Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept

Pavlo Skladannyi[1], Olexandr Trofimov[1], Viktor Korniiets[2], Maksym Vorokhob[1], and Tetiana Opryshko[1]

[1]*Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[2]*Institute of Problems of Mathematical Machines and Systems, 42 Academician Glushkov ave., Kyiv, 03187, Ukraine*

Abstract

The issue of automation of information technology support for distance learning is the subject of many studies and heated discussions among scientific and pedagogical workers, as well as the object of special attention from society. Existing software platforms supporting the educational process provide solutions mainly to problems of management of the digital learning environment, while only partially responding to challenges and threats from cyberspace and the potential for dishonest actions by participants in the educational process. The paper analyzes the characteristics of common learning management systems and identifies the security functions implemented in them. Based on the concept of Zero Trust, the paper proposes an appropriate threat model for the digital learning environment and formulates proposals for building an improved information security policy and implementing relevant mechanisms and architecture for Distance Learning System (DLS) security.

Keywords

Distance learning system, cyber security, Zero Trust concept, security threat model, security mechanisms

1. Introduction

Distance learning spreads easily due to the natural adaptability of young people to the surrounding world and the technologies that evolve in it [1]. The relevance and spread of this education support technology began to grow rapidly in the conditions of strict quarantine due to the COVID-19 pandemic [2]. Recently, advanced experience has been gained in the use of distance learning tools for the training of specialists in various fields of humanitarian and natural sciences. In the conditions of martial law, more and more Participants in the Educational Process (PEP) are forced to switch to distance learning, which determines the need to create Distance Learning Systems (DLS), that by the requirements of the law [3–5] can ensure the protection of personal data processed and stored in them, as well as to prevent unauthorized use of educational resources of systems, violation of their integrity and availability.

A distance learning system is understood as a set of hardware and software platforms, including a Learning Management System (LMS), educational information resources, methodical support, and reporting documents, as well as participants in the educational process who support the functioning of the system and use it as intended [6].

The issue of automation of information technology support for distance learning is the subject of many studies and heated discussions among scientific and pedagogical workers, as well as the object of special attention from society. As the world becomes increasingly digital, the need for secure distance learning systems will only grow, as there is no alternative to investing in modern technologies to ensure the security of digital learning environments. Lack of proper attention to this issue can have negative consequences in the medium and long term [7, 8].

The analysis of the latest scientific and practical publications on the construction of

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: p.skladannyi@kubg.edu.ua (P. Skladannyi); trofimov@gmail.com (O. Trofimov); viktorkorniets@gmail.com (V. Korniiets); m.vorokhob.asp@kubg.edu.ua (M. Vorokhob); t.opryshko@kubg.edu.ua (T. Opryshko)
ORCID: 0000-0002-7775-6039 (P. Skladannyi); 0009-0008-5760-7803 (O. Trofimov); 0000-0002-4967-8395 (V. Korniiets); 0000-0001-5160-7134 (M. Vorokhob); 0000-0002-9282-0182 (T. Opryshko)

reliable and safe DLS, as well as the state of regulatory and legal support of the relevant processes, shows the importance of conducting research and development in the field of information security of digital educational environments [9].

In particular, in [10] a comprehensive analysis of the current situation regarding the application of distance learning technologies in educational establishments as a whole was carried out. Technological solutions were identified that could contribute to improving the results of the application of such technologies in higher educational institutions. In [11], based on studying the requirements of legislation and regulatory documents, the methodological principles of building guarantee-capable protected information DLS of higher education institutions are determined. In [12] it was noted that learning management systems, as an important component of the educational environments of many universities, support a significant number of different types of activities and functions, including aspects of protection. In [13], the experience of using the common LMS Google Classroom and general data on the principles of building a software platform to support distance learning of our development based on the "client-server" architecture are presented, while the issues of protecting the educational environment are not considered.

Existing approaches to the construction of information security policy and its components are generally considered in international and national standards [14–18], but consideration of the peculiarities of the functioning of the educational environment is left to the discretion of designers and developers.

The main provisions and architecture of the concept of Zero Trust are given in [19], and in [20]. In addition, the main directions of its application within the framework of the organization's information security policy are proposed.

It should be noted that the analysis of the publication [21–25] about the features of building software platforms focused on e-learning and the study of messages on PEP forums about the presence of certain problematic situations associated with the use of such platforms, indicate their in complete compliance with the educational process, which is defined by legislation [26, 27], as well as requirements for information protection [3–5]. One of the reasons for this situation is the fact that the vast majority of popular educational platforms, including those used in Ukraine, are aimed at the international market and are not tied to the legislation of specific countries.

The review shows the efforts of scientists and practitioners to solve the problem of building and protecting the digital learning environment of higher education institutions using different approaches. However, the issue of improving their information security policy is still an urgent task.

Taking into account a detailed comparison of the provisions of the concept of Zero Trust [19, 20] and the features of the functioning of the digital educational environment [12, 13, 21–25], it is possible to assert the potential benefit of applying the approaches of the concept to securing valuable information resources of an educational institution by improving the information security policy of the institution and promoting academic integrity in the digital environment.

The purpose of the work is to develop and research the principles and methods of building the Information Security Policy of the domestic distance learning system, including:

- Analysis and comparison of the state of information security of common educational platforms.
- Formation of a model of threats to the DLS based on the concept of Zero Trust.
- Determination of practical aspects of improving the information security policy based on the concept of Zero Trust and mechanisms for ensuring the protection of information resources of the DLS.

2. Analysis of the Security Functions of Common Educational Platforms and Formation of a Threat Model Based on the Zero Trust Concept

Considering the publications [21–25] as a basis, the information (Table 1) about the security functions of common software systems of support of the educational process (LMS) Moodle, Blackboard, Canvas, Google Classroom, Khan Academy (hereinafter products 1–5), which are currently used by educational institutions, is summarized.

Taking into account the analysis of the generalized data, it is possible to pay attention to the fact that the "User authentication" function is implemented in all identified systems, while multifactor authentication is provided in products 1–4.

The Access Control feature in the above-mentioned LMSs is mostly controlled by the learning event organizer, and only in product 1 role-based access control is announced.

The availability of the “Event monitoring, logging” function in products 1, 3, and 5 allows to monitor of the occurrence of certain incidents in environments and facilitates investigation in cases of undesirable situations.

All products in one way or another provide encryption of data transmitted between the server and client browsers, in particular, using the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, which increases the security of confidential information when it is forwarded through an unprotected environment. At the same time, only product 4 provides encryption of data during their storage on servers.

The implementation in products 4 and 5 of the Privacy Policy function allows you to store data only as long as it is necessary to provide the service or allow users to control their data.

Table 1
Security functions of educational process support systems

Security functions of systems	Educational process support systems (LMS)				
	1	2	3	4	5
	Moodle	Blackboard	Canvas	Google Classroom	Khan Academy
User authentication	+	+	+	+	+
Access control/management	+		+	+	+
Event monitoring, log keeping	+		+		+
Data encryption	SSL/TLS	HTTPS	SSL/TLS	TLS/AES/ RSA/D-H	HTTPS
Personal information privacy policy				+	+
Backup copying	+	+			
Security testing/auditing/updating	+	+	+	+	+
Strong password policy	+				

The “Backup copying” function, provided in products 1 and 2, forms the basis for ensuring the stable functioning of the LMS and the possibility of restoring its operation in the event of the implementation of threats that can lead to the destruction of critical information resources.

All analyzed LMSs have built-in “Security Testing/Audit/Update” functions in a certain way, which should be considered a positive factor in terms of responding to possible dangerous changes in the surrounding environment.

Based on the conducted analysis, it is possible to claim that among the considered LMSs, product 1 has the best functionality from the point of view of ensuring the confidentiality and availability of information resources, as well as the observation of processes. It is easy to see that this functionality meets the minimum security requirements defined in [28].

At the same time, none of the above-mentioned systems provides functions and mechanisms for checking the integrity and authenticity of resources as well as their authorship.

Note that the concept of Zero Trust applies to all participants in information exchange, therefore, based on the ontological model of the educational process proposed in [11], it is possible to define the following roles in DLS, which differ in the scope of functional tasks and, accordingly, access rights to information resources.

The role of “security manager” (denoted by M) involves granting them the authority to manage tools, measures, and parameters for the information security of the DLS. This role does not involve access to documents and materials of the learning environment for their modification.

The roles of the officials of the dean’s office of the educational institution (denoted by D) require to be given to them the authority in the system to approve plans, programs, class schedules, and information on the results of the final events as well as implement control over the progress and results of the educational process. The specified roles provide access for modification of the relevant resources and fixation based on the results of measures to control the current state of information resources, including accounting logs.

The role of “teacher” (denoted by P) involves the direct implementation of the educational process, including the development of drafts of programs and plans of the educational discipline, the formation of educational and methodological support, conducting lectures, seminars, practical and laboratory classes, tests, keeping records of attendance at these classes and evaluating students based on their results, final control, etc. The role of P requires, in particular, to give them access to the instructional documents of the educational institution for “reading” and the approved Educational Methodical Support (EMS) for the educational discipline he or she teaches, to “form and edit” drafts of the EMS documents (before their approval).

“Student” roles (denoted as $\boldsymbol{S_1 \dots S_K}$) require access to the resources of the EMS of the educational discipline and the authority to download reporting materials based on the results of training to record their status and integrity and to confirm authorship. Each reporting resource must be certified by the teacher as a fact: “the document as it is at the current time.” The change of reporting documents of the type “modular control work” must be approved by the role “dean’s office” (D).

Potentially, regarding the information resources of the educational environment $\boldsymbol{I_1, I_2, \dots, I_K}$, which are owned (or created) by certain participants of the educational process and require the protection of confidentiality, integrity, or availability, the following operations can be implemented:

- ***Fr*** is a forgery—actions of some of the participants in the educational process aimed at misleading another participant by creating a fictitious information resource.
- ***Md*** is modification—unauthorized actions of some of the participants in the educational process aimed at changing the real state of the information resource or its parameters (for example, the time and date of creation, identifier of the author of the resource, etc.).
- ***Ms*** is masking—the actions of some of the participants in the educational process, aimed at misleading another participant and implemented by bypassing the access control system in the DLS or by using real personal identification and authentication parameters (for example, login and password) of a third participant.
- ***Rj*** is a refusal to receive a certain resource or document placed or created by another participant in the educational process in the educational environment within the time and space frameworks determined by the regulation of the system by the established powers (for example, failure to confirm the fact of receiving the completed task within the specified time limit).

It remains to define the last side of the threat model—the violator of information security (let’s denote them as $\boldsymbol{H_C}$), who can act independently or in collusion with some participant in the educational process for unauthorized access to information resources $\boldsymbol{I_1, I_2, \dots, I_N}$—digital educational environment DLE and can potentially implement any kind of illegal operation(***All***).

Taking into account the assumptions made, a model of threats to the security of DLS was formed based on the concept of Zero Trust (Fig. 1).

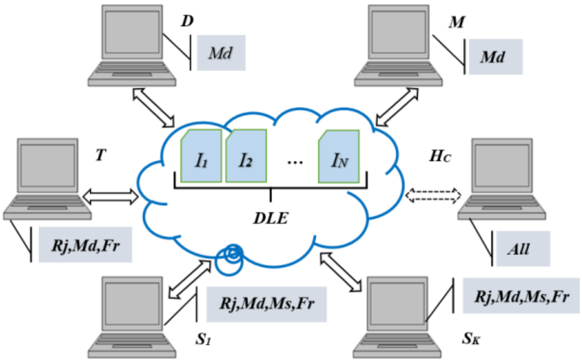

Figure 1: DLS threat model based on the concept of Zero Trust

In the given model, it seems appropriate to assume that only the following roles can potentially “act in a coalition” (collusion), namely: certain ***Si*** and $\boldsymbol{H_C}$, or ***Si*** and ***Sj***, or ***Si*** and ***T***, or ***Si*** and ***D***.

To avoid disagreements or uncertainty in security policy, it is further assumed that the role of security management does not involve coalitions, nor is a coalition of three participants in the educational process possible.

3. Practical Aspects of Building the Information Security Policy of the Distance Learning System based on the Concept of Zero Trust

The following were selected as the initial data for the formation of the Information Security Policy of the DLS:

- The provision of the law defines a safe educational environment as a set of conditions in an educational institution that make it impossible to cause harm to the PEP, in particular as a result of non-compliance with the requirements of the legislation on cyber security or personal data protection [3], as well as academic integrity as a set of ethical principles and rules that have to be guided by the PEP during training, teaching and carrying out scientific activities to ensure trust in the results of learning achievements [4].
- Requirements of standards and regulatory documents on information protection [14–18, 28].

Based on these data, using the constructed model of threats to the digital educational environment, the following basic principles of the Information Security Policy of DLS were formulated:

- Awareness is the participants of the educational process should be informed in detail about the established procedure and conditions for the protection of information resources in the digital educational environment and about their obligation to comply with information security norms.
- Responsibility is the participants are responsible for their actions that negatively affect information security (information dishonesty).
- The response is the participants in the educational process act together to prevent, identify and respond to incidents in the information security system of the digital educational environment promptly.

A detailed definition of a partial response policy to incidents in the system is of special importance for the Information Security Policy of the DLS, which corresponds to the principles of the concept of Zero Trust. At the same time, a detailed incident response plan should be developed, which defines the areas of responsibility of the PEP and their tasks, recommendations regarding the sequence and content of the actions of officials in the event of a security incident and its investigation, proposals for measures to reduce the negative impact of incidents on the educational process and prevent their occurrence in the future (implementation of countermeasures).

Taking into account the recommendations of security standards [18], it is considered appropriate to include the following sections in the typical partial policy of response to information security incidents of DSL:

1. Formation of an incident response team (IRT):

- Determination of the goals and tasks of IRT actions, distribution of responsibilities among group members, in particular, the tasks of the manager, experts in information technologies, cyber security, communications, educational and methodological, and legal issues.
- Development of a communication plan that defines the channels of prompt delivery of information to the PEP and receiving feedback, the procedure for the interaction of IRT members with DLS administrators, and security management during the investigation of incidents.
- Defining and clarifying the procedures for informing the management of the educational institution and the PEP about incidents and regularly updating the status of incidents that have occurred. This information has an important aspect of professional ethics: premature information about the progress of the investigation, which allows identification of the participants in the incident, can harm both the conduct of the investigation and the reputation of the relevant PEP.

2. Identifying and documenting potential incidents:

- Creation of a list of potential DLS incidents. This list should include both cyber security incidents and other types of incidents that may affect the security status of the system, including natural disasters and technical failures.
- Assessment of the probability of occurrence of each incident and their possible consequences.
- Determination of the scale (levels) of incident danger and classification of incidents based on the created scale. This measure should help the IRT to prioritize the handling

of incidents and accordingly allocate resources to investigate and deal with the consequences.

- Development of procedures for identifying and documenting emerging incidents, which may include activities of surveying the PFP, studying documents, copying information on media, viewing e-mail, etc.

3. Formation of response procedures:

- Determination of response tools, which may include localization of the incident, temporary blocking of individual resources and/or users, adjustment of resource access policies, unplanned change of security parameters, etc. These tools are applied at certain steps of the response procedures.
- Development of a basic set of response procedures to be followed by the IRT for each level of incident complexity.
- Development of a list of measures/a plan to contain the incident and restore the initial state of the system. This plan identifies specific steps to prevent the incident from spreading and restore the system to a stable operation.
- Determination of the procedures for checking the effectiveness of the incident localization plan and restoring the initial state.

4. Conclusions, testing, and improvement:

- Adjustment of the basic policy based on the findings of the incident investigation.
- Conducting regular training to keep IRT skills up-to-date.
- Regular testing of the incident response plan to ensure its relevance and effectiveness.

By its very nature, an information security incident response plan should be a guiding document that is regularly updated to reflect new threats and changes in DLS security.

To a large extent, the effectiveness of the implementation of security measures, provided for in the information security policy of the DLS, depends on the reliability and sufficiency of the mechanisms used to protect the educational environment, so it seems appropriate to pay attention to the specifics of their implementation by the concept of Zero Trust.

4. The Architecture and Protection Mechanisms of DLS based on the Concept of Zero Trust

As it was noted, the mechanisms for ensuring the confidentiality and availability of information are implemented in common learning management systems. At the same time, the issues of ensuring integrity remain open. That is why it seems appropriate to pay attention to the requirements for minimizing the risks of illegal transactions in the initial environment ***Fr, Rj, Md, Ms.***

A logical preventive measure to reduce the risk of data forgery operations ***Fr,*** refusal to create or receive *Rj,* or modification *Md* of an information resource created by another participant in the educational process, in conditions of Zero Trust can be the implementation of a parallel structure of a digital collective signature based on asymmetric cryptography [29].

The main disadvantage of this approach is the need for significant financial expenses of the educational institution to create and maintain the functioning of its own secure open-key certification center or to obtain relevant services from an accredited center. It should also be taken into account that the procedures for forming and verifying a digital signature are performed quite slowly compared to symmetric cryptographic transformations.

Under the conditions of the specified assumptions, to ensure data integrity control in the educational digital environment, it is proposed to implement message authentication codes using a reliable block encryption algorithm [30, 31]. So we have:

$$MAC(M) = Choose_m \left(E_k \left(M_L \oplus \dots \oplus E_k\left(M_2 \oplus E_k(M_1)\right)\right)\right), \quad (1)$$

where:

- $MAC(M)$ is a bit string of length *m* which is the authentication code of the message (information resource, data) M supplemented with the time and date of its creation, as well as unique identifiers of its originator and other participants in the information exchange.
- $M = M_1 \parallel M_2 \parallel \dots \parallel M_L$ is the submission of the message M in the form of a concatenation of blocks of equal length for their processing (the last block can be supplemented with a sequence of identical bits up to the specified length of the block to be encrypted).
- E_k is a secure block encryption algorithm using the key k.
- $Choose_m$ is the function of selecting the first *m* bits from the data block.

To prevent the coalitional falsification of information resources in the educational environment, it is proposed to create a joint secret (private) key k [32] of several participants in the educational process. At the same time, the shared key is calculated from the private keys of three participants in the educational process:

$\{Si, T, D\}$ are for the case of resource control created by the student, accepted by the teacher, and confirmed by the dean's office:

$$k_{STD} = k_S \oplus k_T \oplus k_D, \tag{2}$$

$\{T, D, M\}$ are for the case of resource control created by the teacher, confirmed by the dean's office and security management:

$$k_{TDM} = k_T \oplus k_D \oplus k_M, \tag{3}$$

where k_S, k_T, k_D, k_M are private keys of the student, teacher, dean's office, and security management, respectively.

In the case of control of a resource created by the student and by the dean's office and confirmed by the security management, which, according to our assumption, cannot be a member of coalitions, the private key is the result of adding the private keys of the dean's office and the security management:

$$k_{DM} = k_D \oplus k_M. \tag{4}$$

Ensuring the efficient operation of the authentication subsystem is a central task in the process of creating any secure system. At the same time, in the case of the model of Zero Trust, the classic method of PEP authentication based on the "login-password" pair is ineffective due to the potential collusion of some PEPs.

One of the ways to overcome the problem of PEP collusion is the introduction of multifactor authorization technology.

In particular, one of the factors in increasing the reliability of the identification of PEP, as well as reducing the risk of Ms masking, could be the introduction of electronic scorebooks, which was proposed in [33], but at the moment the question of practical developments in this direction remains open.

Encouraging experimental results regarding identification were obtained in [34] based on voice and visual biometric indicators of PEP, while a relatively high level of probability of correct identification $p_{ID} = 0.91$ was achieved.

It should be noted that this means that, on average, in about 10% of cases, the identification procedures may not be satisfactory, and a legitimate PEP may not be identified, which reduces the effectiveness of using this method as the primary mechanism for identifying users of the DLS.

At the same time, the advantage of the method of identifying a person by voice is the possibility of software implementation of the corresponding recognition algorithm [35] in the form of an application in the environment of common operating systems, which can contribute to ensuring the compatibility of stationary and mobile components of DLS. In addition, in this case, unauthorized access attempts to DLS resources, registered in the system event log in the form of personal biometric information, can be used as indisputable evidence during incident investigations. The perspective of this approach is also enhanced by the possibility of creating certain random content during authentication, which can be used to modify the parameters of identification systems and control the integrity of resources.

Another user identification mechanism that has proven its effectiveness, in particular, in bank payment systems, is the confirmation of access to the system through an additional channel, through a smartphone application. This creates an additional way to pass identifying information that is difficult to track even at the *Hc* role level.

Taking into account the above considerations, the DLS user identification procedure will include the following steps:

1. Access to the system using a personal login and password.

2. In the case of a positive conclusion regarding the provided login and password, the system displays a random sequence with an even distribution of decimal digits on the user's monitor screen:

$$\mathcal{A} = \langle a_1, \ldots, a_w, a_i \in \overline{\{0,9\}}, \Pr(a_i = j) = 10^{-1}, \forall j \in \overline{\{0,9\}}, i = 1,2,\ldots,w \rangle, \tag{5}$$

and invites them to read aloud. The length of the sequence *w* must be sufficient to identify the user by voice. On the other hand, to prevent brute force attacks, the length of the sequence $\mathcal{A}$ must satisfy the inequality:

$$10^w > V_{max} \cdot \tau_{ult}, \tag{6}$$

where V_{max}—the maximum speed of sorting through the variants of the sequence $\mathcal{A}$ using the computing equipment at the disposal of the potential infringer, τ_{ult}—the time limit for the attack. In fact, (5) and (6) are the requirements for a strong password.

3. Based on the received audio information, the system attempts to identify the user using a database of standards—samples of PEP voice messages

4. In the case of a positive conclusion about the authentication of the PEP, the system informs them about it and gives them access to the digital learning environment (DLE) according to the access control matrix.

5. If the voice identification procedure is completed with a negative conclusion, a corresponding entry is made in the event log, and the person who applied for identification is offered to confirm the identity by answering questions in the mobile application, but at the same time, some functions of the DLS for the user may be limited.

6. With the help of a secure hashing function H, the sequence of decimal numbers $\mathcal{A}$ presented in the form of a bit string is expanded to the length of the private key of the corresponding PEP, thus creating a mask $\mu = H(\mathcal{A})$, which is used to modify the user's password:

$$Password_{I+1} = Password_I \oplus \mu, \tag{7}$$

where $Password_I$ та $Password_{I+1}$ is respectively, user passwords in the current and next access sessions to the digital learning environment. The length of the password in bits corresponds to the length of the hash function digest.

In the next session of interaction with the DLS, the modified user password will be applied, and this improves the security of copying the key, which is stored on a medium such as flash memory, in compliance with the rules that must be defined by regulatory documents on the security system.

Taking into account the comments made and the established rules of information protection in information and communication systems [28], the basic elements of the architecture of the distance learning system, which works according to the "client-server" principle and takes into account the principles of the concept of Zero Trust, should include the following protection mechanisms (Fig. 2)

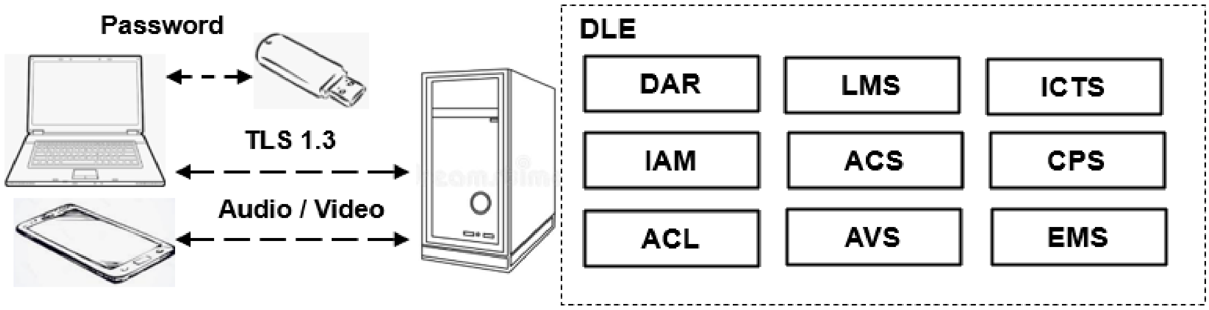

Figure 2: Basic elements of the architecture of the distance learning system based on the concept of Zero Trust

The following abbreviations and designations are used in Fig. 2:

- Identity and Authentication Management (IAM).
- Access Control System (ACS).
- Access Control List (ACL).
- AntiVirus System (AVS).
- A Cryptographic Protection System (CPS) is a cryptographic protection system that provides key management, the generation of initial passwords for new users during their initialization, the formation of MAC codes, and file encryption.
- Database of Audio References (DAR) is a database of voice standards of DLS users.
- Event Management System (EMS) is an event management system including registration.
- Integrity Control and Testing System (ICTS) is the integrity control system and protection system testing.
- Transport Layer Security (TLS 1.3) is a transport layer protection protocol.

To ensure the transparency of the proposed solution, mainly the elements corresponding to the constructed threat model are shown in Fig. 2 not including some other important components that are typical for any protection systems, for example, a system for creating backup copies of a digital learning environment.

5. Conclusions and Further Research

Within the framework of the research, based on the concept of Zero Trust a model of threats to the DSL was developed, and practical aspects of improving the information security policy were determined, taking into account the requirements of the law and the concept of Zero Trust. Also, the mechanisms to ensure the protection of information resources of the DSL were proposed.

It seems appropriate to focus further research on the definition of safety protocols and interfaces of the components of the protection system and on modeling its behavior in conditions of random failures and failures of tools and equipment.

6. References

[1] O. Semenog, et al., Formation of Media Educational Skills of a Future Teacher in the Professional Training, Revista Romaneasca Pentru Educatie Multidimensionala, 12(3) (2020) 219–245.

[2] I. Likarchuk, On the Organization of Distance Learning. URL: https://ru.osvita.ua/blogs/71808/

[3] On the Protection of Information in Information and Telecommunication systems, No. 80/94-VR: Law of Ukraine. Information of the Verkhovna Rada of Ukraine. 1994. No. 31. Art. 286.

[4] On the Protection of Personal Data, No. 2297-VI: Law of Ukraine. Information of the Verkhovna Rada of Ukraine, 2010, No. 34, Art. 481.

[5] On the Basic Principles of Ensuring Cyber Security of Ukraine, No. 2163-VIII: Law of Ukraine. Verkhovna Rada information. 2017. No. 45. Art. 403.

[6] H. Hulak, et al. Formation of requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923 (2021) 137–142.

[7] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[8] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[9] V. Buhas, et al., Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, no. 2 (2021) 273–281.

[10] S. Sysoeva, K. Osadcha, Status, Technologies and Prospects of Distance Learning in Higher Education of Ukraine. Information Technologies and Teaching Aids, 70(2) (2019) 271–284.

[11] H. Hulak, Methodological Principles of Construction of Guaranteed Secure Information Systems for Distance Learning of Higher Education Institutions, Mathematical Machines and Systems, 4 (2020) 148–162.

[12] D. Turnbull, R. Chugh, J. Luck, An Overview of the Common Elements of Learning Management System Policies in Higher Education Institutions, Techtrends, 66(5) (2022) 855–867.

[13] A. Adedoyin, et al., Design and Implementation of an Online Teaching and Learning Management System. February 2023, FUDMA J. Sci. 7(1) (2023) 148–155.

[14] NIST Special publication 800-63 Digital Identity Guidelines. doi: 10.6028/NIST.SP.800-63-3

[15] DSTU ISO/IEC 27001:2015, Information Technologies. Methods of Protecting the Information Security Management System. Requirements, Technical Committee on Standardization “Information Technologies” 2015.

[16] DSTU ISO/IEC TR 13335-2:2003, Information Technologies. Information Technology (IT) Security Management Guidelines. Part 2. Security Management and Planning, Information Technology Technical Committee on Standardization 2003.

[17] ND TZI 3.7-003-2005, The Procedure for Carrying Out Work on the Creation of a Comprehensive Information Protection System in the Information and Telecommunications System, DSTSZI SB of Ukraine 2005.

[18] P. Cichonski, et al., Information Security Incident Response Teams: An Overview, National Institute of Standards and Technology (NIST) Special Publication 800-61, Rev. 2, Computer Security Incident Handling Guide, 2012. doi:10.6028/NIST.SP.800-61r2

[19] M. Buckbee, What Is Zero Trust? Architecture and Security Guide. URL: https://www.varonis.com/blog/what-is-zero-trust

[20] S. Han, Security Policy Deploying System for Zero Trust Environment, in book Big Data, Cloud Computing, and Data Science Engineering, 2023, 83–93, doi:10.1007/978-3-031-19608-9_7

[21] Security and Privacy. URL:https://moodle.com/security-privacy/

[22] Security is top of mind for Blackboard, Blackboard, 2023. URL:https://help.blackboard.com/Learn/Administrator/SaaS/Security#:~:text=Blackboard%20uses%20several%20methods%20to,analysis%2C%20and%20manual%20penetration%20testing.

[23] Our Security Policies at Canvas, Canvas, 2023. URL:https://canvasapp.com/security

[24] Security and Regulatory Compliance, Google Classroom, 2023. URL: https://www.ccn-cert.cni.es/informes/abstracts/5168-google-classroom-security-and-regulatory-compliance/file.html

[25] What are Khan Academy’s security practices?, Khan Academy, 2023. URL: https://support.khanacademy.org/hc/en-us/articles/4406593496077-What-are-Khan-Academy-s-security-practices-

[26] On Education, No. 2145-VIII: Law of Ukraine. Verkhovna Rada information. 2017. No. 38–39. Art. 380.

[27] On Higher Education, No. 1556-VII: Law of Ukraine. Verkhovna Rada information. 2014. No. 37–38. Art. 2004.

[28] On the Approval of the Rules for Ensuring the Protection of Information in Information, Electronic Communication and Information and Communication Systems: Decree of the Cabinet of Ministers of Ukraine dated March 29, 2006, No. 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text

[29] M. Burmester, et al., A Structured ElGamal-Type Multisignature Scheme. Public Key Cryptography. PKC 2000. Lecture Notes in Computer Science, 1751 (2000) 466–483. doi:10.1007/978-3-540-46588-1_31

[30] A. Kuznetsov, O. Korol, V. Bosko. A Model for Generating Message Authentication Codes using Universal Hashing Functions, Information Processing Systems 3(93) (2011) 117–125.

[31] R. Oliynykov, et al., Results of Ukrainian National Public Cryptographic Competition, Tatra Mountains Mathematical Publications 47(1) (2009) 99-113.

[32] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II-2021), 3188 (2021) 197–206.

[33] H. Hulak, et al., Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning, Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS’2021), 2923 (2021) 222–233.

[34] T. Kovalyuk, A. Shevchenko, N. Kobets, Multibiometric Identification of a Student based on his Voice and Visual Biometric Indicators in the Process of Distance Education, Digital Platform: Information Technologies in the Sociocultural Sphere 5(1) (2022) 90–102.

[35] O. Yudin, R. Zyubina, Analysis of Modern Systems and Methods of Audio Signal Recognition in Identification and Verification Tasks, Problems of informatization and management 3(59) (2017) 75–79.