Development of an Online Platform for Enhancing Corporate Cyber Literacy

Danil V. Lazarev[1][a], Natalia I. Pikuleva[1][b], Amina Sh. Khafizova[1][c] and Mariya M. Volkova[2][d]
[1]*Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A. N. Tupolev – KAI, Kazan, Russia*
[2]*Institute of Management, Automation and Information Technologies, Kazan National Research Technological University, Kazan, Russia*
danil.lazarev.90@mail.ru, pikulevan@inbox.ru, aminahafizova@yandex.ru, shadana@mail.ru

Keywords: Cyber Literacy, Phishing Attack, Online Platform Development.

Abstract: In an increasingly digitalized world, the escalation of cyber threats poses significant risks to organizational security. This article focuses on the development of an innovative online platform designed to enhance corporate cyber literacy. Its primary aim is to educate company employees on the fundamentals of cybersecurity, enhancing their awareness of potential cyber threats and fostering a proactive approach to digital safety. The platform integrates interactive training courses that cover various aspects of cybersecurity, including personal data protection, safe internet use, and phishing attack prevention. Through a comprehensive educational framework, the platform ensures that employees not only understand the theoretical underpinnings of cyber threats but also engage in practical, scenario-based learning. This approach significantly improves the overall cyber resilience of organizations by equipping their workforce with the knowledge and skills necessary to mitigate risks and protect critical information assets effectively.

1 INTRODUCTION

In an era where information technology is becoming an integral part of every aspect of our lives, security threats in the digital space continue to grow, posing a serious risk to organizations. Cyberattacks can have catastrophic consequences, including loss of critical information and damage to finances and reputation.
IBM's 2023 report shows that the average cybercrime loss reached $4.45 million, a 15% increase over the previous three years, and more than half of companies plan to increase their cybersecurity budget after data breach incidents. Analytics from Accenture indicates a 31% increase in cyberattacks between 2020 and 2021.

People often become the weak link in the security chain due to social engineering used by attackers to gain access to sensitive information. This can manifest itself in the form of phishing attacks or fraudulent calls. A lack of risk awareness can lead to the creation of weak passwords or the opening of malicious files, which increases the vulnerability of the organization.
In this context, educating employees on cybersecurity becomes critical to protect companies from cyber threats. Possessing a high level of corporate cyber literacy enables organizations to protect their data, preserve their reputation, and avoid financial losses. Therefore, the development of this area is becoming increasingly important for modern companies.

2 OVERVIEW OF THE SUBJECT AREA

Corporate cyber literacy is the ability of an organization's employees to effectively and safely use information technologies in their work. It includes knowledge of the basic principles of information security, the ability to recognize threats and attacks in

[a] https://orcid.org/0009-0004-5986-7239
[b] https://orcid.org/0009-0002-4561-6303
[c] https://orcid.org/0009-0008-3803-3613
[d] https://orcid.org/0009-0001-3436-2961

the network, and the rules of safe behavior in the digital space.

Key aspects of corporate cyber literacy include:

- Employee training. Organizations should conduct regular information security training and education to increase employee awareness and reduce the risk of potential cyberattacks;
- Development of security policies. Companies should develop and implement strict security policies that define rules for the use of information resources, access to data, procedures for responding to security incidents, etc.;
- Threat Monitoring and Analysis. Organizations must continuously monitor and analyze security threats to respond quickly and prevent potential attacks;
- Legal Compliance. Companies must also comply with information security and data protection legislation to avoid potential fines and violations.

Thus, to cover all aspects, a corporate cyberliteracy training system should include the following core functionality:

- Training materials: providing access to online courses, video tutorials, presentations, and other training materials on information security topics;
- Testing and knowledge assessment: conducting tests and quizzes to test employees' knowledge of cybersecurity issues;
- Interactive lessons: using interactive simulations, games, and cases to train staff in practical security skills;
- Progress monitoring: tracking employee training progress, analyzing test results, and evaluating training effectiveness;
- Expert support: the ability to seek help and advice from information security specialists as part of the training system;
- Reports and analytics: generating reports on training progress, test results, statistics on employee participation in training, and other analytical information.

3 DESIGNING

3.1 Search for Actors and Use Cases

Actor – an acting subject who performs actions directed at others. Fig. 1 shows the main candidates for the actors of the system.

The system includes four roles:

- A system administrator is a system user with the right to administer the system as a whole;
- Company administrator – a system user with rights to administer their companies;
- A company employee is a user of the system with rights to take courses, training with a teacher;
- A company trainer is a system user with the right to train employees within the company.

After analyzing the subject area based on the roles of the system, the following functionality can be identified, as presented in Table 1.

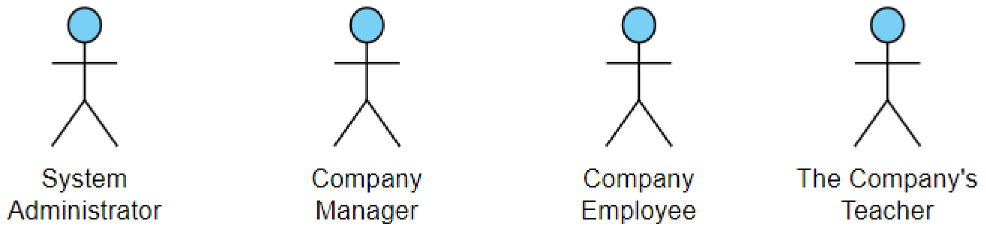

Figure 1: Actors of the system.

Table 1: The functionality of the system.

Actor	Capabilities	Brief description
System administrator	Authentication and authorization	The user can pass authentication and authorization
	Creating, deleting, and editing courses	The user can manage training courses
	Creating, deleting, and editing phishing emails	Users can manage phishing domains, email templates
Company Manager	Registration, authentication, and authorization	The user can pass registration, authentication, and authorization
	Inviting employees	The user can invite their employees to the company
	Reporting and monitoring of course completion	The user can generate reports as well as monitor how workers are being trained
	Creation of study groups	The user can create training groups and add workers and courses to them
	Simulated phishing attacks	Users can create simulated phishing attacks
	Instructor Assignment	The user can assign an instructor to a company
	Creating, deleting, and editing companies	The user can manage their companies
	Scheduling videoconferences	The user can schedule video conferences for their employees
	Adding your slides to the course	Users can supplement courses with their slides
Company employee	Registration, authentication, and authorization	Passing registration, authentication, and authorization
	Course completion	The user can take courses according to the schedule
	Chatting	The user can chat with the group and with the instructor
	Participation in a videoconference	The user can participate in video conferences
The company's teacher	Registration, authentication, and authorization	Passing registration, authentication, and authorization
	Chatting	A user can chat with a group
	Scheduling videoconferences	The user can schedule videoconferences for learners
	Participation in a videoconference	The user can participate in video conferences

All use cases can be represented in the form of a Use case diagram. A use case diagram is the most general representation of the functional purpose of the system. It allows you to understand what actions actors can perform in the system and what functionality the system provides to achieve certain goals. Using a case diagram helps to see the overall picture of user interaction with the system and is the basis for further system design. The diagram is presented in Fig. 2. It shows all roles with their use cases. It should be noted that all actions include authentication and authorization processes.

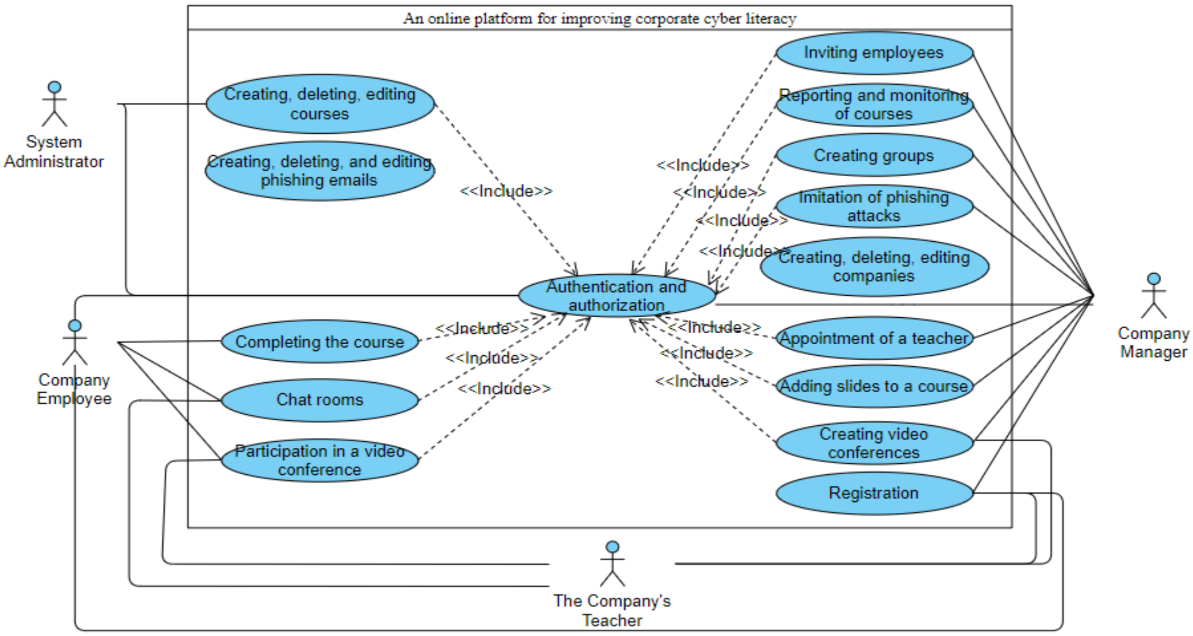

Figure 2: Use case diagram.

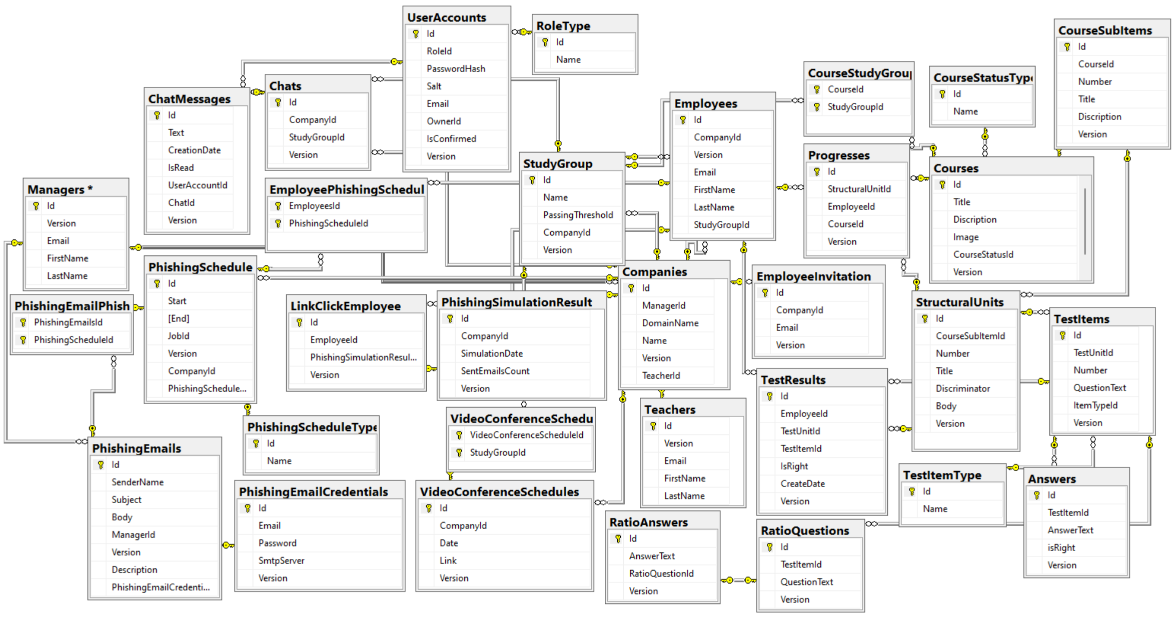

Figure 3: Entity Relationship diagram.

3.2 Conceptual database design

Entity Relationship (ER) diagram is a graphical representation of the database structure that shows entities, their attributes, and the relationships between entities. ER diagram helps to describe the structure of data, define the relationships between different entities, and see how data will be stored and interact in the database. It is an important tool for database design and provides an understanding of the structure of information in the system. Fig. 3 shows the ER diagram of the system.

3.3 Deployment Diagram

A deployment diagram is a diagram designed to describe the placement of components relative to the computing resources involved.

It helps to visualize how the system components are distributed across different nodes and servers and how they are interconnected. The deployment diagram is shown in Fig. 4.

It consists of four nodes:

- The client Device is a node device, which is a personal computer with a browser through which the user can access the online platform;
- A web Server is a device node, which is a server on which an online platform is deployed. The node itself consists of two components: the Backend app and the Frontend app. Both components run on the Windows operating system;
- Blob Server is a device node that is a server for storing files. The node consists of a single component, the S3 server. The component runs in the Windows operating system;
- A Database Server is a device node that represents a database server. The node consists of a single component – MS SQL Server. The component runs in the Windows operating system;

Client Devices can be infinitely many. The "Client Device" and "Web Server" nodes use the HTTP protocol for data transfer. Between "Web Server" and "Database Server" nodes TCP/IP protocol is used for data transfer. Between "Web Server" and "Blob Server" nodes TCP/IP protocol is used for data transfer.

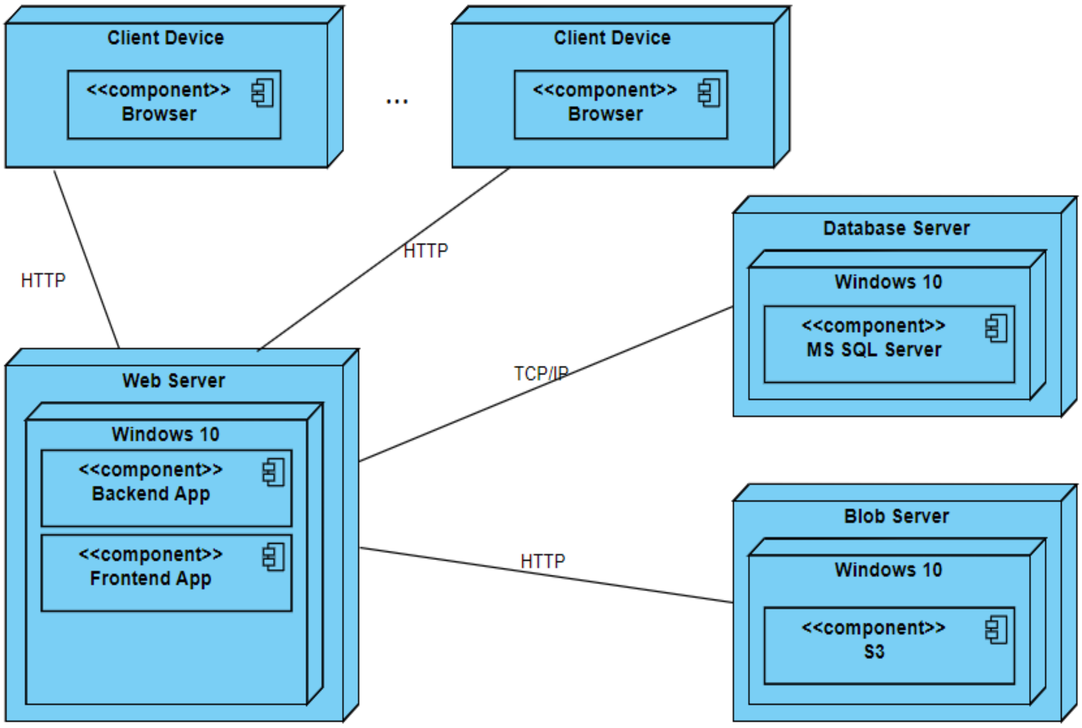

Figure 4: Deployment diagram.

4 TECHNOLOGIES FOR DEVELOPMENT

React will be used to develop the web client. React is a JavaScript library that is used to create the user interface.

MS SQL Server, a relational database management system developed by Microsoft Corporation, will be used as a database. To store files, S3 (Simple Storage Service) will be used – this is a cloud service offered by Amazon Web Services, which allows you to store files of any type and size.

The web server will be written in C# using ASP .NET Core technology and the .NET 8 framework. Key libraries with which the web server will be implemented:

- Hangfire – a multi-threaded and scalable task scheduler;
- MediatR – a simple implementation of the "mediator" pattern;
- AutoMapper is a library that allows you to project one model onto another;
- EF Core is an object-oriented, lightweight, and extensible technology from Microsoft for data access. It is an ORM (object-relational mapping) tool.

5 CONCLUSIONS

In an era marked by the burgeoning complexity and scope of cyber threats, the development and implementation of an online platform dedicated to enhancing corporate cyber literacy is both timely and essential. This platform is presented as a dynamic educational tool designed to equip company employees with the necessary skills and knowledge to effectively navigate and mitigate potential cyber risks. It combines interactive simulations, video tutorials, and real-time assessments into an engaging learning environment that caters to various learning styles.

The platform is adaptive, and regularly updated to include the latest cyber threats and countermeasures, ensuring that the training remains relevant and effective. This continuous evolution is crucial for keeping employees informed about the newest cybersecurity practices and technologies.

Among its core features, the platform integrates interactive lessons and simulations that provide hands-on experience with cyber threats, making the learning process both engaging and practical. It also incorporates continuous assessment tools to track learning progress and ensure knowledge retention and application. The availability of cybersecurity experts who provide advice and feedback enhances the learning experience and offers necessary support. Additionally, comprehensive reporting tools allow organizations to monitor the effectiveness of the training, assess vulnerabilities, and ensure compliance with security protocols.

By adopting this platform, organizations not only strengthen their security posture but also foster a culture of continuous learning and vigilance against cyber threats. This proactive approach is vital for minimizing the risk of data breaches and other security incidents, thereby safeguarding the organization's assets, reputation, and trustworthiness.

In conclusion, the successful deployment of this online platform signifies a strategic advancement in corporate cybersecurity. It furnishes employees with crucial skills and knowledge, thereby fortifying the overall security framework of the organization. As cyber threats grow increasingly complex, such educational initiatives will become ever more critical in ensuring the resilience and security of corporate entities against digital threats.

REFERENCES

Pikuleva, N. I., Khafizova, A. S., Khakov, R. A., 2020. Query processing for heterogeneous data sources in SQL generator. In *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, pp. 1-7.

Burris, J. W., 2017. Test-Driven Development for Parallel Applications. In *2017 Second International Conference on Information Systems Engineering (ICISE)*, pp. 27-31.

Pikuleva, N. I., Khafizova, A. S., Gashigullin, D. A., 2021. Event correlation with undefined data. In *2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pp. 479-483.

Yogesh, T., Vimala, P., 2020. Test-Driven Development of Automotive Software Functionality. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 1162-1165.

Fontela, C., Garrido, A., 2013. Connection between Safe Refactorings and Acceptance Test Driven Development. *IEEE Latin America Transactions* 11(5): 1238-1244.

Gibadullin, R. F., Vershinin, I. S., Minyazev, R. S., 2018. Development of load balancer and parallel database management module. In *2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pp. 1-6.

Guerra, E., 2014. Designing a Framework with Test-Driven Development: A Journey. *IEEE Software* 31(1): 9-14.

Amrit, C., Meijberg, Y., 2018. Effectiveness of Test-Driven Development and Continuous Integration: A Case Study. *IT Professional* 20(1): 27-35.
Moe, M. M., Oo, K. K., 2020. Evaluation of Quality, Productivity, and Defect by applying Test-Driven Development to perform Unit Tests. In *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)*, pp. 435-436.
Dookhun, A. S., Nagowah, L., 2019. Assessing The Effectiveness Of Test-Driven Development and Behavior-Driven Development in an Industry Setting. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, pp. 365-370.
Viktorov, I., Gibadullin, R., 2023. The principles of building a machine-learning-based service for converting sequential code into parallel code. *E3S Web of Conferences* 431: 05012.
Kozlov, E, Gibadullin, R, 2023. Prerequisites for developing the computer vision system for drowning detection. *E3S Web of Conferences* 474: 02031.
Gorodova, J., Pachina, N., Tkachenko, S., Pachin, G., 2021. Digital Literacy in the Aspect of Continuing Teacher's Education. In *2021 1st International Conference on Technology Enhanced Learning in Higher Education (TELE)*, pp. 220-223.
Yoqubjonov, J., Gibadullin, R., Nuriev, M., 2023. Advanced robotic process automation for enterprise efficiency. *E3S Web of Conferences* 431: 07011.
Kondratiev, V., 2020. Fundamental Changes in Mathematics Education in the Context of Digital Transformation. In *2020 Ivannikov Ispras Open Conference (ISPRAS)*, pp. 75-77.
Shakirzyanov, M., Gibadullin, R., Nuriyev, M., 2023. Prerequisites for the development of the system of automatic comparison of video and audio tracks by the speaker’s articulation. *E3S Web of Conferences* 419: 02029.
Chituc, C. -M., 2022. An Analysis of Technical Challenges for Education 4.0 and Digital Education Ecosystems. In *2022 IEEE German Education Conference (GeCon)*, pp. 1-5.
Gibadullin, R. F., Perukhin, M. Y., Mullayanov, B. I., 2020. Optimization of water supply by the method with model predictive. In *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, pp. 1-6.