Anti-fraud protection in learning outcomes assessment: from didactic requirements to technological solutions

Conference Paper · October 2023

DOI: 10.58503/icvl-v18y202303

CITATIONS
0

READS
20

1 author:

Burlacu Natalia
Technical University of Moldova
24 PUBLICATIONS **29** CITATIONS

SEE PROFILE

Anti-fraud protection in learning outcomes assessment: from didactic requirements to technological solutions

Natalia BURLACU

Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, 9/7 Studentilor street, Chișinău city, Rep. Moldova, MD-2020

natalia.burlacu@iis.utm.md

Abstract: *The present research turns out to be a theoretical study with methodological and applied accents in the field of educational sciences, as also the professional training of future ICT specialists. The author discusses the problem of educational fraud, examining the phenomenon from a notional, social perspective through the analysis of specialized literature related to the announced topic, here several areas are outlined that intersect and influence each other, such as: (A). educational fraud, cheating, plagiarism, but also (B). the solutions - didactic and technological - are analyzed and proposed for use in order to prevent, reduce, potentially and eliminate the phenomenon of fraud from educational practice, especially from the didactic context of the university environment.*

Keywords: Educational fraud, Digital anti-fraud tools, Methodological anti-fraud tools.

1. Introduction

Periodically, teachers who interact with their students at various stages of schooling and / or professionalization are faced with evidence of fraud acts able to attest the presence and / or quality of skills possessed by students who intend to confirm and / or certify certain knowledge, abilities corresponding to a given field of study (thematic and / or professional area, academic subjects, study program, etc.) and / or a qualification level.

Probably, there are no such types of teachers (primary and / or high schools' teachers; university teaching staff, beginning with mentors, assistants, and lecturers, until the holders of the most notorious scientific and didactical titles in the academy) who have not encountered at least once the phenomenon of fraud and cheating behavior among students.

The purpose of this article is to describe the possibilities of anti-fraud protection through the lens of the analysis of the fraud phenomenon in the assessing process of the skills acquired by the learner during his studies and also to inform the didactic and scientific community about the set of technological tools capable to ensure the protection against educational fraud.

https://doi.org/10.58503/icvl-v18y202303

In the context of the announced goal, the following objectives were formulated: (1). A brief description of the phenomenon of fraud in education from a conceptual perspective; (2). Analysis of the term fraud in education from an ethical perspective, in particular through the prism of the principles formulated by the Council of Europe for the Ethics, Transparency and Integrity Platform (ETINED); (3). Analysis of specialized literature regarding the phenomenon of fraud in education from the perspective of didactic activities related to the evaluation and measurement of skills obtained by the learner with the aim of diversifying evaluation strategies, but also increasing their objectivity; (4). Presentation of the methodological aspects of anti-fraud protection methods applicable in education; (5). The review of technological anti-fraud protection tools, applicable, but also already used in education; (6). The phrasing of conclusions related to this research.

2. The phenomenon of educational fraud (EF)

2.1 Conceptual and ethical context

As a rule, the fraud and misleading behavior of the learner is associated with a formal educational setting, but it can also extend to other situations related to the process of assessment/measuring / proving the competencies of the potential applicant(s) for the particular jobs: either within the various contests with the aim of occupying certain positions; admission to another level of studies, professional activity; and also for participation in various competitions with the aim of determining eventual, the best, winners.

Regardless of obtaining which facilities or access to certain goods, **fraud, and deception is the act that deprives the one who deserves it** (in this role can be anyone, a natural and/or legal person represented by any public or private institution, sometimes even by the state itself) **of something valuable.**

Speaking of a formal institutional educational framework, we refer to all educational organizations, whether public or private, recognized by the authorities of a country that operate in the field of education and provide services related to the declared field within institutionalized, intentional, and planned limits.

Currently, the formal institutional educational framework of a country consists, for the most part, of initial and general education institutions, educational institutions for beneficiaries with special needs, and institutions that offer special educational programs, these being part of the field of adult education, but and vocational education institutions.

The latter are also recognized as components of professional education (Tertiary education, starting with level 3-4 ISCED and ending with level 5-7 of studies, these being usually delivered by universities), a fact defined in accordance with the International Standard Classification of Education ISCED 2011 issued by

The UNESCO Institute for Statistics (UIS) (UNESCO Institute for Statistics, 2012). There is also a dedicated term for frauds tangential to educational processes/activities. This term is "Educational Fraud" (EF), defined by the Council of Europe for Ethics, Transparency, and Integrity Platform (ETINED).

In the determination given by ETINED, EF is associated with behavior or action occurring in the field of education, intended to deceive and obtain an unfair advantage. Correspondingly, in the ETINED's view, EF could include more activities such as:

A. The activities of diploma, accreditation, visa, and essay bank factories, etc.;

B. Impersonation by performing in whole or in part any work or assessment required as part of a program in place of an enrolled student;

C. Illegal or unregulated use of authentic documents;

D. Copying the learning results to the assessment tests (of different levels and in various didactic contexts);

E. Plagiarism;

F. Producing or using falsified, plagiarized, or counterfeit documents;

G. Offering unrecognized or unaccredited qualifications with intent to defraud another.

In our article, we are going to discuss more regarding the aspects that can serve as solutions to the problems contained in points B, D, and E. These are elements that are directly within the scope of education sciences, general and / or particular didactics; are embedded as some educational management components (Burlacu, 2022d), and also as issues related to the process of managing the technical and technological infrastructure to secure the contents of evaluation/measurement/marking of learning results.

The Platform for Ethics, Transparency, and Integrity of the Council of Europe (ETINED) delivered a series of rules called "ETINED Principles" which would be followed and promoted in accordance with its mandate. The "ETINED Principles" authors were based on the idea that **quality education should only be achieved when educational fraud will also be effectively addressed.** This was a goal forwarded when issuing the "ETINED Principles".

In other words, the "ETINED Principles" will be real to apply if all relevant sectors of society adhere fully to a set of fundamental ethical principles, both in public and professional life, while being based on legal norms and structures such as the development, integration, and support of the culture of " [...] democracy and participation based on the principles of ethics, transparency, and integrity in education" (UNESCO Institute for Statistics, 2012). So, one of the tools able to support the promotion of quality education is the fight against educational fraud.

2.2 Review of the specialized literature: the dimensions of the EF problem

Scientific articles that discuss various aspects related to the phenomenon of educational fraud address a wide spectrum of subjects, some of which outline new sides of the stated problem, others come with certain didactic solutions either of purely methodological content or with technological implications, but all being characterized through a series of operationalization modalities that would allow the easy application of these ideas in practice. In particular, we consider it worth mentioning the following topics related to the given research problem:

I. The aspects associated with the methodology of organizing and carrying out the assessment process of the learning outcomes of students in various disciplines, but also through the application of various strategies, methods, and/or techniques, such as general and particular didactics:

- Computer Science and professional training of future ICT specialists (Burlacu, 2016);
- The assessment of the learning progress during optional courses in the curricular area of Romanian language and literature through projects (Cartaleanu, 2017) and test-type tests (Cartaleanu, 2018);
- The teaching-learning-assessment of the subject Chemistry by applying interactive methods, but also by means of eLearning techniques and tools, including the Moodle platform utility (Melentiev, Calmuțchi & Cerbușca, 2021).

II. The analysis of the possibilities of developing and implementing innovative strategies for evaluating the learner's skills, these being based on the diversification of evaluation methods and procedures, as well as capitalizing on their potential (Burlacu, 2022a; Burlacu, 2022c).

- Reflecting on the theoretical benchmarks of some methods and procedures able to support the teaching staff in building a modern assessment strategy of learning outcomes of the learner on the example of the specific didactic context of the study programs with the specializations in the field of Computer Sciences and ICT (Burlacu, 2016; Burlacu, 2022c);
- Description of a formative assessment tool based on criteria and descriptors that could be implemented within the educational activities specific to seminar classes within the study programs of specializations with professionalization in the field of Computer Science and ICT, but not only (Burlacu, 2021c).

III. The assessment of technology-assisted learning outcomes (Balmus & Burlacu, 2017; Burlacu, 2020a; Burlacu, 2020b; Burlacu, 2022b). Given the direction of research is represented by studies that touch on the side of digital

transformations (Burlacu, 2021d; Burlacu, 2021e) that all of us are traveling through, as the actors who design, create, and implement the changes. And, above us, as members of society who go across the torrent of metamorphoses of the digital age–related to the changes in the educational process (Burlacu, 2022c; Burlacu, 2022d).

- The ways of creative assessment, either assisted by technology or organized and carried out with the aim of developing skills that generate innovative ideas (Burlacu N., 2022a) and are sustainable and/or have the potential to train future generations of responsible people, able to think critically and strategically, as well as to act rationally (Burlacu & Irimiciuc, 2018; Burlacu, 2022c).

IV. Works that debate some forms of educational fraud phenomenon, such as plagiarism, and also some software solutions for checking plagiarism (Burlacu & Irimiciuc, 2017; Burlacu, 2022a);

V. The use of LMS platforms for educational purposes, obviously also to evaluate the skills acquired throughout the studies: capitalizing on the actual tools available on Moodle (Deinego, 2016; Burlacu, 2021a; Burlacu, 2021b) and/or virtual classes (Burlacu, 2020a).

3. Anti-fraud protection methods

3.1 Methodological aspects of anti-fraud protection

Obviously, it is insufficient to talk to students about undesirable behaviors during assessment tests, but also their consequences. Although each educational institution reflects the given aspect in its internal regulations, regardless of whether or not there is a code of ethics that establishes the attitude towards such actions, as a rule, the teaching staff also does this there.

Every member of the teaching staff, in his/her turn, was once a student. Moreover, since he/she was passing along the professional training through multiple assessments, exams, checks, and confirmations, today's teacher has encountered at least one such case of fraud in evaluation tests. Does not matter what kind and/or level of studies it was about, and it is not also important about what type of status he/she was in when these happened: he/she could be in the position of a student/trainee, or in the position of a teacher already.

As our basic purposes in the present material are: (A). The analysis of the fraud phenomenon in the assessment during certifications and/or colloquiums, tests and/or passing exams, and the completion of a discipline (either school or university, etc.); (B). The description of some technological tools to prevent the phenomenon of copying, plagiarism, and/or any other kind of deception that would devalue and/or reduce to zero the credibility and authenticity of the learning results.

We would like to mention that, certainly, there are also methodological solutions for designing, structuring, developing, and applying assessments so that they are less exposed to the risk of fraud. Broadly speaking, among the respective measures we could list the following:

• **How to construct/formulate the questions in the sheet/form/evaluation grid.** Here we mean that it should be conceptualized in such a way that from the start will exclude the student's need to search/find the answer on the Internet so that the correct answer is trivially copied and placed in the given assessment place and presented as his own. Resulting of this approach, the items formulated for a possible assessment test of the learning outcomes should contain complex and creative components (even in the case of exact sciences). So that the given answer would reflect the capacity of analysis, synthesis, generalization, and deduction of the evaluated student. It is clear, that the development of such assessment items also requires a higher degree of competence, creativity, and dedication from the teacher.

It is easier to make superficial test sheets that a priori do not have the potential to measure the depth and quality of the skills, knowledge, and abilities possessed by the student, and also to confirm the veracity and/or belonging of the particular answer to the evaluated learner. Without a doubt, if the assessment and/or tests are more standardized, the answer given by the student, will not bear the individual imprint of him/her. Only argumentative and/or open-text answers, essays, and code design in a programming language will bring clarity to the originality of the answer, but also of the assessment itself.

• **The developing of unique assessments for each student.** There are several scenarios here. The uniqueness of the assessment variant can be implemented either by developing an X number of test variants, equal to the number of students to be evaluated; or by diversifying/customizing only a certain part of the test with an obvious application content.

For example: When we are talking about the real sciences, only the problem(s) proposed to be solved within the practical task can be different from one variant to another variant. Providing that the practical task will reflect the same degree of complexity, and also will test potentially the same skills of each learner. In the case when exist a few assessment variants should be distinct at least the operational values, and/or some problem statement aspects, and/or some content of the initial template of the assessment grid.

• **Carrying out identity verification of the assessed.** The given procedure is also called the identity authentication process and consists of taking measures to ensure that the student who wrote the answers is also the student who will take the grade. Physical supervision of the classroom by the teacher and his assistants (including surveillance through the camera) also is opportune here. If the exam is online, digital solutions can be used to perform two-factor authentication (2FA) when accessing the system and entering the teaching-learning-assessment platform.

2FA is a security system that requires two separate, distinct ways of identification in order to access something (in educational needs it can be, as in our case, the teaching-learning-assessment platform). Usually, the first factor is a password and the second commonly includes a text with a code sent to the user's and/or learner's smartphone. In circumstances requiring increased security levels, the given 2FA systems can include the biometrics data scan such as the user's fingerprint, face, or retina.

• **Assessment Course: Fraud Prevention by Intervening in the Process of the Assessment.** If there are suspicions that the assessment is fraudulent and/or there are signs of undesirable student behavior, the assessment test (digital grid or paper) can be removed from final verification with or without canceling what was written, and the student can be penalized.

There are numerous reports about fraud cases and deception discovered during the assessments carried out in reputable educational institutions (public and private schools, colleges, and universities) in the international mass media sources. The reflected of the international press's occurrences ended with the sending down of the students who committed these violations.

3.2 Technological anti-fraud protection tools

The fact is that currently there are technological tools that could reduce and / or eliminate actions related to the fraud phenomenon of the learner in the world.

Conventionally speaking these are of two kinds: (1). Hardware, and also (2). Software.

From the hardware category, we refer to the possibilities of external supervision of the evidence-supporting process, the one that takes place under the video cameras, as is happening at the baccalaureate sessions in the Republic of Moldova beginning in 2012. We will talk about a few software anti-fraud protection solutions.

3.2.1 Mobile authentication apps

These kinds of applications (see Table 1) offer the connecting possibility to various online accounts, as well as websites through 2FA, or even multi-factor authentication.

Table 1. Mobile Multi-factor Authentication Apps

ON	**Application Description** *(App Name & Producer)*
1.	*Duo Mobile App; Cisco; USA*
The application is intended for enterprise users who deserve the software development process. Given product has proposed a set of innovative	

business organization features, especially, (A.) the multi-user deployment and provisioning options and (B.) one-tap push authentication. The last one is a mechanism that responds to a single tap in comparison with usually used one-time passcodes. Duo Mobile backups can be performed using: Google Drive for Android and/or iCloud KeyChain for iPhone.	
2.	*Google Authenticator; Google; USA*
The given application is a basic one with additional possibilities for its own services, such as Microsoft Authenticator. Google Authenticator does not offer an online backup for account codes, although the user can import them from an old phone or another digital device to a new one. It should be mentioned that there is currently no Apple Watch app for Google Authenticator.	
3.	*Microsoft Authenticator; Microsoft; USA*
Microsoft Authenticator incorporates strong password generation and lets you sign in to Microsoft accounts with the push of a button. The app also allows educational organizations and workplaces to register users' devices. In the case when the user adopts this app, it should make sure to enable account recovery. That way, when the user gets a new device, he / she'll see a recovery option by signing in to his Microsoft account, providing more steps of verification. The user can request to unlock his/her phone with a PIN or biometric verification to see the codes. Password management options can be found in a separate tab at the bottom. Also is possible to sync with the user's Microsoft account associated with the alternative authenticator, and then he/she would see own logins saved and synced, for example, in the Edge browser. There is one problem (and it's an Apple lock-in problem) here if a user backs up to iCloud, you can't transfer your saved MFA accounts to an Android device, even though this is the case with most authenticators that offer cloud backup.	
4.	*LastPass Authenticator (used for iPhone); GoTo, formerly LogMeIn; USA*
The LastPass Authenticator is separate from the LastPass password manager, although it does offer some interaction with the password manager. Installing LastPass Authenticator is a breeze, and if the user already has an MFA-enabled LastPass account, he/she can easily authorize LastPass by tapping a push notification. Also, once the app is set up with the user's LastPass account, it's easy to back up the login accounts to the LastPass vault, which optimizes the process of data transfer to a new phone.	
5.	*Twilio Authy; Twilio; USA*
One of Twilio Authy's big advantages is the encrypted cloud backup. Nevertheless, it is worrying that the analyzed app can add up another phone using "a PIN code sent-a call or an SMS", which is able to open in a new window. There's an extra option to enter a private password or	

passphrase that the given product uses to encrypt login information for your cloud accounts.
The password is known only to the user, so if he/she loses it, this app will not be capable of recovering the account. Certainly, it means that authorities cannot force Authy owners and/or developers to unlock users' accounts. Unlike the other products with similar functions, described in the present paper, the Authy app requires the user's phone number when he/she first configures it. This requirement is the best solution for the majority of users as they would prefer the app to treat their phones as anonymous hardware pieces. Moreover, some experts have suggested that asking for a phone number opens the app up to SIM-swapping fraud. The Authy Help Center proposes ways to mitigate the vulnerabilities, but some beneficiaries choose to work more with authentication apps made by other corporations. The Apple Watch app version has been developed for those devoted users who need and plan to use it in any case.

Authenticator Apps like the ones listed above - Authy, Google Authenticator, and Microsoft Authenticator represent cyber security ways. The use of such application would ensure the protection of the user's identity and/or his / her reputation.

Because in our case, we are talking about the assessment process of the learning outcomes and/or about the final decision during a competition, etc. which is intended to confirm, and then certify the eligibility of the assessed candidate for a possible position that requires a certain level of competence and/or entry into possession of a diploma for the successful completion of a course and/or of the study program, etc. we adhere to the opinions of cybersecurity and GDPR (General Data Protection Regulation) policy experts who confidently recommend these digital tools, including for educational and anti-fraud purposes.

3.2.2 Kiosk mode analysis: functionality and usability

Kiosk Mode is a feature, mostly provided to users of a range of operating systems such as Windows, Linux, Ubuntu, and Mac.

This mode can be characterized as a digital tool that enables the smart display of an application in a full-screen mode on a secured device. This function exists for several versions of browsers. Thus, some are able to run Google Chrome, Microsoft Edge, and Mozilla Firefox.

The Kiosk mode configuration provides the user's computing system with a protected and focused browsing environment where corporate users, such as educational institutions – colleges and universities; companies in various social, economic, and industrial sectors could: (A). increase the productivity of employees and beneficiaries and/or (B). streamline the user experience by providing secure connections to implement host business resources.

Among the beneficial characteristics of the implementation of the Kiosk mode in didactics are considered:

I. **Increasing the assessor's concentration on digital content** *that can be both learning-teaching and assessment of the learning objectives.* Increasing the user's focus is achieved by restricting the ability to navigate to websites and/or web applications with certain contents. In the case of employees and not students, it can be used to reduce the possibility of distracting employees from professional activities during working hours; while in the case of students to eliminate, and reduce the consultation of didactic contents for the purpose of copying and cheating on assessment tests.

II. **Increasing the level of cyber security.** *Kiosk mode prevents users from accessing unauthorized Web locations and/or intentionally or unintentionally changing system settings.* The Kiosk module provides a secure browsing environment, protecting: (A). The sensitive information (commercial, and also non-commercial, but which should not be disclosed; in our case, this could be - the contents of the evaluation sheets and or the bank of items); (B). The computer system against malware and/or theft of personal and or commercial data.

III. **Provides the user with a relatively simple interaction experience** *during intuitive browsing sessions, transforming the virtual workspace into an ideal protected area for both ICT professionals and other types of users.* The Kiosk mode users will manipulate readable, highly functional, unambiguous menus. It means the given menus will not create any misunderstanding regarding the action that will be produced after activating the menu command by the user. To rephrase it, users won't feel like they're navigating through a maze of menus, which will allow them to not worry about causing accidental actions.

IV. **It showcases branding and customization options to companies and educational institutions that use it.** Kiosk mode allows host institutions that choose to use the tool to tailor their browsing experience to their specific needs. It allows customization of the web location landing page: (A). with or without displaying the institution's brand with or without (B). to provide information regarding the services it can offer; (C). thus, strengthening the potential for brand identity and improving user engagement.

It is certain the use of the Kiosk mode promotes concentration and improves the general productivity of users, but it also diminishes. Also is proven the Kiosk mode reduces to zero the cheating possibility on assessments which aim the measuring the skills and knowledge acquired by students. This was the reason for the integration of the given mode in the Learning Platforms or course management system (CMS), such as Moodle.

In our opinion, both types of analyzed digital anti-fraud tools - 2FA-type applications and Kiosk mode facilities for Web applications - have a broad spectrum of valuable features. We consider that these are able to improve multiple

didactic aspects not only in the context to ensure anti-fraud protection during assessments of learning outcomes. We believe that the described technological solutions also have the potential to increase the quality of the learner's acquisition of the assimilated material. Also, these may aid the student to produce in more depth reflections (exposed within the assessment activities), by creating an appropriate individual psychological and emotional comfort.

Using the solutions listed above, the teacher will not have to be the guardian of the assessed student, and the student could be sure that the inviolability of his identity will be respected; and the answers given by him during the evaluation will be measured and quantified in an impartial and standardized way (it means the same evaluation criteria will be applied as for his other colleagues during the assessment of learning outcomes).

4. Conclusions

The experience of combining several digital tools, such as those described in this article - of authentication applications that eliminate the possibility of unauthorized access to certain educational contents and/or Web locations with the use of Kiosk mode, including in the Moodle system - substantially reduces, and in some places, it even eliminates situations of fraud in the assessment of the learning objectives.

It is worth mentioning that such practices are implemented at the Technical University of Moldova. In particular, the accessing method of the available online several institutional microservices is achieved through double authentication (2FA) for all categories of users, from students and teaching staff to employees of the auxiliary, non-teaching staff, and also the administrative staff.

As for the use of the Kiosk mode, usually, it is personally configured by the teacher and/or Moodle course creator, as well as used for periodic, current, and/or final assessment activities that can be organized both online and in mixed - these are the facts that happen.

REFERENCES

Balmuș N. & Burlacu N. (2017) Manualul interactiv de informatica - repere metodologice de realizare și implementare în procesul de instruire. (Interactive computer science manual - methodological landmarks for development and implementation in the training process). In: *Processing of the 9-th International Conference of "Microelectronics and Computer Science" & the 6-th Conference of Physicists of Moldova, 19-21 October 2017, Chisinau, Moldova*. pp. 369-370.

Burlacu, N. (2016) Învățarea centrată pe student în formarea profesională la specialitățile de Informatică și Tehnologii Informaționale. (Student-centered

learning in vocațional training in the specialties of Computer Science and Information Technologies). *Revista de Ştiinţe Socioumane.* 1 (32), 45-52.

Burlacu, N. (2020a) Virtual classroom in the digital age: concept, product and applicability. *Journal of social sciences.* III (3), 11-17.

Burlacu, N. (2020b) Soluții IT pentru educația la distanță: realitate între concept și aplicabilitate. In: *Materialele Conferinței Naționale de Învățământ Virtual, CNIV 2020, 31 2020 Octombrie, Suceava, România.* Editura Universității din București. pp. 97-105.

Burlacu, N. (2021a) Elemente de dezvoltare și management ale unui curs plasat pe Moodle. In: Burlacu N. (ed.), Ababii V., Ciorbă Dm. etc. *Soluții pentru studii online în învățământul universitar ingineresc. Ghid de bune practici: Din experiența cadrelor didactice FCIM,* Chișinău: Editura „MS Logo" SRL. pp. 32-43.

Burlacu, N. (2021b) Evaluarea pe Moodle: de la idee la aplicare. In: Burlacu N. (ed.), Ababii V., Ciorbă Dm. etc. *Soluții pentru studii online în învățământul universitar ingineresc. Ghid de bune practici: Din experiența cadrelor didactice FCIM*. Editura „MS Logo" SRL, Chișinău. pp. 70-85.

Burlacu, N. (2021c) Aspects of assessment of students' activity in the seminar classes: problems and solutions. *Journal of Social Sciences.* IV(4), 63-74.

Burlacu, N. (2021d) Didactic transformations of the distance educational process in universities in engineering in (post) pandemic times. In: *The 17 th International Scientific Conference eLearning and Software for Education Bucharest, ELSE 2021, 22-23 April 2021, Bucharest, Romania.* Publisher: Adl Romania. Vol. 1, pp. 352-361. doi: 10.12753/2066-026x-21-045.

Burlacu, N. (2021e) Digitalization of university courses in the focus of educational management. In: *The 16th Interational Conference on Virtual Learning, ICVL 2021, 20 November 2021, Bucureşti, România*. Editura Universităţii din Bucureşti. pp. 23-32.

Burlacu, N. (2022a) Capstone Project: From Theory to Practice. In: *Processing of The International Conference on Virtual Learning, ICVL 2022, 25-26 November 2022, Bucharest, Romania.* vol. 17, pp. 63-75. https://doi.org/10.58503/icvl-v17y202205 [Accessed 30th June 2023].

Burlacu, N. (2022b) EdTech: Concept and Connections. In: *The 12 th International Conference on Electronics, Communications and Computing, ECCO 2022, 20-21 October 2022, Chisinau, Republic of Moldova.* Organizatori: UTM; FCIM. pp. 285-290. https://doi.org/10.52326/ic-ecco.2022/KBS.01 [Accessed 30th June 2023].

Burlacu, N. (2022c) Multilateralitatea procesului de evaluare a studenților în condițiile studiilor hibrid și/sau online (Multidimensionality of the student

assessment process in the conditions of hybrid and/or online learning). *Revista științifică - Studia Universitatis Moldaviae. Stiinte ale educatiei*. 5(155), 87-95.

Burlacu, N. (2022d) Procesul didactic digitalizat: viziuni și perspective privind managementul educațional (The digitized teaching process: visions and perspectives on educational management). *Akademos, Journal of science, innovation, culture and art (Akademos, Revistă de ştiinţă, inovare, cultură şi artă).* 1(64), 86-93.

Burlacu, N., Irimiciuc, S. D (2017) Produsele software de detectare a plagiatului: analiză din perspectiva principiilor interdisciplinarității (Plagiarism detection software: analysis from the perspective of the principles of interdisciplinarity). In: *Materialele Conferinței a XV-a Naționale de Învățământ Virtual „VIRTUAL LEARNING – VIRTUAL REALITY. Tehnologii Moderne în Educaţie şi Cercetare. MODELS & METHODOLOGIES, TECHNOLOGIES, SOFTWARE SOLUTIONS", 28 octombrie 2017, Bucureşti, România.* Editura Universității din București. pp. 69-76.

Burlacu, N. & Irimiciuc, S. D. (2018) Validarea conceptului STE(A)M din perspectiva modelelor ecosistemice de învățare (Validation of the STE(A)M concept from the perspective of ecosystem learning models). In: *Materiale din a XV-cea Conferinţă Naţională de Învăţământ Virtual „VIRTUAL LEARNING – VIRTUAL REALITY. Tehnologii Moderne în Educaţie şi Cercetare. MODELS & METHODOLOGIES, TECHNOLOGIES, SOFTWARE SOLUTIONS", 26-27 Octombrie 2018, Bucureşti, România.* Editura Universităţii din Bucureşti. pp. 120-126.

Cartaleanu, T. (2017) Evaluarea prin proiecte în cadrul cursurilor opționale pe aria curriculară "Limbă şi comunicare". In: *Probleme ale ştiinţelor socioumanistice şi modernizării învăţământului: materialele conferintei ştiintifice anuale a profesorilor şi cercetătorilor UPS „Ion Creangă". Universitatea Pedagogică de Stat „Ion Creangă"*, Chişinău, 2017. Tipogr. UPS „Ion Creangă". vol. 4 (seria 19), pp. 201-210.

Cartaleanu, T. (2018) Cursul opțional – oportunitate de testare a unor probe de evaluare. In: *Probleme ale științelor sociumanistice şi modernizării învățământului: materialele conf. şt. anuale a profesorilor şi cercetătorilor UPS „Ion Creangă". Universitatea Pedagogică de Stat „Ion Creangă", Chişinău, 2018*. Tipogr. UPS „Ion Creangă". Vol. 3, (seria 20), pp. 66-72.

Deinego, N. (2016) Testarea adaptivă. Mecanisme de realizare pe platforma moodle. *Ştiinţă, educaţie, cultură.* 1, 551-554.

Melentiev, E., Calmuțchi, L. & Cerbușca, El. (2021) Aplicarea metodelor interactive de predare, învățare și evaluare online la Chimie. In: *Materialele Conferinței Republicane a Cadrelor Didactice, 27-28 februarie 2021, Chişinău, Moldova.* Vol. 2, pp. 198-205.

Regulations Regulation (EU) (2016) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

UNESCO Institute for Statistics. (2012) *International Standard Classification of Education ISCED 2011*. http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf [Accessed 30th June 2023].