# Development of information security policy for distance education services using risk assessment method

Orest Polotai[1,†], Bohdana Polotai[2,†], Oleh Harasymchuk[3,*,†] and Andriy Ivanusa[1,†]

[1]Lviv State University of Life Safety, Kleparivska Str., 35, Lviv, 79000, Ukraine
[2]Lviv University of Trade and Economics, Tugan-Baranovskogo Str., 10, Lviv, 79005, Ukraine
[3]Lviv Polytechnic National University, Stepan Bandera Str.,12, Lviv, 79000, Ukraine

## Abstract

The paper is devoted to the development of organizational measures of information security pol-icy when providing distance education services. For this purpose, the experience of organizing distance education by higher education institutions in modern conditions is analyzed. The subject of the study is the modular object-oriented dynamic e-learning system Moodle, as a popular tool for providing distance education services. The scheme of structural elements of the e-learning sys-tem Moodle is shown and the classification of methods and means of ensuring information secu-rity in an electronic course, as the main component of the e-learning system, is given. A scheme-process of management and assessment of information security risks when providing dis-tance education services is proposed. Based on it, a model of internal and external violators of in-formation security of a distance education service is built with a ranking of the level of damage of each violator, as well as a model of specific threats to information security when providing dis-tance education services. A set of rules for the information security policy of an electronic course, as an environment for providing distance education services, is proposed.

## Keywords

information security, distance education service, e-learning, e-course, information security risks

## 1. Introduction

Distance education services [1] are a learning system built using information and telecommunication technologies, which are widely used by students and teachers in modern conditions. The e-learning system [2] allows for the teaching of educational courses, receiving information and communication between teachers and students.

Distance education services are used in developed countries of the world, as they provide the following advantages [3, 4, 5]:

- Access anywhere and at any time;
- Allows the use of various and modern means and methods of learning (text, video, tests, etc.);
- Provides the opportunity for students to communicate with each other and with teachers online outside the classroom;
- Simultaneous access of a large number of students to many sources of educa-tional information;
- Application in the educational process of new achievements of information technologies that contribute to the entry of a person into the global information space;
- Use of specialized forms of quality control of educational achievements. applications—from individual users to large corporate and government entities. Key aspects of this approach include

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

orest.polotaj@gmail.com (O. Polotai); bogdanaf@ukr.net (B. Polotai); oleh.i.harasymchuk@edu.lpnu.ua (O. Harasymchuk); ivaaanusa@gmail.com (A. Ivanusa)
0000-0003-4593-8601 (O. Polotai); 0000-0003-1600-2724 (B. Polotai); 0000-0002-8742-8872 (O. Harasymchuk); 0000-0001-9141-8039 (A. Ivanusa)

**Table 1**
Comparative Capabilities of Functions SPDES.

| Criteria | Moodle | Lotus Learning Space | REDCLASS | Blackboard Learning System | GEKADEM |
|---|---|---|---|---|---|
| User activity monitoring | + | + | + | + | + |
| Help | + | + | +- | + | + |
| Management | + | + | + | + | + |
| Automated testing and evaluation | + | + | + | + | + |
| Support | + | + | + | + | + |
| Security administration | + | + | + | + | + |
| Compatibility with educational institution standards | + | - | + | + | + |
| Distribution conditions | Free | Paid | Paid | Paid | Conditionally free |

the protection of biometric data privacy, the reliability of signature generation algorithms, and ensuring compatibility with existing electronic signature standards and Public Key Infrastructure (PKI) [6, 7, 8, 9].

The first e-learning institution - the Berlin Institute for the Study of Foreign Languages, was created by foreign language teachers of the University of Berlin, Ch. Toussaint and G. Lanchensteidt in 1856. Education there took place by correspondence, which was called "corresponding learning".

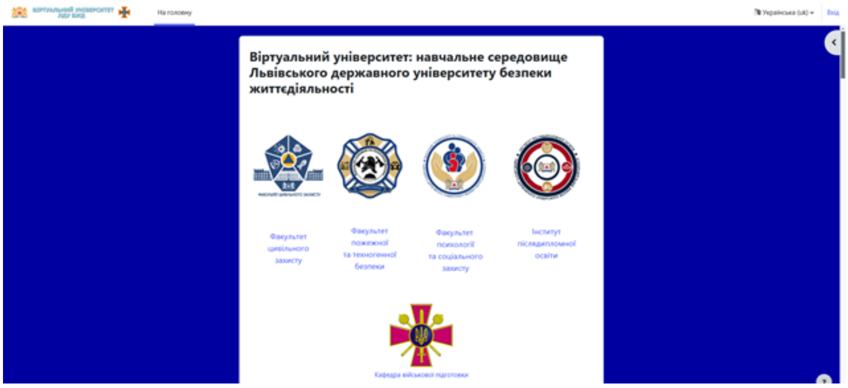
At present, significant experience has already been accumulated abroad in the implementation of systems for providing distance educational services (SPDES). In the USA, about 1 million people study in the distance education system, for which public television is used. Canadian e-learning universities provide training courses on tradi-tional media. Courses usually consist of printed materials and include methodological guidelines, a selection of articles for additional education, instructions for conducting laboratory exercises, etc. Only some universities use the capabilities of computer-based learning and e-mail as part of the education system. The Open University of Great Britain has established itself as a world leader in non-traditional education.

Following the example of the Open University of Great Britain, educational insti-tutions of a similar type were created in Canada, Austria, Spain, Pakistan, the Nether-lands, Turkey, India, Israel, etc.

Among the most popular SPDES are the following: Moodle, Lotus Learning Space, REDCLASS, Blackboard Learning System, GEKADEM. Distance education service de-livery systems have a common goal – software support for the distance learning pro-cess, but they have different parameters and capabilities. Table 1 shows the functions and tools that are available or not available in them.

Moodle is the name of a program that allows anyone to master educational mate-rial remotely, using the Internet. This program provides students with access to nu-merous electronic courses. Many educational sites operate on the basis of the Moodle system [10, 11, 12, 13], which use this system as a shell for providing distance educational ser-vices. This indicates that this type of service is developing dynamically throughout the world. Some universities already have a well-established system for providing distance educational services, others are just beginning to develop it. The advantage of the Moodle platform is the fact that since 1999, it has been repeatedly modified and sup-plemented with new solutions and tools. The platform software is written in PHP using free publicly available databases (MySQL, PostgreSQL). The Moodle platform can be installed on any operating system (MS Windows, Unix, Linux).

Taking into account the above, we note that the Moodle system can be used not only to organize the provision of distance education services in higher education in-stitutions, but also to support the traditional educational process of higher education using a blended (combined) model.



Віртуальний університет: навчальне середовище Львівського державного університету безпеки життєдіяльності

Віртуальний університет ЛДУ БЖД
На головну
Українська (uk)
Вхід
Факультет цивільного захисту
Факультет пожежної та техногенної безпеки
Факультет психології та соціального захисту
Інститут післядипломної освіти
Кафедра військової підготовки

**Figure 1:** The main window of the SPDES.

## 2. Materials and methods

### 2.1. Location of the study

The research was conducted on the basis of SPDES Lviv State University of Life Safety "Virtual University" [14], which operates on the Moodle platform (Figure 1).

SPDES, shown in Figure 1, runs on a server supported by cloud services and ad-ministered by the Information Technology Department and the Department of Infor-mation Security Management of the Lviv State University of Life Safety. It is worth noting that a similar system of this type operates at the Lviv Polytechnic National University and the Lviv University of Trade and Economics, therefore all the results of the research can be applied in these higher education institutions.

### 2.2. Software

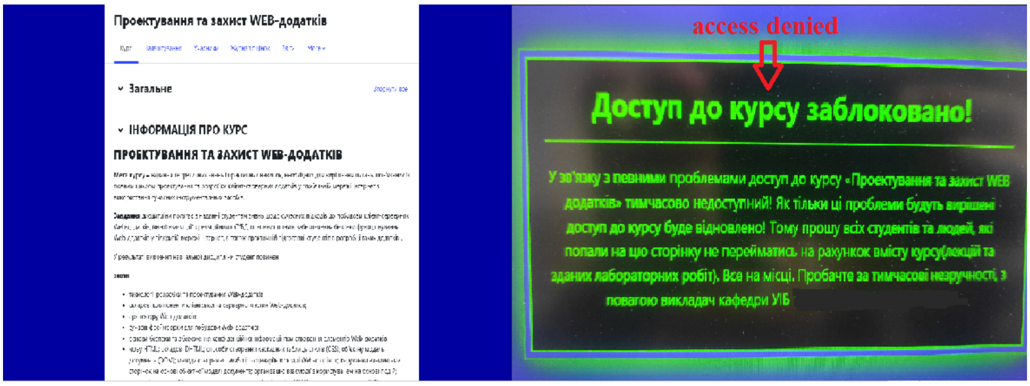
A stored xss cyberattack was experimentally carried out on the SPDES system under study, using an account with the rights of a “teacher”. The cyberattack was carried out by employees of the department where the distance education services system is maintained, in order to identify vulnerable entry points in the Moodle system.

XSS (Cross-Site Scripting) [15] is a type of web application vulnerability that allows attackers to inject malicious JavaScript code into the page that the user is viewing. This code can be used to steal confidential data, redirect users to phishing sites, and perform other malicious actions.

The XSS vulnerability was first discovered in the late 1990s, when web applications were becoming more widespread. Over time, such attacks have become more sophisticated, and today they remain one of the main methods of cyberattacks. Along with the development of technologies and web standards, such as HTML, CSS and JavaScript, methods of protection against XSS have also developed. However, the threat remains relevant and requires constant attention and updating of protection measures. The fragment of malicious code for carrying out a stored xss attack is based on the following Algorithm 1.

Algorithm 1. Using a stored xss attack to embed malicious code into the SPDES body

```
<font color=red >
<div id="header"></div>
<script>
var a=window.document.cookie;console.log(a);
var img=document.createElement("img");
img.src="https://your_malware_server_blablabla.com/steal_session.php
session="+btoa(a);
var src=document.getElementById("header");
src.appendChild(img);
console.log(btoa(a));
```



Проектування та захист WEB-додатків

Курс Налаштування Учасники Журнал оцінок Звіти Більше

Загальне Згорнути все

ІНФОРМАЦІЯ ПРО КУРС

ПРОЕКТУВАННЯ ТА ЗАХИСТ WEB-ДОДАТКІВ

Мета курсу [illegible]

Завдання дисципліни [illegible]

У результаті вивчення навчальної дисципліни студент повинен

знати:

- технології розробки та проектування Web-додатків
- складові компоненти клієнтської та серверної частини Web-додатків
- архітектуру Web-додатків
- сучасні фреймворки для побудови Web-додатків
- основи безпеки та забезпечення конфіденційної інформації при створенні елементів Web-додатків
- мову HTML; складові DHTML; способи створення каскадних таблиць стилів (CSS); об'єктну модель документа (DOM); [illegible]

Доступ до курсу заблоковано!

У зв'язку з певними проблемами доступ до курсу «Проектування та захист WEB додатків» тимчасово недоступний! Як тільки ці проблеми будуть вирішені доступ до курсу буде відновлено! Тому прошу всіх студентів та людей, які попали на цю сторінку не перейматись на рахунок вмісту курсу(лекцій та зданих лабораторних робіт). Все на місці. Пробачте за тимчасові незручності, з повагою викладач кафедри УІБ [redacted]

**Figure 2:** System status before and after the cyberattack.

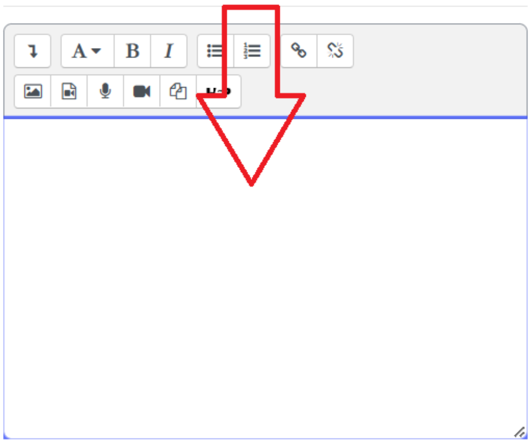


**Figure 3:** Entry point into the system for implementing a cyberattack.

```
console.log(atob(btoa(a)));
</script>
```

The result of this attack is blocking access to course materials, i.e. the property of information - accessibility - is violated, while the integrity of the materials is not violated (Figure 2).

The implementation of this attack turned out to be possible through the resource or text data loading field, where you can load a bat.file with the text of algorithm 1 and run it for execution (Figure 3).

It is worth noting that the implementation of such a cyberattack can only be carried out from an account not lower than the "teacher" level. It was experimentally found that users with lower rights, such as "student", will not be able to implement such an attack, since the Moodle distance education service system filters downloaded files. But on the other hand, a user at the "student" level can intercept an IP packet with the credentials of users with higher privileges and implement such an attack. Therefore, there is a need to investigate SPDES information security violators, the threats they can implement and assess the risks of implementing the corresponding threats and the level of damage that may arise as a result.

## 3. Results

A large number of works are devoted to issues of information security and cybersecurity in various fields [16, 17, 18, 19]. The problem of standardization in this direction is also relevant. A large number of works are devoted to issues of information security and cybersecurity in various fields [20, 21]. Information security is understood as "the state of information security in which its confidentiality, availability and integrity are ensured" [22]. In this case:

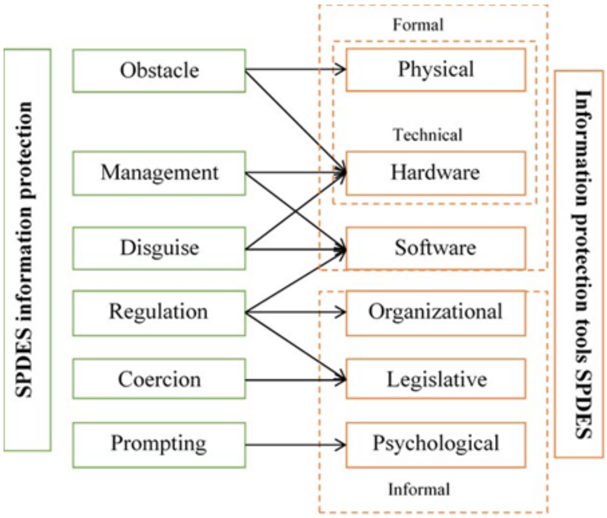


**Figure 4:** Classification of means of ensuring the security of information processing processes in systems for providing distance educational services SPDES.

1. Confidentiality is ensuring access to information only to authorized users.
2. Integrity is ensuring the reliability and completeness of information and methods of its processing.
3. Availability is ensuring access to information to authorized users as necessary.

The complex nature of the protection problem suggests that a combination of legislative, organizational and software-technical measures is necessary to solve it.

Knowledge of possible threats, as well as vulnerabilities of the information system, is necessary in order to choose the most effective means of ensuring security.

One of the most dangerous and frequent are unintentional errors of users, opera-tors, system administrators and other persons servicing information systems. Some-times such errors lead to direct damage (incorrectly entered data, an error in the pro-gram that caused the system to stop or collapse). Sometimes they create weaknesses (most often due to administrative errors) that can be exploited by attackers.

Theft and falsification are in second place in terms of damage. In most cases, the culprits were full-time employees of organizations who were perfectly familiar with the operating mode and protective measures.

A key stage in building a reliable information system is the development of a se-curity policy [23]. There are several definitions of this concept. Here are some of them. Security policy is a set of guiding principles, rules, procedures and practical tech-niques in the field of security that regulate the management, protection and distribu-tion of valuable information [22, 24]. The key point of the security policy for SPDES is the methods and means of ensuring information protection and their analysis.

Graphically, this classification is presented in Figure 4.

The SPDES information security policy for users with the "student" role should be available at each educational institution and specified in the form of information security rules. Necessary measures to protect SPDES from intentional and unintentional actions of students: administrator control, personalization and restriction of access to critical resources, control and response to unauthorized actions of software protection tools.

The main goal of the SPDES security policy is to ensure that users with the "student" role comply with information security rules that prevent or minimize the harm they can cause by their actions. This goal is implemented through organizational, software, hardware, and educational measures.

Organizational measures include the development, implementation, and monitoring of the implementation of the SPDES information security system security policy for student users. Implementation monitoring is the responsibility of the administrator.

The hardware and software of the adopted security policy are implemented through a user access

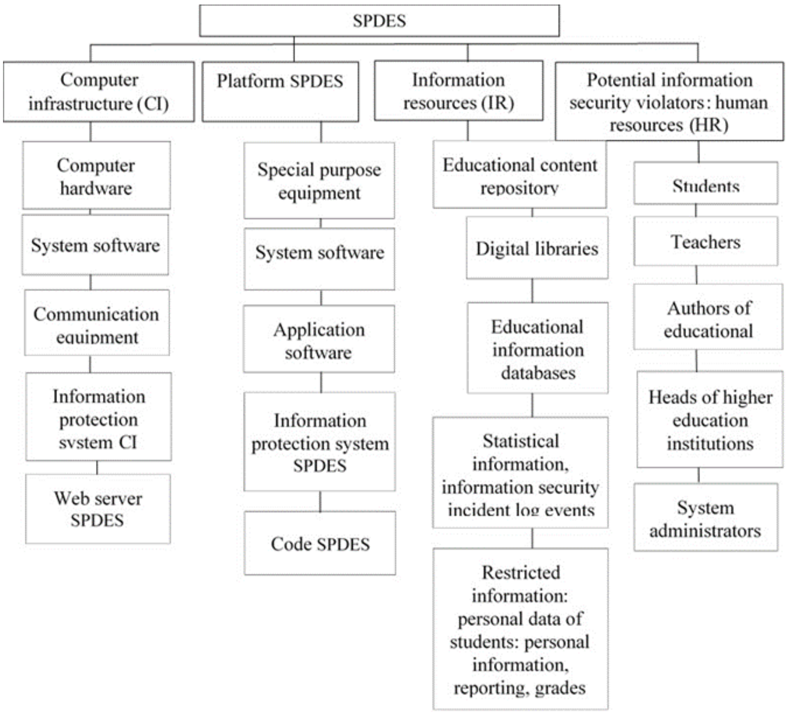

SPDES
Computer infrastructure (CI)
Platform SPDES
Information resources (IR)
Potential information security violators: human resources (HR)
Computer hardware
System software
Communication equipment
Information protection system CI
Web server SPDES
Special purpose equipment
System software
Application software
Information protection system SPDES
Code SPDES
Educational content repository
Digital libraries
Educational information databases
Statistical information, information security incident log events
Restricted information: personal data of students: personal information, reporting, grades
Students
Teachers
Authors of educational
Heads of higher education institutions
System administrators

**Figure 5:** Architecture SPDES.

management system to resources, which includes user identification and authentication, resource access control, logging and auditing of user actions [25, 26, 27]. The hardware and software must guarantee the protection of critical components of the SPDES software (Figure 5) from unauthorized and erroneous user actions.

In Figure 5, SPDES is considered as a scalable system that can operate on a separate computer, in local and/or global networks in Web, GRID and cloud environments.

The purpose of the computer infrastructure is to provide computing resources to support the operation of SPDES. It includes computer hardware, system software, communication equipment and the CI information protection system.

The SPDES platform includes a set of software and hardware that form an appropriate electronic learning environment using information resources and SPDES security policy mechanisms, special-purpose equipment, SPDES system and application software, and the SPDES platform information protection system.

Information resources include the main content of SPDES, including information with limited access, such as a database with system user credentials.

SPDES human resources unite all participants in the educational process who receive and provide educational services, as well as support the functioning of SPDES. Human resources are the most critical factor in the implementation of information security threats.

Each component of the SPDES architecture has its own vulnerabilities and the threats they cause

$$< CI + Platfom + IR + HR >= ISTh, \quad (1)$$

where ISTh is information security threats.

To describe specific threats, we will build an information security threat model SPDES, in which we will indicate the name of the threat, its description, and the components of the SPDES architecture vulnerable to it (Table 2).

As can be seen from the Table 2, most of the specific threats arise at the SPDES platform level. Critical components from the point of view of information protection are administrative systems, training repository, assessment system, communication module.

**Table 2**
ISTh SPDES Model.

| ISTh | Description | Vulnerable component | What does it affect? |
|---|---|---|---|
| Fake content | An attacker can gain unauthorized access to the system and upload fake content if SPDES has vulnerabilities in identification, authentication, and authorization mechanisms | Administrative System, Authoring System | Integrity |
| The exam can be reviewed before the exam date | An attacker can gain unauthorized access to the system and view uploaded exams before the exam date if SPDES has vulnerabilities in identification, authentication, authorization, and confidentiality mechanisms | Administrative system, Learning Repository | Privacy |
| The exam can be deleted | An attacker can gain unauthorized ccess to the system and delete downloaded exam files if SPDES has vulnerabilities in identification, authentication, authorization, integrity, and availability mechanisms | Administrative system, Learning Repository | Integrity, accessibility |
| The exam may be taken by another person | A student may knowingly disclose their identification and authentication data to an unauthorized person who may take the exam instead of the student | Evaluation system | Reliability, confidentiality |
| Exam date change | An attacker can gain unauthorized ccess to the system and change the exam date if the SPDES has vulnerabilities in the integrity mechanism | Administrative system, assessment system | Accessibility, reliability |
| Unauthorized interception of the result | An attacker can gain unauthorized access to the system, intercept other students' results, and present them as their own work | Communication module, assessment system | Privacy |
| Unauthorized access to educational content | An attacker can use "holes" in the PDES security system for unauthorized access to educational content that the does not have the right to access | Administrative system, learning repository | Confidentiality, integrity, availability |
| Unauthorized access to code | An attacker, using system vulnerabilities, embeds malicious code into the system code structure and thus blocks the system from working | IR | Accessibility |
| Threats associated with technical and software failures of equipment and operating systems |  | IR administrative system, learning repository | Confidentiality, privacy, accessibility |

Let us consider in more detail human resources HR, among which there may be potential attackers - violators of SPDES information security.

A violator is a person who, by mistake, due to ignorance, purposefully, with malicious intent or without it, using various capabilities, methods and means, attempted to perform operations that led to or may lead to a violation of the properties of information defined by the security policy [26].

The goal of the intruder may be:

- Obtaining the necessary information in the required volume;

- Being able to make changes to information flows in accordance with their intentions;
- Causing damage by destroying material and information values.

Violators are divided into two main groups: external and internal. Among internal intruders, the following can be distinguished:

- system users;
- personnel servicing technical equipment;
- employees of software development and maintenance departments;
- security service employees;
- managers of various levels and job hierarchy.

Among external intruders, the following can be distinguished:

- clients (representatives of organizations, citizens);
- visitors (invited for any reason);
- hackers;
- persons who accidentally or intentionally violated the access regime (without the purpose of violating security);
- any persons outside the controlled area.

Each offender can be described by a model using certain indicators, which together form a detailed description of him with the level of threats he can implement

$$\text{ISB SPDES} = M + Q + O + T + P \to L, \tag{2}$$

where ISB - Information security breacher; M – motive; Q – qualification; O – opportunities; T – time; P – place; L - losses.

To minimize and prevent negative actions, it is proposed to introduce the SPDES information security risk assessment process model (Figure 6).

Let's consider in more detail the SPDES information security threat identification model-scheme (Figure 7).

All SPDES information security threats and violators acting as their sources should be analyzed by an expert group using the brainstorming method. The result of the expert group's actions is the creation of a database of information security threats.

Similarly, we will present a model-scheme for determining the level of damage L when carrying out an attack by the SPDES information security violators described above (Figure 8).

The determination of the level of damage L when carrying out an attack by the above-described SPDES information security violators is also carried out by an expert group using the brainstorming method. In this case, the expert group must include specialists in the field of distance education services.

So, in summary, we can offer a generalized scheme for establishing the values of information security risks in the provision of distance education services using SPDES (Figure 9).

Let's consider each component of the ISB model. The model of the offender by the motive of the offender is shown in Table 3. Four main motives for violations can be distinguished:

- irresponsibility (losses – 1);
- self-assertion (losses – 2);
- self-interest (losses – 3);
- professional duty (losses – 4).

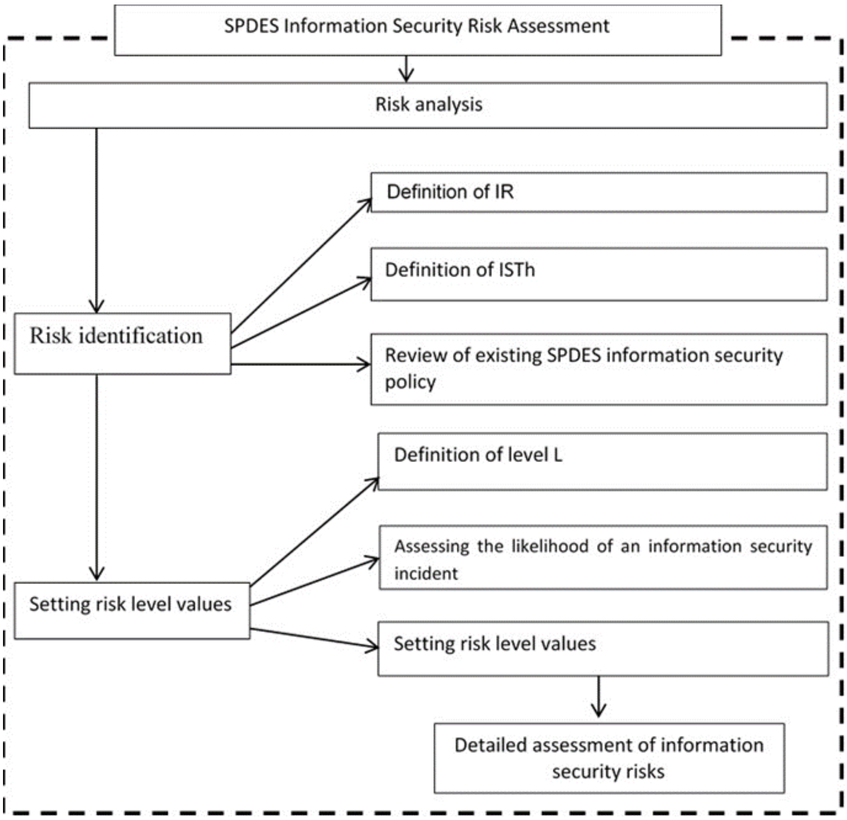

SPDES Information Security Risk Assessment
Risk analysis
Definition of IR
Definition of ISTh
Risk identification
Review of existing SPDES information security policy
Definition of level L
Assessing the likelihood of an information security incident
Setting risk level values
Setting risk level values
Detailed assessment of information security risks

**Figure 6:** SPDES information security risk assessment process model-diagram.

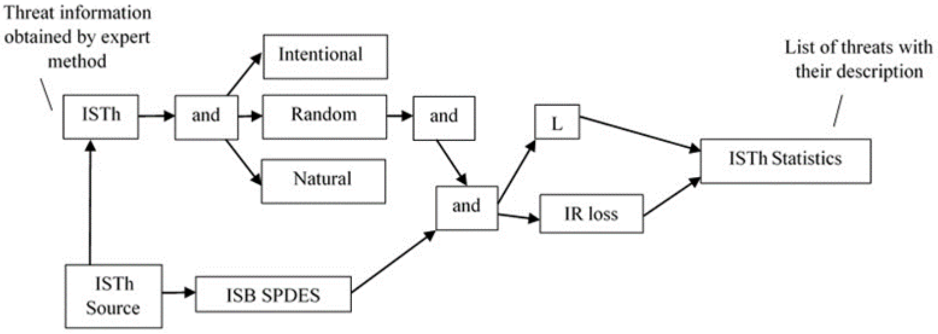

Threat information obtained by expert method
ISTh
and
Intentional
Random
Natural
and
and
L
IR loss
ISTh Statistics
List of threats with their description
ISTh Source
ISB SPDES

**Figure 7:** SPDES information security threat identification model-scheme.

In the case of irresponsible violations, the user intentionally or accidentally performs destructive actions that are not associated with malicious intent. In most cases, this is a consequence of incompetence or negligence. Some users consider gaining access to system data sets to be a significant success, starting a kind of game for the sake of self-affirmation either in their own eyes or in the eyes of colleagues [27, 28, 29].

A SPDES security breach can be caused by the self-interest of the SPDES user. In this case, he will purposefully try to overcome the protection system for unauthorized access to information in SPDES.

The level of threats is an assessment of the possible damage that an attacker can cause, provided that the appropriate characteristics are present. The level of damage is characterized by the following categories: 1 - insignificant; 2 - acceptable; 3 - average; 4 - very significant.

The model of the attacker by qualification features is shown in Table 4.

All attackers can be classified by the level of awareness:

- knows the functional features of SPDES, the main patterns of forming data arrays and streams of

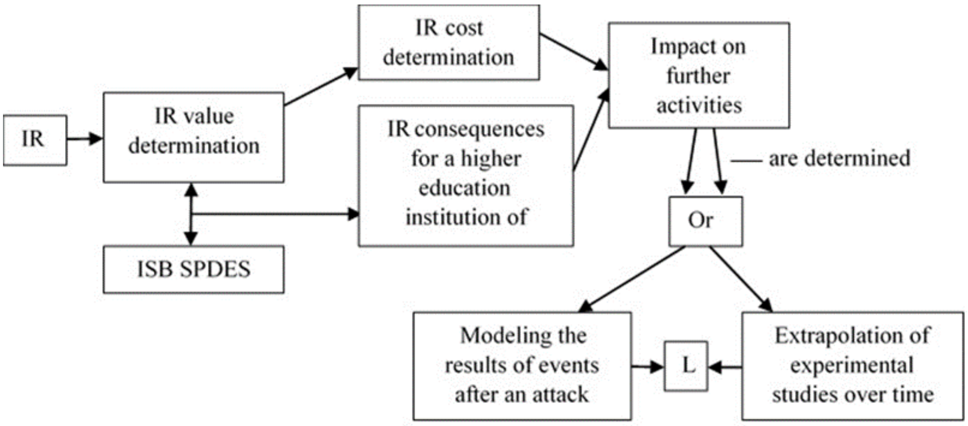

IR
IR value determination
ISB SPDES
IR cost determination
IR consequences for a higher education institution of
Impact on further activities
— are determined
Or
Modeling the results of events after an attack
L
Extrapolation of experimental studies over time

**Figure 8:** SPDES model-scheme for determining the level of losses L.

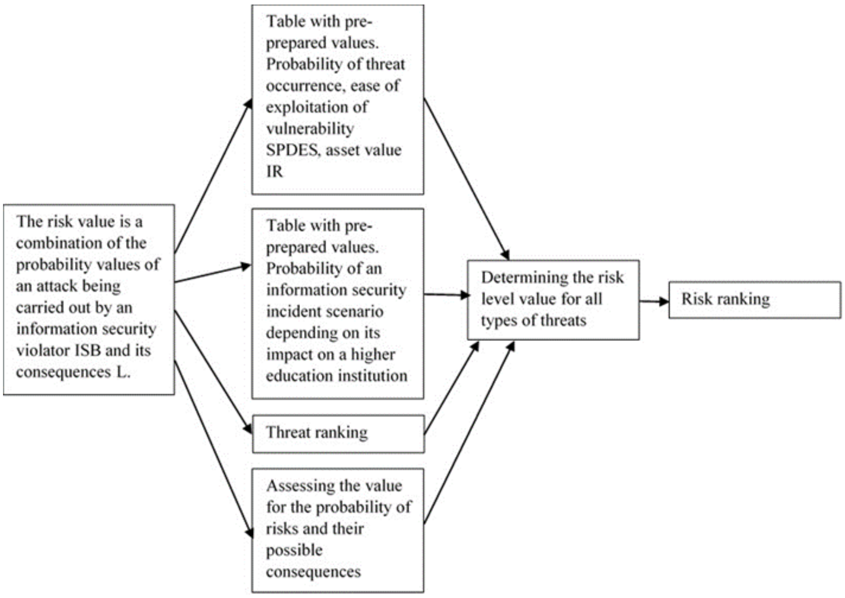

The risk value is a combination of the probability values of an attack being carried out by an information security violator ISB and its consequences L.
Table with pre-prepared values. Probability of threat occurrence, ease of exploitation of vulnerability SPDES, asset value IR
Table with pre-prepared values. Probability of an information security incident scenario depending on its impact on a higher education institution
Threat ranking
Assessing the value for the probability of risks and their possible consequences
Determining the risk level value for all types of threats
Risk ranking

**Figure 9:** SPDES scheme for establishing information security risk values.

requests to them in it, knows how to use standard tools; losses - 1;

- has a high level of knowledge and experience in working with the technical means of the system and their maintenance; losses - 2;
- has a high level of knowledge in the field of programming and computing, design and operation of automated information systems; losses - 2;
- knows the structure, functions and mechanism of action of protection tools, their strengths and weaknesses; losses - 3.

The model of the offender by capabilities is shown in Table 5. By the level of capabilities, methods and means used:

- uses only agent methods of obtaining information; losses – 1;
- uses passive means (technical means of interception without modification of system components); losses – 2;
- uses only standard means and shortcomings of the protection system to overcome it (unauthorized actions using permitted means), as well as compact magnetic media that can be secretly carried through security posts; losses – 3;

**Table 3**
Information Security Breach Model Based on the Breacher's Motive.

| Violator category or External Infringer Model | M | L |
|---|---|---|
| Technical staff (technical administrator) | M1, M2, M4 | 1+2+4=7 |
| Personnel servicing technical equipment (main administrator) | M1, M2, M4 | 1+2+4=7 |
| Personnel servicing technical equipment (educational department administrator) | M3, M4 | 3+4=7 |
| SPDES users (head of department) | M1, M3 | 1+3=4 |
| SPDES users (head of faculty) | M1, M3 | 1+3=4 |
| SPDES users (teachers) | M1, M3 | 1+3=4 |
| SPDES users (students) | M1, M3 | 1+3=4 |
| Managers of different levels of job hierarchy (SPDES program administrator) | M2, M3, M4 | 2+3+4=9 |
| Employees of software development and support departments (security department employees) | M1, M3, M4 | 1+3+4=8 |
| Visitors | M2, M3 | 2+3=5 |
| Competitors | M2, M3 | 2+3=5 |
| Hackers | M2, M3 | 2+3=5 |

**Table 4**
Model of Information Security Violator by Qualification Criteria.

| Violator category or External Infringer Model | Q | L |
|---|---|---|
| Technical staff (technical administrator) | Q1, Q2, Q4 | 1+2+3=6 |
| Personnel servicing technical equipment (main administrator) | Q1, Q2, Q3, Q4 | 1+2+2+3=8 |
| Personnel servicing technical equipment (educational department administrator) | Q1, Q4 | 1+3=4 |
| SPDES users (head of department) | Q1, Q4 | 1+3=4 |
| SPDES users (head of faculty) | Q1, Q4 | 1+3=4 |
| SPDES users (teachers) | Q1, Q4 | 1+3=4 |
| SPDES users (students) | Q1, Q4 | 1+3=4 |
| Managers of different levels of job hierarchy (SPDES program administrator) | Q1, Q4 | 1+3=4 |
| Employees of software development and support departments (security department employees) | Q1, Q2, Q3, Q4 | 1+2+2+3=8 |
| Visitors | Q2, Q3 | 2+2=4 |
| Competitors | Q2, Q3, Q4 | 2+2+3=7 |
| Hackers | Q2, Q3 | 2+2=4 |

- uses methods and means of active influence (modification and connection of additional technical means, connection to data transmission channels, implementation of software bookmarks and use of special instrumental and technological programs); losses – 3.

The model of the attacker by the time of action is shown in Table 6.
By the time of action, the attackers are classified by the time when they can carry out their attack:

- during the operation process (during the operation of the SPDES components); losses – 3;
- during the period of inactivity of the system (during non-working hours, during planned breaks in its operation, breaks for maintenance and repairs, etc.); losses – 2;
- both during the operation process and during the period of inactivity of SPDES; losses – 4.

**Table 5**
Model of an Information Security Violator by Capabilities and Characteristics.

| Violator category or External Infringer Model | O | L |
|---|---|---|
| Technical staff (technical administrator) | O3, O4 | 3+3=6 |
| Personnel servicing technical equipment (main administrator) | O3, O4 | 3+3=6 |
| Personnel servicing technical equipment (educational department administrator) | O4 | 3 |
| SPDES users (head of department) | O2 | 2 |
| SPDES users (head of faculty) | O2 | 2 |
| SPDES users (teachers) | O1, O2 | 1+2=3 |
| SPDES users (students) | O1, O2 | 1+2=3 |
| Managers of different levels of job hierarchy (SPDES program administrator) | O2 | 2 |
| Employees of software development and support departments (security department employees) | O2 | 2 |
| Visitors | O1, O2 | 1+2=3 |
| Competitors | O1, O4 | 1+3=4 |
| Hackers | O1, O2, O4 | 1+2+3=6 |

**Table 6**
Information Security Breach Model by Time of Action.

| Violator category or External Infringer Model | T | L |
|---|---|---|
| Technical staff (technical administrator) | T1 | 3 |
| Personnel servicing technical equipment (main administrator) | T1, T2, T3 | 3+2+4=9 |
| Personnel servicing technical equipment (educational department administrator) | T1, T2, T3 | 3+2+4=9 |
| SPDES users (head of department) | T1 | 3 |
| SPDES users (head of faculty) | T1 | 3 |
| SPDES users (teachers) | T1 | 3 |
| SPDES users (students) | T1 | 3 |
| Managers of different levels of job hierarchy (SPDES program administrator) | T1, T2, T3 | 3+2+4=9 |
| Employees of software development and support departments (security department employees) | T1, T2, T3 | 3+2+4=9 |
| Visitors | T2 | 2 |
| Competitors | T2 | 2 |
| Hackers | T2 | 2 |

The model of the intruder by location is shown in Table 7.
By time of action, intruders are classified by location from which they can carry out their attack:

- without access to the controlled territory of the organization; losses – 1;
- from the controlled territory without access to buildings and structures; losses – 1;
- inside the premises, but without access to technical means; losses – 2;
- from the workplaces of end users (operators); losses – 2;
- with access to the data zone (databases, archives, etc.); losses – 3;
- with access to the security management zone; losses – 4.

Table 8 shows the aggregated model of the offender.

**Table 7**
Information Security Breach Model at the Scene of Action.

| Violator category or<br>External Infringer Model | P | L |
|---|---|---|
| Technical staff (technical administrator) | P4, P5, P6 | 2+3+4=9 |
| Personnel servicing technical equipment (main administrator) | P4, P5, P6 | 2+3+4=9 |
| Personnel servicing technical equipment (educational department administrator) | P4, P5, P6 | 2+3+4=9 |
| SPDES users (head of department) | P1, P3 | 1+2=3 |
| SPDES users (head of faculty) | P1, P3 | 1+2=3 |
| SPDES users (teachers) | P1, P3 | 1+2=3 |
| SPDES users (students) | P1, P3 | 1+2=3 |
| Managers of different levels of job hierarchy (SPDES program administrator) | P3 | 2 |
| Employees of software development and support departments (security department employees) | P6 | 4 |
| Visitors | P3 | 2 |
| Competitors | P1, P2, P3 | 1+1+2=4 |
| Hackers | P1, P2, P3 | 1+1+2=4 |

**Table 8**
General Table of the Offender Model ISB SPDES.

| Violator category or<br>External Infringer Model | M | Q | O | T | P | L |
|---|---|---|---|---|---|---|
| Technical staff (technical administrator) | 7 | 6 | 6 | 3 | 9 | 31 |
| Personnel servicing technical equipment (main administrator) | 7 | 8 | 6 | 9 | 9 | 39 |
| Personnel servicing technical equipment (educational department administrator) | 7 | 4 | 3 | 9 | 9 | 31 |
| SPDES users (head of department) | 4 | 4 | 2 | 3 | 3 | 16 |
| SPDES users (head of faculty) | 4 | 4 | 2 | 3 | 3 | 16 |
| SPDES users (teachers) | 4 | 4 | 3 | 3 | 3 | 16 |
| SPDES users (students) | 4 | 4 | 3 | 3 | 3 | 16 |
| Managers of different levels of job hierarchy (SPDES program administrator) | 9 | 4 | 2 | 9 | 2 | 26 |
| Employees of software development and support departments (security department employees) | 8 | 8 | 2 | 9 | 4 | 31 |
| Visitors | 5 | 4 | 3 | 2 | 2 | 16 |
| Competitors | 5 | 7 | 4 | 2 | 4 | 22 |
| Hackers | 5 | 4 | 6 | 2 | 4 | 21 |

Figure 10 shows a diagram of SPDES information security violators in terms of the damage they can cause.

Therefore, the main source of SPDES information security breaches is within the information systems themselves, so internal protection should be mandatory for any of them. Table 9 shows the ranking of information security threats risks when providing distance education services using SPDES.

## 4. Discussions

For reliable and secure work with SPDES and the electronic course, which is one of its key elements, it is necessary to adhere to the main login measures of the information security policy:

1. Administrator and teacher users must have a password for their account that meets the password

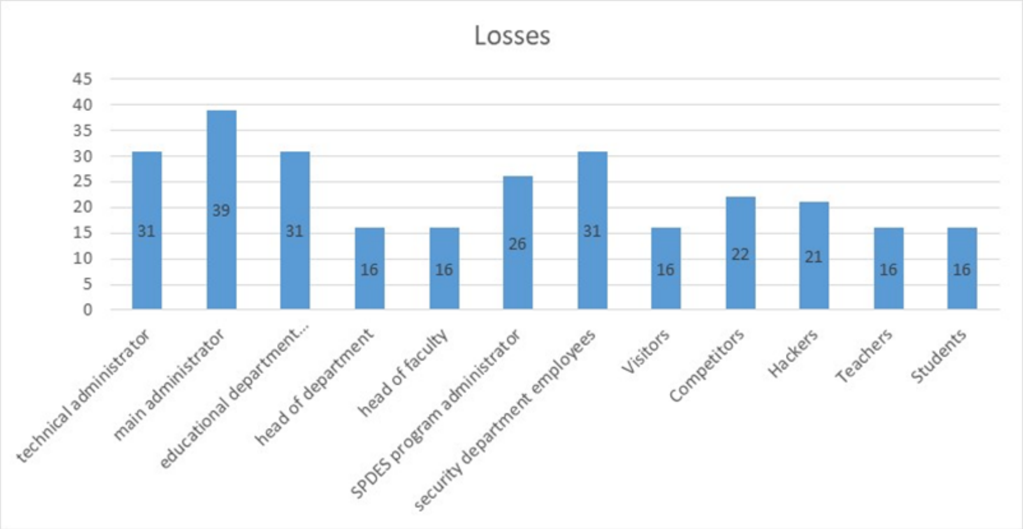


**Figure 10:** Diagram of damages from violators' actions.

**Table 9**
Ranking of Information Security Threats Risks SPDES.

| ISTh | Consequences | The degree of probability of a threat occurring | Risk measure | Ranking of threats in order of decreasing risk decreasing risk from 1 (maximum risk) to 6 (minimum risk) |
|---|---|---|---|---|
| Fake content | 4 | 2 | 8 | 2 |
| The exam can be reviewed before the exam date | 4 | 1 | 4 | 5 |
| The exam can be deleted | 3 | 4 | 12 | 1 |
| The exam may be taken by another person | 3 | 1 | 3 | 4 |
| Exam date change | 1 | 1 | 1 | 6 |
| Unauthorized interception of the result | 4 | 3 | 12 | 1 |
| Threats associated with technical and software failures of equipment and operating systems | 5 | 1 | 5 | 3 |

format requirement as per the password policy.

2. Users such as a student, guest, and authenticated user must have a minimum set of rights to work with the electronic course, that is, the course must be configured in this way.

3. When creating each electronic course in SPDES, it is necessary to configure rights to work with each of its elements.

4. After creating an electronic course, it is imperative to create a backup copy of it.

5. After creating an electronic course, it is necessary to configure the features of user registration for it and be sure to disable the possibility of self-registration for the course.

6. When working with an electronic course in SPDES, the user's personal computer must have activated and updated antivirus software that will protect against unwanted viruses that can damage part of the electronic course.

7. After the end of the training period on the electronic course, the teacher must clear it of old

statistics, reports, delete all completed tasks, and exclude all former users from the course.

8. After cleaning the course, it must be hidden and students must be denied access to it.

## 5. Conclusions

Ensuring information security is one of the most important tasks of organizations in providing distance education services. Speaking about information as a resource of management systems, it can be noted that ensuring its security requires a comprehensive approach that will allow to comprehensively ensure, firstly, integrity, secondly, accessibility, thirdly, confidentiality. The diversity and wide application of SPDES in various spheres of human activity, as well as their dependence on the security of the information resource, enhance the significance and relevance of the SPDES study.

The relevance of the issue of information security of such systems is due to the problems of ensuring integrity, accessibility and confidentiality in parallel with the is-sues of ensuring compatibility, extensibility and scalability of these systems.

It should also be noted that there are commercial and open-source systems. The information security settings of such systems differ somewhat for obvious reasons, but the key points of their administration are the same.

The advantages of commercial software are widely known: for the most part, these are reliable products (especially those that have taken root in the market), with an appropriate level of user support, regular upgrades and new versions.

However, there are also disadvantages. For example, there is a problem of "closed doors" when using systems for providing distance education services on closed plat-forms. First, the source code is not available to the organization's technical support, so even small changes at the user level are not possible. The organization can try to con-tact the manufacturing company if it has suggestions for improvement, but it is very unlikely that its ideas will be implemented in a short period of time, if at all. In addi-tion, the disadvantages include the high cost of any commercial product, regular pay-ments for a license, for increasing the number of users (which is actually a mandatory factor of any network system), and so on.

Open-source systems allow you to solve the same tasks as commercial systems, but at the same time users have the opportunity to refine and adapt a particular sys-tem to their needs and the current educational situation. Most open-source systems are cross-platform solutions and are not tied to specific operating systems or specific Web browsers.

Current trends in the development of OpenSource LCMS are directed towards universalization and increasing the functionality of systems. In terms of their capabili-ties, the most advanced systems are not inferior to commercial analogues, and some even surpass them.

Open-source SPDES allow you to implement the same set of functional capabili-ties as commercial solutions, but with significantly lower economic costs.

Therefore, the analysis and application of SPDES security tools is a priority task for achieving the maximum level of security. These include, in particular, SPDES ad-ministration tools. With their help, thanks to a flexible system of settings, it is possible to ensure maximum privacy for users and confidentiality of information stored in the educational database of the system. To configure the entire system, there is an admin-istrator (in the case of course settings, his role can be performed by a teacher), who needs to:

1. Create accounts and assign them roles. Here you can register, delete and edit ac-counts of system users. There is also a form in which the personal data of this user, his blog, full activity reports, his messages are stored. In the settings, you can assign a role to a user (A role is a set of rights (permissions) defined for the site as a whole, which can be assigned to specific users in a given context).

2. Configure the course. This means the ability to both create a new course and use an existing one, in other words, there is a function of cloning courses and settings. As well as control user access to the system's educational resources.

3. Fill the course with educational materials. The system has a wide variety of mod-ules (course

elements) that can be used to create courses of any type. Depending on the content of the course and the teaching concept, the administrator includes the most suitable elements and resources provided by the system.

4. Administer the learning process. In particular, this function includes timely up-dating and/or deleting accounts, checking the relevance of data (information about users, educational materials) stored in the system. Changing access rights and reas-signing roles for participants in the learning process.

Thus, the administrator is a user with the broadest rights, the main purpose of which is to maintain stable system operation, user management, setting the main system parameters, information security of the course and personal data of users, backups and much more. It is from his thoughtful and, as a result, effective work that the work of the entire SPDES will depend on.

## Declaration on Generative AI

The authors have not employed any Generative AI tools.

## References

[1] W. Oliveira, L. A. M. do Amaral, Distance education as a service system, in: 2019 IEEE World Conference on Engineering Education (EDUNINE), Lima, Peru, 2019, pp. 1–6. doi:10.1109/EDUNINE.2019.8875822.

[2] S. R. Thakkar, H. D. Joshi, E-learning systems: A review, in: 2015 IEEE Seventh International Conference on Technology for Education (T4E), Warangal, India, 2015, pp. 37–40. doi:10.1109/T4E.2015.6.

[3] E. Samsari, N. Palaiologou, G. Nikolaou, The impact of the COVID-19 pandemic in the inclusion of refugee students in Greek schools: Pre-service teachers' views about distance learning, Societies 14 (2024) 60. doi:10.3390/soc14050060.

[4] M. Selim, Distance learning and its effectiveness in improving literacy, education and skills development for remote population and for overcoming the challenges of COVID 19, in: 2020 Sixth International Conference on e-Learning (econf), Sakheer, Bahrain, 2020, pp. 66–71. doi:10.1109/econf51404.2020.9385522.

[5] Wang-Peng, Distance education service system in western underdeveloped regions, in: 2010 International Conference on Optics, Photonics and Energy Engineering (OPEE), Wuhan, China, 2010, pp. 184–186. doi:10.1109/OPEE.2010.5508060.

[6] Y. Wang, L.-J. Zhang, H. Cai, J. Sun, N. Li, Evaluating the quality of distance education services by using modern information technology, in: 2012 IEEE Asia-Pacific Services Computing Conference, Guilin, China, 2012, pp. 192–199. doi:10.1109/APSCC.2012.50.

[7] M. Tunay, A new approach model of e-visual career application in distance education, in: 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2020, pp. 1–7.

[8] V. V. Vyshnivskyi, M. P. Hnidenko, G. I. Haydur, O. O. Ilyin, Organization of distance education. Creation of electronic training courses and electronic tests. Study guide, DUT, Kyiv, 2014.

[9] O. O. Popov, et al., Immersive technology for training and professional development of nuclear power plants personnel, in: Proceedings of the CEUR Workshop, volume 2898, CEUR-WS.org, 2021, pp. 230–254.

[10] L. L. Salekhova, K. S. Grigorieva, T. A. Zinnurov, Using LMS moodle in teaching CLIL: A case study, in: 2019 12th International Conference on Developments in eSystems Engineering (DeSE), Kazan, Russia, 2019, pp. 393–395. doi:10.1109/DeSE.2019.00078.

[11] Y.-C. Chang, J.-W. Li, D.-Y. Huang, A personalized learning service compatible with moodle e-learning management system, Applied Sciences 12 (2022) 3562. doi:10.3390/app12073562.

[12] S. H. Gamage, J. R. Ayres, M. B. Behrend, A systematic review on trends in using moodle for teaching and learning, International Journal of STEM Education 9 (2022) 1–24.

[13] V. Tkachuk, Y. Yechkalo, S. Semerikov, M. Kislova, Y. Hladyr, Using mobile ICT for online learning during COVID-19 lockdown, in: Communications in Computer and Information Science, volume 1308, Springer, 2021, pp. 46–67. doi:10.1007/978-3-030-77592-6_3.

[14] Electronic learning system of the Lviv State University of Life Safety "Virtual university", 2025. URL: https://virt.ldubgd.edu.ua/, accessed: 2025-07-29.

[15] D. Lu, L. Liu, Research on cross-site scripting attack detection technology based on few-shot learning, in: 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2023, pp. 1425–1429. doi:10.1109/ITNEC56291.2023.10082596.

[16] Y. Martseniuk, et al., Universal centralized secret data management for automated public cloud provisioning, in: Cybersecurity Providing in Information and Telecommunication Systems II, 2024, pp. 72–81.

[17] D. Shevchuk, O. Harasymchuk, A. Partyka, N. Korshun, Designing secured services for authentication, authorization, and accounting of users, in: Cybersecurity Providing in Information and Telecommunication Systems II, 2023, pp. 217–225.

[18] Y. Martseniuk, et al., Shadow IT risk analysis in public cloud infrastructure, in: Cyber Security and Data Protection, 2024, pp. 22–31.

[19] A. Al-Mufairej, L. BinGhaith, D. AlShareef, N. S. M. Jamail, Cyber security risk management: E-learning system, in: 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 2022, pp. 146–149. doi:10.1109/WiDS-PSU54548.2022.00041.

[20] O. Deineka, O. Harasymchuk, A. Partyka, A. Obshta, N. Korshun, Designing data classification and secure store policy according to SOC 2 type II, in: CEUR Workshop Proceedings, volume 3654, 2024, pp. 398–409.

[21] O. Deineka, et al., Information classification framework according to SOC 2 type II, in: Cybersecurity Providing in Information and Telecommunication Systems II, 2024, pp. 182–189.

[22] The official site of the LON-CAPA system, 2025. URL: http://www.loncapa.org, accessed: 2025-07-29.

[23] R. Setiawan, et al., E-learning pricing model policy for higher education, IEEE Access 11 (2023) 38370–38384. doi:10.1109/ACCESS.2023.3266954.

[24] J. Yong, J. Li, H. Wang, Portable devices of security and privacy preservation for e-learning, in: 2008 12th International Conference on Computer Supported Cooperative Work in Design, Xi'an, China, 2008, pp. 1029–1034. doi:10.1109/CSCWD.2008.4537121.

[25] Y. Martseniuk, A. Partyka, O. Harasymchuk, N. Korshun, Automated conformity verification concept for cloud security, in: CEUR Workshop Proceedings, volume 3654, 2024, pp. 25–37.

[26] C. M. A. Irfan, S. Nomura, K. Ouzzane, Y. Fukumura, Face-based access control and invigilation tool for e-learning systems, in: 2009 International Conference on Biometrics and Kansei Engineering, Cieszyn, Poland, 2009, pp. 40–44. doi:10.1109/ICBAKE.2009.43.

[27] P. Saxena, H. Sanyal, R. Agrawal, Application of rules and authorization key for secured online training — A survey, in: Proceedings of International Conference on Sustainable Expert Systems, volume 176, 2021, p. 41.

[28] O. O. Budik, V. F. Chekurin, Specific threats to information security of e-learning systems, Bulletin of the Lviv Polytechnic National University. Automation, Measurement and Control (2012). URL: http://science.lp.edu.ua/uk/node/2044.

[29] O. I. Polotai, N. P. Kuharska, Development of electronic courses in a virtual learning environment, SPOLOM, Lviv, 2021.