ИНФОРМАТИКА

COMPUTER SCIENCE

МРНТИ 28.23.25, 28.01.29
УДК 378.4

https://doi.org/10.51889/ 9350.2022.33.96.016

ANALYSIS OF ANTIFRAUD METHODS AND CYBERSECURITY FOR ONLINE QUIZ APPLICATIONS

Abeshev K.[1], Kulzhanova A.[1,2], Bakibayev T.[1], Dolayev M.[1]*
[1]Alamaty Management University, Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[*] e-mail: kulzhanova.akbota1594@gmail.com

Abstract

Online quizzes have become an increasingly popular way to test knowledge and engage students in learning. Online quiz systems have become even more prevalent with the rise of remote learning due to the COVID-19 pandemic. However, with the convenience of online quizzes comes the risk of cheating. To combat this, many online quiz systems have implemented various anti-fraud mechanisms. This article will review some of the most popular online quiz systems and their anti-fraud mechanisms. Other topics discussed include methods of statistical data analysis in the context of various statistical operations, such as fraud data; general anti-fraud mechanisms; anti-fraud features of the popular online quiz systems; pros and cons of webcam and microphone monitoring.

Keywords: online education, education, information security, testing platform, fraud detection, antifraud system development.

Аңдатпа
К.Ш. Абешев [1], А.А. Кульжанова [1,2], Т.И. Бакибаев [1], М.А. Долаев [1]
[1]Алматы Менеджмент Университеті, Алматы қ., Қазақстан
[2] аль-Фараби атындағы Қазақ Ұлттық Университеті, Алматы қ., Қазақстан

ОНЛАЙН ТЕСТІЛЕУ ҚОЛДАНБАЛАРЫНА АРНАЛҒАН АНТИФРОД ӘДІСТЕРІ ЖӘНЕ КИБЕРҚАУІПСІЗДІК ЖҮЙЕСІНІҢ АНАЛИЗІ

Онлайн викториналар білімді тексерудің және студенттерді оқуға тартудың танымал әдісіне айналды. Онлайн викторина жүйелері COVID-19 пандемиясына байланысты қашықтан оқытудың өсуімен одан да кең тарады. Дегенмен, онлайн викториналардың ыңғайлылығымен студентердің алдау қаупі бар. Бұған қарсы тұру үшін көптеген онлайн викториналық жүйелер алаяқтыққа қарсы әртүрлі механизмдерді енгізді. Бұл мақалада ең танымал онлайн викторина жүйелері мен олардың алаяқтыққа қарсы механизмдері қарастырылады. Талқыланатын басқа тақырыптарға әртүрлі статистикалық операциялар контекстінде статистикалық деректерді талдау әдістері жатады, мысалы, алаяқтық деректері; алаяқтыққа қарсы жалпы механизмдер; танымал онлайн викториналық жүйелердің алаяқтыққа қарсы мүмкіндіктері; веб-камера мен микрофонды бақылаудың артықшылықтары мен кемшіліктері.

Түйін сөздер: онлайн оқыту, білім беру, ақпараттық қауіпсіздік, сынақ платформасы, алаяқтықты тексеру, алаяқтыққа қарсы жүйені дамыту.

Аннотация
К.Ш. Абешев [1], А.А. Кульжанова [1,2], Т.И. Бакибаев [1], М.А. Долаев [1]
[1]Алматы Менеджмент Университет, г.Алматы, Казахстан
[2]Казахский Национальный Университет имени аль-Фараби, г.Алматы, Казахстан

АНАЛИЗ МЕТОДОВ АНТИФРОД-СИСТЕМ И СИСТЕМ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ПРИЛОЖЕНИЙ ОНЛАЙН-ВИКТОРИН

Онлайн-викторины становятся все более популярным способом проверки знаний и вовлечения учащихся в процесс обучения. Системы онлайн-викторин стали еще более распространенными с ростом дистанционного обучения из-за пандемии COVID-19. Однако удобство онлайн-викторин сопряжено с риском мошенничества.

Для борьбы с этим во многих системах онлайн-викторин реализованы различные механизмы защиты от мошенничества. В этой статье будут рассмотрены некоторые из самых популярных систем онлайн-викторин и их механизмы защиты от мошенничества. Другие обсуждаемые темы включают методы анализа статистических данных в контексте различных статистических операций, таких как данные о мошенничестве; общие механизмы борьбы с мошенничеством; антифрод-функции популярных систем онлайн-викторин; плюсы и минусы мониторинга веб-камеры и микрофона.

Ключевые слова: онлайн-образование, образование, информационная безопасность, платформа тестирования, выявление мошенничества, улучшение качеств системы антифрода.

Introduction

Many educational institutions are trying to improve their learning processes and use various new technologies. Over the past decades, teaching methods and learning technologies have undergone major changes [1, 2]. The quality and safety of e-learning technologies and online exams are attracting the attention of educators who are actively involved in both offline and online learning. Every year, a multi-billion-dollar budget is allocated for online learning. We can't ignore apps and sites for a comfortable experience. Recently, as the Covid pandemic has forced colleges and schools to replace classroom learning with online learning, the use of e-learning technologies has expanded exponentially. At the same time, there has been a sharp increase in vulnerability in the transition to online cybersecurity education with online educational technologies. The issue was data security and privacy. Among the different types of e-learning, remote online exams are much more prone to fraud than traditional offline exams. So, why do students cheat? Cheating has become a pervasive issue in schools, colleges, and universities across the globe. There are many reasons why students cheat on exams, and understanding these reasons is critical to finding solutions to this problem. In this article, we will explore some of the most common reasons why students cheat on their exams:

1. Pressure to Succeed. One of the most common reasons why students cheat on their exams is the pressure to succeed. Many students feel that the only way to get good grades and succeed academically is to cheat. They may feel that their future is at stake and that they will not be able to achieve their goals without good grades. This pressure to succeed can be particularly strong in highly competitive environments, such as selective colleges or programs.
2. Lack of Preparation. Another reason why students cheat on their exams is because they are not adequately prepared. Students may feel that they do not have the knowledge or skills needed to do well on the exam, and therefore feel compelled to cheat. This lack of preparation may be due to a variety of factors, such as poor time management, procrastination, or difficulty understanding the material.
3. Fear of Failure. Many students cheat because they are afraid of failing. They may feel that they are not smart enough or capable enough to do well on the exam. Cheating may provide a temporary solution to this fear, as it allows students to obtain better grades without having to face the possibility of failure. However, cheating ultimately undermines a student's ability to learn and grow, and can lead to long-term consequences.
4. Peer Pressure. Peer pressure is another common reason why students cheat. Students may feel pressure from their peers to cheat, particularly if they believe that everyone else is doing it. This pressure can be particularly strong in situations where cheating is normalized or accepted by the culture or community.
5. Easy Access to Technology. The availability of technology has made cheating easier than ever before. Students can easily access information online, collaborate with their peers, or use software to complete assignments or exams. This easy access to technology has created new opportunities for cheating that may not have existed in the past.
6. Lack of Consequences. Finally, many students may cheat because they feel that there are no real consequences for their actions. If cheating is not punished or if the consequences are not severe, students may feel that there is no real risk in cheating. This lack of consequences can create a culture where cheating is normalized and accepted, leading to even more cheating in the future [2].

We will compare the most popular quiz apps like Kahoot, Quizlet, Google Forms, ProProfs Quiz Maker, Moodle Quiz, Platonus, and the brand new quiz application - Delicatest, and look at cheat detection methods and how to implement them in them, as well as in our project called Delicatest. We will also try to understand whether they properly address the security issues of online training and testing. The security controls used for online learning are very different from the methods used in traditional classrooms. The teacher watches the students in the classroom. But in online exams, the focus of such dependency is shifting to technical controls such as the webcam and software, which is the focus of this study.

Many educational institutions use a learning management system (training management system) for motivation and organizational needs that are subject to the involvement of advanced effectiveness of learning technologies to support learning [3]. The learning management system can be implemented in various forms of student learning activities [4]. A learning management system is a computer program that helps and guides students in the learning process [5]. It can be recalled that the future learning platform is one of the most important and important issues means of distance learning via the Internet [6].

It is very important to devote time and resources to the development and implementation of the approaches needed to prevent fraud in an organization, as this strongly supports the continued resilience and continuity of the business. Taking into account the losses incurred after the fact of fraud is a highly inefficient and time-consuming process, and most organizations cannot fully recover the losses incurred. However, the methodologies developed to prevent fraud are not able to ensure the complete integrity of the organization [4]. Accordingly, an organization should apply other specific policies to ensure system continuity after fraud has occurred. This is mainly achieved through fraud detection. Fraud detection methodologies typically use ad-hoc procedures that rely heavily on analytical approaches and reporting systems to identify and summarize the presence of inconsistencies and anomalies.

Materials and methods

Literature reviews, unlike original research papers, do not draw new conclusions from data; rather, they aim to analyze what has been published in primary research on a particular subject. As a result, the main goal of this literature review is to provide readers with a better understanding of risk, risk management, and its manifestations in fraud planning and succession in quiz applications [3]. First, you need to understand what a quiz is. The quiz is the shortest, most common, and most random form of assessment. What is a quiz app? You create a test and give it a name. You can then add questions and answers to the test. In the context of the course, teachers most often conduct tests to better understand how well students have mastered the topic. The test covers a small amount of material, such as one lesson, page, or concept. Quiz question formats include one or two answer choices, answer gaps, multiple choice, and true or false. In the context of the course, teachers most often conduct tests to better understand how well students have mastered the topic. The test covers a small amount of material, such as one lesson, page, or concept. Quiz question formats include one or two answer choices, answer gaps, multiple choice, and true or false.

The literature search for this review was a descriptive review search that relied primarily on two major electronic databases, including Google Scholar and Scopus. The articles used in this descriptive review were selected based on the search terms like cybersecurity, antifraud system, authentication, authorization, and information security, either alone or in combination. All report titles and abstracts have been carefully studied. The full texts of potentially relevant articles were examined, and the reference lists of these publications were searched for other related articles.

Let’s consider methods of statistical data analysis. Statistical data analysis for fraud detection performs various statistical operations such as fraud data collection, fraud detection, and fraud verification [4]. These technologies are divided into the following types:

1. The calculation of statistical parameters refers to the calculation of various statistical parameters such as means, quantiles, performance measures, and probability distributions for fraud-related data collected during the data collection process [7].
2. Regression analysis allows you to study the relationship between independent and dependent variables. This helps to understand and determine the relationship between several fraud variables, which also helps to predict future fraudulent activities [5].
3. In Probability Distributions and Models.
4. The probabilities of various fraudulent activities in a business are compared either in terms of various parameters or in terms of probability distributions [6].
5. Data matching is used to compare two sets of collected data (i.e. fraud data). The process can be carried out either based on algorithms or programmed cycles [8].

What mechanism should be used to combat fraud? The type of anti-fraud mechanism that should be implemented will depend on the nature of the exam and the level of scrutiny required. However, some general anti-fraud mechanisms that could be effective include:

1. Randomizing questions and answers: This makes it more difficult for students to share answers with each other or to look up answers online. It ensures that each student has a unique set of questions and answers.

2. Time limits: Setting time limits for exams can prevent students from having enough time to cheat or look up answers online. This ensures that students demonstrate their knowledge in a more authentic way.
3. Multiple question banks: Providing a variety of question banks with many variations can make it more difficult for students to share answers with each other or to memorize answers ahead of time.
4. Lockdown browsers: Lockdown browsers can prevent students from accessing external resources or other programs during the exam, which ensures that they cannot cheat or communicate with other students.
5. Webcam and microphone monitoring: As we discussed in a previous question, webcam and microphone monitoring can be controversial, but it can be effective in preventing cheating and ensuring exam integrity.

Ultimately, the anti-fraud mechanism that should be implemented will depend on the specific needs and requirements of the exam. Educators should evaluate the available options and choose the mechanism or combination of mechanisms that are best suited for the exam at hand. Additionally, it is important to communicate the importance of academic integrity and the consequences of cheating to students to help create a culture of honesty and fairness.

Let's look at the Antifraud features of the popular online quiz systems:

1. Kahoot

Kahoot is a popular online quiz system that is widely used in classrooms around the world. Kahoot's anti-fraud mechanism is centered around a two-step login process. When a student logs in to Kahoot, they must enter a username and password, as well as a PIN code specific to the quiz. This makes it more difficult for students to share quiz content with each other. Kahoot also includes monitoring features that alert teachers when a student is suspected of cheating. For example, if a student answers questions too quickly, the teacher can receive an alert and investigate further.

2. Quizlet

Quizlet is another popular online quiz system that is used by many teachers and students. Quizlet uses a variety of anti-cheating measures, including timed quizzes, randomized questions, and verification codes that prevent students from sharing quiz content with each other. The timed quizzes ensure that students do not have enough time to cheat or look up answers online. The randomized questions mean that each student gets a different set of questions, making it more difficult for students to share answers. The verification codes ensure that students cannot share quiz content with each other outside of the platform.

3. Google Forms

Google Forms is a popular quiz system that is widely used by teachers to create and distribute quizzes. Google Forms has built-in anti-cheating features that are designed to prevent students from cheating. For example, teachers can limit responses to one per user, which ensures that students cannot retake the quiz or submit multiple answers. Google Forms also includes features that allow teachers to shuffle answer choices, making it more difficult for students to share answers. Additionally, Google Forms uses captcha tests to prevent automated bot attacks.

4. ProProfs Quiz Maker

ProProfs Quiz Maker is a quiz system that is designed specifically for educators. It offers a range of security features that are designed to prevent cheating. For example, ProProfs Quiz Maker allows teachers to password protect their quizzes, which ensures that only authorized students can access the quiz. ProProfs Quiz Maker also includes timed quizzes, which ensure that students do not have enough time to cheat or look up answers online. In addition, ProProfs Quiz Maker uses IP address tracking to monitor and prevent cheating. Lastly, the question bank contains a large number of variations to prevent students from sharing answers.

5. ExamSoft

ExamSoft is a secure testing platform that is designed for high-stakes exams. It is widely used by professional organizations, such as bar examiners, medical boards, and law schools. ExamSoft offers a range of anti-fraud mechanisms that are specifically designed to ensure exam integrity. When students take an exam on ExamSoft, the platform locks down their computers, preventing access to other programs or the internet. This means that students cannot cheat by accessing external resources or communicating with other students. ExamSoft also uses facial recognition technology to verify the identity of the student taking the exam. Finally, live proctoring is available to monitor exams and ensure that no cheating occurs.

6. Platonus

Platonus is an information system that is designed to provide effective information support for the management of the education system, as well as the management of the educational process of higher and

secondary educational institutions. The information system Platonus will provide a set of tasks in the following areas: a) Improving the efficiency of management in the field of education based on the information and technical support for solving the problems of monitoring compliance with the check of the contingent; b) Improving the quality of the provision of educational services based on the improvement of information technology support for the activities of higher and secondary educational institutions, their employees, and students; c) Raising the awareness of students of higher and secondary educational institutions on the issues of conducting the educational process, as well as the implementation of activities in the field of education based on providing the possibility of electronic interaction with the relevant authorized bodies [9].

7. Moodle Quiz

Moodle is a popular learning management system that is widely used in schools and universities. Moodle Quiz is the built-in quiz system that is included in Moodle [10]. Moodle Quiz allows teachers to set a variety of anti-cheating measures, such as randomizing question order and answers, setting time limits, and providing immediate feedback on correct answers. The randomization of questions and answers ensures that students do not have the same set of questions or answers, making it more difficult for students to share answers. The time limit ensures that students do not have enough time to cheat or look up answers online. Finally, providing immediate feedback on correct answers ensures that students cannot share answers with each other.

8. Delicatest

We will also consider the functionality of the online quiz system Delicatest. Delicatest allows you to compose test questions. Questions can be exported and imported to CSV so that they can be shared with colleagues. You can use images for questions, use the Latex functionality for mathematical formulas, and even insert program code. Let’s consider the main idea of the antifraud process of Delicatest. The main idea that we currently have to implement in our project is as follows.

1. We have a quiz that has a list of questions.
2. We have a student who wants to take the quiz.
3. Every time the student answers a question, we check if the student has already answered this question before. If the student has already answered this question, we do not allow the student to answer the question again. We also do not allow the student to change the answer.
4. We also check the time that the student has taken to answer the question. If the student has taken too much time to answer the question, and the question was relatively simple, this answer becomes suspicious.
5. If the student answers a question too quickly, and the question was relatively difficult, this answer also becomes suspicious.Now, the question is to recognize if the question itself was difficult or not.

We have a list of questions. We can use the number of correct answers to a question to recognize if the question was difficult or not. If the number of correct answers is high, the question is easy. If the number of correct answers is low, the question is hard. We can also use the number of students who answered the question to recognize if the question was difficult or not. If the number of students who answered the question is high, the question is easy. If the number of students who answered the question is low, the question is hard. But that is not all. Our goal is to know how much time is necessary to answer the question. We only look at the correct answers and save the time that the student has taken to answer the question. Now, the speed of each student is different. So, we need to normalize the time that the student has taken to answer the question. We can do this by dividing the time that the student has taken to answer the question by the average time that the students have taken to answer the question. Now, we have a normalized time. We can use this normalized time to recognize if the question was difficult or not. If the normalized time is high, the question is easy. If the normalized time is low, the question is hard.

After all the questions are answered, having all the normalized times, we can detect cheating [6]. We can detect cheating by comparing the normalized time of each student to the normalized time of the other students. If the normalized time of a student is too high or too low, this student is most probably cheating. Also, we can detect cheating using the unique code. We generate a unique code for each student. This code is generated using the student's name, the quiz's name, and some random numbers. This code is saved to the local storage of the student's browser. The student cannot change this code. It happens that one student is helping another. Each student has a personal link to the quiz, and the student can share this link with his friends. When the student shares the link with his friends, the student's unique code stays unchanged, and it is sent to the server together with the answers. If we see the same code for different users, this is a sign of cheating.

In Figure 1, we can see an IP address. This is the IP address of the student who answered the question. To protect the personal data of students, the surnames, names, and mail of the students were covered up.

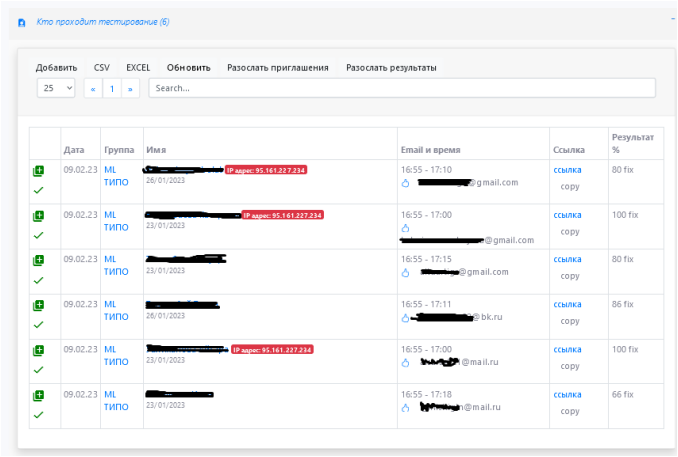

Figure 1. List of identical IP addresses of the students

We relied on this field for some time to detect cheating. However, we found out that this is not a reliable way to detect cheating. The reason is that students can use a VPN to change their IP address. Also, when after the Covid pandemic, students started to take the quiz from universities, and they were using the same IP address. So, this field is not reliable for detecting cheating. We have another method here to mention. We generate a unique code for each student. This code is generated using the student's name and the quiz's name. We use this code to detect cheating. We will talk about this method in the next section.

Delicatest makes it possible to track the activity of students. For example, using the telegram bot, you can track how many students have passed the test out of those enrolled for passing the test, how many are passing at a given time, and the average score, it allows exporting to csv, xls formats, and also provides detailed information on the scores of each student. Let's see how it looks with the help of Figure 2.

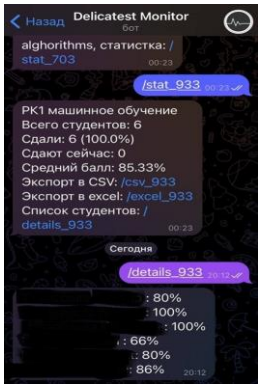

Figure 2. An example of using a telegram bot for data analytics on passed tests in Delicatest

What features are more important? There are several anti-fraud mechanisms that are important in preventing cheating in online quiz systems. However, the most important mechanisms depend on the nature of the quiz and the level of scrutiny required. For high-stakes exams, measures such as locking down the computer, using facial recognition technology to verify the identity of the test taker, and live proctoring are critical to ensuring exam integrity. These measures ensure that students cannot cheat by accessing external resources or communicating with other students. For low-stakes quizzes, anti-fraud mechanisms such as timed quizzes, randomization of questions and answers, and verification codes can be effective. These mechanisms make it more difficult for students to share answers or cheat by looking up answers online. Additionally, tracking features that monitor and identify unusual activity or behavior can be helpful in detecting cheating. Ultimately, the most effective anti-fraud mechanisms are those that are tailored to the specific needs and requirements of the quiz or exam. Educators should carefully evaluate the available options and choose the mechanisms that best suit their needs. If we talking about Webcam and Microphone monitoring, webcam and microphone monitoring during an online exam can be a controversial issue. Some people believe that this type of monitoring is necessary to prevent cheating and ensure exam integrity, while others view it as a violation of

privacy. In this article, we will explore the pros and cons of webcam and microphone monitoring during online exams to determine whether it is appropriate [11].

Let's take a look at the pros of webcam and microphone monitoring:

1. Prevents Cheating

Webcam and microphone monitoring can be an effective way to prevent cheating during online exams. When students know that they are being monitored, they are less likely to cheat, which ensures that the exam results are more accurate and reflect the student's actual knowledge.

2. Ensures Exam Integrity

Webcam and microphone monitoring can also ensure exam integrity by preventing students from accessing external resources or communicating with other students during the exam. This ensures that the exam is fair and that all students have an equal opportunity to demonstrate their knowledge.

3. Deters Potential Cheaters

The presence of webcam and microphone monitoring can act as a deterrent to potential cheaters. When students know that they are being monitored, they are less likely to cheat, which can help to maintain the integrity of the exam.

Let's also look at the cons of webcam and microphone monitoring:

1. Violation of Privacy

Webcam and microphone monitoring can be seen as a violation of privacy. Students may feel uncomfortable knowing that they are being monitored during the exam and may feel that their privacy has been violated.

2. Technical Issues

Webcam and microphone monitoring can also be challenging from a technical perspective. Students may have technical difficulties that prevent them from participating in the exam or that disrupt their performance. This can lead to inaccurate results or unfair treatment of students.

3. Ineffective for Some Forms of Cheating

Webcam and microphone monitoring may not be effective for preventing some forms of cheating, such as using a second device or communicating with others outside of the monitoring range. In these cases, students may still be able to cheat despite the monitoring. And of course, the main question is, what mechanism to use? The type of anti-fraud mechanism that should be implemented will depend on the nature of the exam and the level of scrutiny required. However, some general anti-fraud mechanisms that could be effective include: Randomizing questions and answers. This makes it more difficult for students to share answers with each other or to look up answers online. It ensures that each student has a unique set of questions and answers:

1. Time limits: Setting time limits for exams can prevent students from having enough time to cheat or look up answers online. This ensures that students demonstrate their knowledge in a more authentic way.
2. Multiple question banks: Providing a variety of question banks with a large number of variations can make it more difficult for students to share answers with each other or to memorize answers ahead of time.
3. Lockdown browsers: Lockdown browsers can prevent students from accessing external resources or other programs during the exam, which ensures that they cannot cheat or communicate with other students.
4. Webcam and microphone monitoring: As we discussed in a previous question, webcam and microphone monitoring can be controversial, but it can be effective in preventing cheating and ensuring exam integrity.

Ultimately, the anti-fraud mechanism that should be implemented will depend on the specific needs and requirements of the exam. Educators should evaluate the available options and choose the mechanism or combination of mechanisms that are best suited for the exam at hand. Additionally, it is important to communicate the importance of academic integrity and the consequences of cheating to students to help create a culture of honesty and fairness.

Conclusion

With the growth of information, information and data processing plays an important role in the efficient operation of departments within the organization and outside it, for example, in educational institutions. Processing data is time-consuming because there are large and ever-growing volumes of data in any organization. Accordingly, information systems, in light of advances in computer systems, have been developed to rationalize specific methods associated with data processing, in particular for collecting, storing, processing, and analyzing data, as well as for extracting and disseminating information for certain purposes. However, in addition to the wide range of benefits that information systems provide to organizations, they also

present some potential risks to the organization. The risks associated with the implementation and development of information systems are closely related to the development of information and data security. Consequently, worldwide attention and investment in resources towards standardization and the development of specific frameworks with which to reduce the associated risks can be increased. There are many online quiz systems available today, each with their own unique features and anti-fraud mechanisms. It is important for educators to evaluate these systems based on their specific needs and requirements. While some systems may be better suited for low-stakes quizzes, others are designed for high-stakes exams. By using these anti-fraud mechanisms, educators can ensure that students are learning and demonstrating their knowledge in an honest and fair manner.

In the article we have covered:

1. Methods of statistical data analysis in the context of various statistical operations, such as fraud data;
2. General anti-fraud mechanisms;
3. Anti-fraud features of the popular online quiz systems;
4. Pros and cons of webcam and microphone monitoring.

Within such structures, risks are identified, systematized, analyzed both qualitatively and quantitatively, and then responded to, which is combined with the development of specific policies to prevent the occurrence of such risk events. Webcam and microphone monitoring during an online exam can be appropriate, but it is important to consider the pros and cons carefully. While it can be an effective way to prevent cheating and ensure exam integrity, it may also be seen as a violation of privacy and may not be effective for preventing all forms of cheating. Educators should consider these factors when deciding whether or not to use webcam and microphone monitoring during online exams. Additionally, it is important to communicate with students about the purpose and importance of webcam and microphone monitoring and to ensure that the monitoring is carried out in a fair and consistent manner. It can be concluded that the integrity of information plays an important role in modern society. Every day we are exposed to risks and fraud, so the invention of information and data protection tools is important today. In conclusion, cheating is a complex problem that has many different causes. Understanding these causes is critical to finding solutions to this problem. To prevent cheating, it is important to create a culture of academic integrity that emphasizes the importance of learning and honesty. This can be done through educational programs, clear policies and consequences for cheating, and support for students who may be struggling academically. By addressing the root causes of cheating, we can create a more honest and fair educational system that benefits everyone.

References:

1 Slusky L. Cybersecurity of online proctoring systems //Journal of International Technology and Information Management. – 2020. – Т. 29. – №. 1. – С. 56-83.

2 Bauer T. N. et al. Privacy and cybersecurity challenges, opportunities, and recommendations: Personnel selection in an era of online application systems and big data. – 2020.

3 Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours //Heliyon. – 2017. – Т. 3. – №. 7. – С. e00346.

4 Obaidat M. S., Traore I., Woungang I. (ed.). Biometric-based physical and cybersecurity systems. – Cham: Springer International Publishing, 2019. – С. 1-10.

5 Fraud detection // linkedin.com URL: https://www.linkedin.com/pulse/fraud-detection-nishi-kumari 29.11.2022.

6 Meszaros J., Buchalcevova A. Introducing OSSF: A framework for online service cybersecurity risk management //computers & security. – 2017. – Т. 65. – С.300-313.

7 Prasad R., Rohokale V. Cyber security: the lifeline of information and communication technology. – Cham, Switzerland: Springer International Publishing, 2020.

8 Wulandari I. A. I. et al. Application of lesson study during the COVID-19 pandemic in online learning using problem-based learning to increase student collaboration skills //AIP Conference Proceedings. – AIP Publishing LLC, 2023. – Т. 2569. – №. 1. – С. 020013.

9 Abeldina Z. et al. Experience in Education Environment Virtualization within the Automated Information System" Platonus"(Kazakhstan) //International Journal of Environmental and Science Education. – 2016. – Т. 11. – №. 18. – С. 12512-12527.

10 Mustafa A. S., Ali N. The Adoption and Use of Moodle in Online Learning: A Systematic Review. – 2023.

11 Isaac O. et al. Online learning usage within Yemeni higher education: The role of compatibility and task-technology fit as mediating variables in the IS success model //Computers & Education. – 2019. – Т. 136. – С. 113-129.