Scientific Portal	A network resource that is part of an isolated computer subnet and supports scientific research, processes and stores its results.
Digital Library	A highly accessible network resource containing electronic publications.
Software Repository	A repository of software products that allows you to quickly update or recover software after failures.
Accounting Department, HR Department and Legal Service	A network resource that is part of an isolated computer subnet and carries out accounting calculations and auditing, and also stores personal information of employees and legal documentation.
Expert Decision Making System	A network resource that is part of an isolated computer subnet and has connections to the subnet of the accounting department, human resources department, legal service and provides decision-making support at the level of the university administration.
University Television	A highly available network resource that supports editing, storing and broadcasting video content.
Video Conferencing System	A highly available network resource that supports video conferencing between client devices in the university information space.
User Identification System	A network resource that supports user identification through electronic keys and access cards.
System for Determining User Location and Navigation on Campus	A network resource that determines the user's physical location on the university's territory and provides him with information about the location of structural units.

Let us illustrate the abovementioned views by analyzing the process of user interaction with a video conferencing system, built on the basis of a complex of web cameras, a video conferencing support server, mobile devices and stationary screens located in public places. In addition to their direct purpose, web cameras are used to identify and search for users.

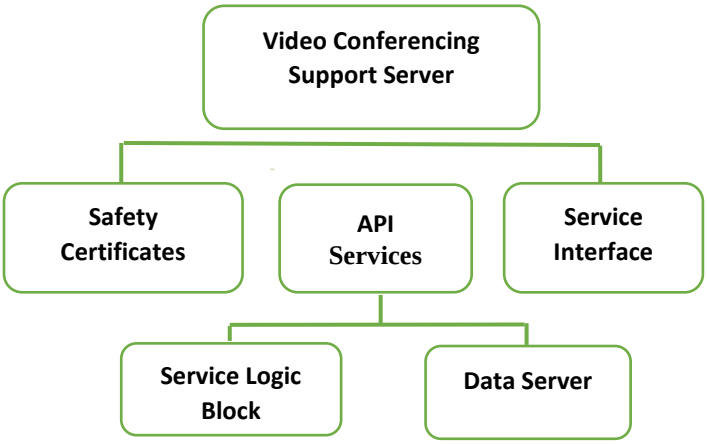

Fig.1. Structure of the video conferencing support service

The main feature of the video conferencing service is its interactivity, which allows users to be identified and authenticated using web cameras or fingerprint scanning modules of mobile devices of users [1], who are able to interact with the service using a web application installed on a mobile communication device (smartphone, tablet, laptop). Administrators control the operation of the service through a web interface and an Event Log.

The video conferencing support server generates a one-time token and displays them on a stationary screen or monitor in the form of a QR code. The user scans this QR code through a web application, which, in turn, using a token received from the system, connects to the video conferencing support service through its API. This allows the user, within the framework of the rights granted to him, to interact with the video conferencing support service through the mobile application interface.

The video conferencing support service API is implemented based on the GraphQL query and data manipulation language and provides the ability to implement two types of GraphQL queries within the system under consideration, namely:

1. query – to obtain information about the current status of the video conferencing support service;

2. mutation – to change the state of a service by sending one or another service command.

The request addressed to the video conferencing service will look like this:

```
query {
    monitor (id: <ID >, key: <key>) {
        currentMedia,
        status,
        medias {
            id,
            name
        }
    }
}
```

In the case of a request to a video conferencing support service, <ID> indicates the identifier of one or another stationary screen of this service, <key> is a token generated by the video conferencing support service server for user authorization and is required when sending the first session request. The rest fields, such as currentMedia, status, ID, name are optional, and they are used to requesting certain data. As an example, Table 2 shows the possible composition of the request fields.

Table 2. Request fields for the video conferencing service of the Bunin Yelets State University.

Field Name	Field Values
currentMedia	*Fixed Screen ID*
status	Fixed Screen Status Flags 1 – connection error

	2 – debugging and calibration mode 4 – enable data caching 8 – pause mode 16 – desktop screen lock mode
medias.id	ID of the selected media file
medias.name	the name of the selected media file

In this case, the mutation request will look like this:

```
mutation {
        sendMessage (id: <ID>, commands: <commands>) {
                status
        }
}
```

The <commands> field specifies one or more commands that control the state of the stationary screen, where the ";" sign is used as a separator. Table 3 lists some possible control commands.

Table 3. Some commands that control the states of fixed screens of the video conferencing service of the Bunin Yelets State University.

Command for managing the states of stationary screens	Command Description
lock [on | off]	enable/disable desktop screen lock
debug [on | off]	enable/disable fixed screen debugging mode
reload	restarting the desktop screen service application
load<ID>	loading a media file with the specified ID
next	calling a media file with the next ID
prev	calling media file with the previous ID
pause [on | off]	enable/disable pause when playing a media file

Processing a user request initiates the launch of a separate task, for which the required software and hardware resource is allocated; the lack of these resources can provoke a decrease in the availability of the video conferencing service. To eliminate the threat, a user request management procedure is used [14], which allows increasing the availability metrics of the corresponding service.

We also note that the use of a video conferencing service as a component of the university's information security system makes it possible to uniquely identify a user logging into the system via a mobile communication device that has identification tools such as FaceID or a fingerprint scanner and a SIM card associated with them. At the same time, the use of webcams of the service allows you to accurately localize the place and time of connection. All this allows us to fully utilize administrative measures to protect the university's information system, relying on legislation and legal practice.

5. Conclusion

Experience has proven that services like video conferencing services are increasingly susceptible to DDoS attacks, causing failures and denial of service. In particular, there are a significant number of attacks such as HTTP-flood, SYN-flood and TCP-flood. Protection against these attacks consists of comparing the characterizing parameters of some packets and, if they match, a conclusion is drawn about the presence of a threat to information security and a certain interval of IP addresses is temporarily blocked. In addition, a database is created containing the characteristic parameters of packets and messages that have previously participated in similar network attacks and the IP addresses associated with them. This may provide grounds for permanent blocking of such addresses.

From our point of view, the proposed integration of the video conferencing service into the university's information security system increases its efficiency and sustainability and allows us to fully rely on legislation

and legal practice when ensuring information security. However, unfortunately, at present there are no comprehensive methods for ensuring university information security, which leaves us with a wide field of activity.

The authors express their gratitude to the management of Bunin Yelets State University for the financial support of this study.

Refrences

[1] Tarov D., Tarova I., Roshchupkin S. (2023). Information Security Enhancements of the University's Automated Information System. Lecture Notes in Networks and Systems, 722, 45-53. DOI: 10.1007/978-3-031-35311-6_6

[2] Podgaeckij N. A., Transformation of Organizational Structures of Technical Universities in the Innovative Economy. Aktual'nye voprosy jekonomiki, menedzhmenta i innovacij: Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii uchenyh, specialistov, prepodavatelej vuzov, aspirantov, studentov, Nizhnij Novgorod, 17 nojabrja 2021 goda [Current issues of economics, management and innovation: Materials of the International Scientific and Practical Conference of Scientists, Specialists, University Teachers, Postgraduates, Students, Nizhny Novgorod, November 17, 2021]. Nizhny Novgorod, 2021, pp. 329-336 (in Russisn) – EDN WOHNVO.

[3] V.V. Goryunova, T.I. Goryunova, Y.V. Molodtsova.Integration and Security of Corporate Information Systems in the Context of Industrial Digitalization in Proceedings - 2020 2nd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, SUMMA 2020 : 2, Virtual, Lipetsk, 10–13 ноября 2020 года. – Virtual, Lipetsk, 2020. – P. 710-715. – DOI 10.1109/SUMMA50634.2020.9280663.

[4] S. Ramanauskaitė, N. Urbonaitė, Š. Grigaliūnas, S. Preidys, V. Trinkūnas, A. Venčkauskas. Educational Organization's Security Level Estimation Model - Applied Sciences (Switzerland), 2021, 11(17), 8061. DOI: 10.3390/app11178061

[5] Maksimjak I. N., Potapov M. L. Neobhodimost' kompleksnoj avtomatizacii upravlenija obrazovatel'noj dejatel'nost'ju vysshih uchebnyh zavedenij v sovremennyh uslovijah [The Need for Comprehensive Automation of Management of Educational Activities of Higher Educational Institutions in Modern Conditions]. Ufa, Nika, 2019, pp. 71-75

[6] S. Yazawa, K. Sakaguchi, and K. Hiraki. 2021. "GO-E-MON: A New Online Platform for Decentralized Cognitive Science" Big Data and Cognitive Computing 5, no. 4: 76. https://doi.org/10.3390/bdcc5040076

[7] Dolmatov A. V., Dolmatova L. A., Prerequisites and Prospects for the Transformation of Russian Legislation in the Field of Information Security. Vestnik Sankt-Peterburgskoj juridicheskoj akademii [Bulletin of the St. Petersburg Law Academy], 2019, no 1(42), pp. 66-72 (in Russisn)

[8] W. Villegas-Ch, I. Ortiz-Garces, S. Sánchez-Viteri. Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. Computers. 2021; 10(8):102. https://doi.org/10.3390/computers10080102

[9] Proskurjakov N. E., Jakovlev B. S. Determination of Parameters for Automated Backup of Digital Data of Printing Houses and Publishing Houses without the Use of External Network Technologies. Dinamika sistem, mehanizmov i mashin [Dynamics of Systems, Mechanisms and Machines], 2018, t. 6 (no 2), pp. 50-57 (in Russisn) – DOI 10.25206/2310-9793-2018-6-2-50-57

[10] Sopin K. Ju., Dichenko S. A., Samojlenko D. V. Monitoring Data Integrity When Scaling Storage Systems under the Destructive Influence of an Attacker and Disturbances in the Operating Environment Avtomatizacija processov upravlenija [Automation of Management Processes], 2021, pp. 15-27 (in Russisn) – DOI 10.35752/1991-2927-2021-4-66-15-27

[11] Levonevskiy D., Vatamaniuk I., Saveliev A. Processing models for conflicting user requests in ubiquitous corporate smart spaces // MATEC Web of Conferences. 2018. T. 161.

[12] Levonevskiy D., Afanasieva I., Fedorchenko L., Novikov F. Verification of Internet Protocol Properties Using Cooperating Automaton Objects. Proceedings of the 12th International Conference on Security of Information and Networks (SIN-2019). 2019. C. 1-4. DOI: https://doi.org/10.1145/3357613.3357639

[13] Perov R. A., Lauta O. S., Kribel' A. M., Fedulov Ju. V. Method for Detecting Anomalies in Network Traffic. Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli [High technology in space exploration of the Earth], 2022, pp. 25-31 (in Russisn) – DOI 10.36724/2409-5419-2022-14-3-25-31

[14] Sumin V. I., Grachev E. D., Lukin M. A. Analysis of Methods for Managing Server Load in Distributed Large-Scale Information Systems. Vestnik Voronezhskogo instituta FSIN Rossii [Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia], 2021, no 3, pp. 116-124 (in Russian)