Управление на риск от измами при онлайн изпити

Александрина Мурджева

Managing the risk of fraud in online exams

Aleksandrina Murdzheva

Abstract:

The increasing use of online exams poses serious challenges to ensuring academic integrity. This report examines the risk of fraud in the digital exam environment and identifies the main threats, including unauthorized assistance, use of external resources and identity theft. Modern approaches to their limitation, technological and organizational, such as online proctoring, behavioral analysis and anomaly detection algorithms, are analyzed in the context of achieving a balanced approach between control, reliability and protection of personal data and the specificity of the number of participants. The report proposes a risk management approach that combines technological and organizational measures.

Keywords: online examination, academic integrity, risk management, cheating prevention, risk prevention stratgeies, Multi-layer strategy

For contacts: Aleksandrina Murdzheva, amurdjeva@unwe.bg

ВЪВЕДЕНИЕ

Дигитализацията на висшето образование фундаментално променя средата на академичното оценяване. Онлайн изпитите, които някога бяха допълнение към присъствената проверка на знания, се превърнаха в основен метод за оценка в много университети, и не само, по света. Тази промяна, предизвикана от пандемията COVID-19, донесе значителни ползи по отношение на достъпността и логистичната гъвкавост на образованието. Но това създаде нови и до голяма степен неизследвани уязвимости и предизвикателствата към академична етика и почтенност.

Резултатите от изследвания по темата са недвусмислени: измамите с онлайн изпити се се увеличили значително, тъй като оценяването се премести изцяло в дигитални среди. Докладваните онлайн измами са се увеличили от 29,9% преди пандемията до 54,7% по време на COVID периода — статистически значима разлика с голям ефект [4]. Появата на инструменти за генеративен изкуствен интелект поставя темата за академичната етика и почтенното участие в образователния процес в нова светлина. До 2025 г. 88% от студентите бакалаври във Великобритания съобщават, че използват генеративен AI за оценявана работа, което е увеличение спрямо 66% през предходната година [5].

Въпреки това университетите до голяма степен реагират реактивно, прилагайки индивидуални технически контроли без последователен систематичен подход. В настоящия доклад предлагаме тезата, че управлението на риска, дисциплина, добре установена във финансите, инженерството и информационната сигурност, предоставя рамка за управление риска, приложима и в процеса на проверка на знания. Систематичен подход към идентифициране, анализ и контрол на рисковете от измама позволява на институциите да вземат принципни, пропорционални решения за това кои контроли да се прилагат и на каква цена.

Мащабът на измамите с онлайн изпити: Емпирични доказателства

Преди да се проектира отговор за управление на риска, е необходимо да се разбере мащабът и естеството на проблема. Литература по темата онлайн измами на изпити значително се е увеличила от 2020 г. Таблица 1 обобщава ключовите открития в някои източници.

Таблица 1: Ключови статистики за преписване на онлайн изпити

Индикатор	Value
Процент на преписване на онлайн изпити по време на COVID-19 [4]	**54.7%**
Процент на преписване на онлайн изпити преди COVID-19 [4]	**29.9%**
Британски бакалаври, използващи GenAI за оценявана работа (2025) [5]	**88%**
Според студенти от Великобритания преписвали са с GenAI (2023/24) [6]	**22%**
Процент на преписване на неконтролирани изпити [7]	**70%**
Процент на преписване на изпити под надзор [7]	**15%**
Учениците са по-малко склонни да преписват, ако съществува риск от откриване [9]	**73%**
Преписващи ученици, които съобщават, че са били хванати [7]	**<2%**
Отговорите на изпита по ChatGPT незабелязани от човешки маркери [10]	**94%**
Ученици, обезкуравани от страх от обвинение в измама [5]	**53%**
Ученици, които не се притесняват от влиянието на измамата върху бъдещето [9]	**33%**

Няколко обобщения от тези данни заслужават специално внимани: **(a) разликата между нивото на преписване и степента на откриване е тревожна**: докато мнозинството ученици в неконтролирани условия проявяват нечестно поведение, по-малко от 2% от тези, които преписват, съобщават, че са били хванати. Това е сериозен неуспех в процеса по възпирането — ако очакваната цена на преписването е близо до нула, рационалните студенти ще мамят, независимо от изивканията. **(b) възходът на измамата с помощта на AI представлява качествена промяна в средата на заплахите**. Когато 94% от отговорите, генерирани от изкуствен интелект, остават незабелязани от човешки маркери, когато AI-генерираните отговори имат по-висок среден резултат от истинските студентски отговори [10], традиционният модел на текстова оригиналност като заместител на академична автентичност не успява. **(c) възпиращият ефект от наблюдението е реален и значим**. Разликата между 70% процент на преписване в неконтролирани условия и 15% под наблюдение-

намаление с 55 процентни пункта е един от най-големите ефекти от интервенция, документирани в литературата за академична почтеност.

Управление на риска: концептуални основи

Управлението на риска е систематичен процес за идентифициране, анализ, оценка и контрол на потенциални заплахи и уязвимости, с цел намаляване на тяхното негативно въздействие върху дадена дейност или организация [2][3]. Първоначално разработена в контекста на финансовия и инженерния риск, дисциплината постепенно се прилага в информационната сигурност, здравеопазването и от скоро в образователната администрация.

Основните елементи на процеса на управление на риска [3], са следните: (**a) Контекст на риска**: Основният слой, който определя кой носи отговорност за управлението на риска, какви са целите, какво ниво на риск е приемливо (толерантност към риск) и какви политики и рамки управляват процеса; (**b) Идентифициране на риска**: Систематичното откриване и описание на потенциални заплахи — в случая на онлайн изпити, пълния спектър от методи, чрез които студентът може да получи несправедливо предимство; **(c) Анализ на риска**: Преглед на всеки идентифициран риск по отношение на неговата вероятност (P) и потенциално въздействие (I); **(d) Оценка на риска**: Приоритизиране на рисковете чрез формулата за оценка на риска $R = P \times I$, обикновено представена чрез матрица на риска. Качествените и количествените представяния са приложими; **(e) Лечение на риска**: Избор и прилагане на подходящи контролни мерки. Възможностите за лечение включват избягване, смекчаване, прехвърляне, приемане, споделяне, диверсификация и планиране при извънредни ситуации; **(f) Мониторинг и контрол**: Постоянно наблюдение на рисковете и ефективността на мерките за контрол, актуализирано при промяна на обстоятелствата; **(g) Комуникация и докладване**: Гарантиране, че информацията за риска достига до правилните хора в точното време; **(h) Култура на риска**: Нагласите, поведението и ценностите на хората в организацията по отношение на риска. Без подходяща култура дори най-сложната рамка за управление на риска ще се провали.

Всеки от тези елементи има пряк еквивалент в управлението на интегритета на онлайн изпитите. За съжаление културата на риска, често се подценява: институция може да прилага цялостни технически контроли, като политическата неяснота или ниски нива на прилагане дават незначителни резултати.

Техники за управление на риска

Управлението на риска се отнася до избора на подходящ отговор на идентифициран риск. В контекста на измами при онлайн изпити, основните техники за превенция могат да се дефинират като: **(a) Избягване на риска** (Risk Avoidance): Премахване на дейността, която поражда риска. В контекста на изпита това може да означава отказ от провеждане на изпит в несигурна среда или замяна на изпитния формат с дизайн на оценка, който по същество има по-ниска риск от измами (например оценка, базирана на проекти). **(b) Намаляване на риска** (Risk Mitigation/reduce): Прилагане на мерки, които намаляват вероятността или последствията от измама. Това е най-често прилаганата обработка и обхваща пълния набор от технически и процедурни контроли. **(c) Прехвърляне на риска** (Risk Transfer): Прехвърляне на риска на трета страна. Използването на външно

сертифицирана платформа за прегледи - като Pearson VUE, Prometric или специализиран доставчик на надзор - представлява форма на прехвърляне на риска, прехвърляйки основната отговорност за сигурността на доставчика. **(d) Приемане на риск** (Risk Acceptance): Съзнателно приемане на риск, когато той е нисък или неизбежен. Институциите могат например да приемат определено ниво на дребни технически пропуски в онлайн платформа като присъща характеристика на дигиталната оценка. **(e) Споделяне на риска** (Risk Sharing): Разпределение на риска между множество участници. Комбинацията от автоматизирано и ръчно маркиране, или институционален и регулаторен надзор, е пример за споделяне на риска. **(f) Диверсификация** (Risk Diversification): Разпределяне на оценката в множество формати, така че нито един единствен вектор на измама да не компрометира цялата оценка. **(g) Планиране при извънредни ситуации** (Contingency planning): Поддържане на “План Б” — алтернативен път за оценка — в случай че първичните контроли се провалят.

Модел на разход-ползи за поведението на студентите при измама

Разбирането защо учениците мамят е предпоставка за разработване на ефективни контрамерки. Моделът ‚разход-полза‘ може да се дефинира като: студентите мамят, когато очакваната полза от преписването надвишава очакваната цена.

Измамата възниква, когато: Полза (измама) > Цена (измама)

Където: Полза = подобрение × вероятност за успех; Цена = тежест на санкцията × вероятност за откриване

Ползата от уравнението е голяма, когато: (а) изпитът е с високи залози [1], затова оценките имат голямо значение; (б) Налични са AI инструменти, които правят измамата бърза и с малко усилия; (в) дизайните на въпросите са статични и преизползвани, така че ключовете за отговори са вече познати.

Цената е ниска, когато: (а) степента на откриване е близо до нула; (б) санкциите са леки, неясни или непоследователно прилагани; (в) институционалната култура третира академичната почтеност като формалност.

Този модел влияе пряко избора на работеща стратегия за превенция. **Подходи, които се фокусират изключително върху техническо откриване, без да адресират страната на ползите ще имат ограничено въздействие**. Цялостната стратегия трябва едновременно да:

1. Намалява ползата от преписването (чрез нови оценъчни стратегии).
2. Увеличава разходите за измама (чрез достоверни механизми за откриване и смислени санкции).
3. Увеличава ползата от честните усилия (чрез обратна връзка, видимо признаване на академичните постижения и култура, която цени истинското учене).

Целта на модела не е да се елиминира напълно измамата, практически непостижима цел, а да се измести уравнението между разходи и ползи така, че измамата да изглежда рисковано, неефективно и недостатъчно усилието в сравнение с простото изпълнение на работата, с други думи да се предпочете принципа „по-изгодно ми е да спазвам правилата, от колкото да ги нарушавам“.

Стратегии за превенция: многослойна рамка

Нито една мярка за превенция и контрол на риска, приложона самостоялтено, не е достатъчна, за да се справи с пълния спектър от рискове от измами при онлайн изпити. В литературата се подкрепя многопластовия подход [4], при който провалът на един контрол се компенсира от присъствието на други. Дефинираме това като **многослойна стратегия срещу измамата**, при която дизайнът на оценката, механизмите за откриване и факторите на учебната среда заедно увеличават разходите и намаляват ползите от измамата, като по този начин насърчават честно поведение чрез рационално вземане на решения.

Наличните стратегии могат да бъдат организирани в пет основни категории.

(a) Проверка на самоличността: Самоличностната измама, трета страна, която провежда изпита вместо студента, е един от най-сериозните рискове при дистанционната оценка. Контролите включват многофакторна проверка на идентичността при влизане (проверка на снимка в комбинация с разпознаване на лице), непрекъснато съвпадение на лица по време на сесията и анализ на динамиката на натискания на клавиши за откриване на аномалии в моделите на писане. Основните рискове, свързани с тези контроли, са поверителността (съответствие с GDPR, съхранение на биометрични данни) и фалшиви положителни резултати, които могат да поставят ученици с определени увреждания или от определени демографски среди; (b) Наблюдение и мониторинг: Живото или автоматизирано наблюдение остава най-мощният възпиращ фактор, идентифициран в литературата, като намалява нивата на измами от приблизително 70% на 15%. Съвременните системи за наблюдение работят на няколко нива: браузъри за заключване, които възпрепятстват достъпа до външни приложения; Мониторинг на уебкамери с изкуствен интелект, който открива подозрителни модели на поглед, множество лица или аудио аномалии; и анализи след изпита, които отбелязват статистически нередности в моделите на отговори или сходствата на отговорите. Етичните и регулаторните рискове, свързани с наблюдението, са значителни: непрекъснатото записване на ученици в домовете им повдига съществени въпроси относно поверителността, достойнството и пропорционалността; (c) Оценка и дизайн на въпроси: Дизайнът на оценката е може би най-устойчивата дългосрочна стратегия, защото намалява стойността на измамата. Ключови подходи включват: Рандомизирани пулове от въпроси, Персонализирани набори от данни, Въпроси, базирани на сценарии и приложни въпроси, Отворена книга и ‚дизайн за вкъщи‘, (d) Устен преглед; (e) Плагиатство и откриване на използване от AI; (f) Политики за почтеност и академична култура

Стратегии за превенция: реактивни и проактивни

Изхождайки от модела ‚разход-полза‘ към проблем с измамите по време на онлайн изпит, е възможно да се дефинират два подхода**: (a) реактивен (ограничаващ):** Силно реактивните стратегии дават своите резултати, но бързо се изчерпват. **(b) активен (мотивиращ)**. промяна на поведението към отказа от измамно такова по време на изпит. Прилагане на техники за увеличаване на ползите от почтено поведение и намаляване на ползите от измамното, е дългосрочното решение на проблема.

Пропорционалност и минимални стратегически набори

Основен принцип в управлението на риска е пропорционалността: сложността на контрола трябва да е съобразена с залозите на защитаваната дейност. Таблица 2 представя рамка за съпоставяне на минималните стратегически набори към три нива на оценяване.

Таблица 2: Минимални набори от стратегии по вид изпит

Тип изпит	Минимален препоръчан набор от стратегии
Професионален изпит с високи залози [11]	Всички стратегии: проверка на самоличността, наблюдение на живо, браузър за локдаун, рандомизирани пулове с въпроси, политика за почтеност, откриване на изкуствен интелект/плагиатство, устна вива проба
Изпит за университетска степен	Дизайн на въпроси (случайни пулове + времеви лимити), мониторинг на записи от сесии, откриване на плагиатство и AI, политика за почтеност / кодекс за чест
Изпит с ниски залози в класната стая	Оценяване извън традиционната изпитна рамка (базирана на проект, портфолио, рефлективен дневник) — преминаване към формати, където преписването има ниска възвръщаемост

Рисковете на стратегиите за управление на риска

Отговорният анализ на управлението на риска трябва да признае, че самите стратегии също носят рискове. Ето едно примерно обобщение

Таблица 3: Вторични рискове, свързани със стратегии срещу измама

Стратегия	Риск от GDPR	Етичен риск	Технически риск	Препоръчителна употреба	
Проверка на самоличността	**Високо**	**Високо**	**Средно**	Само за изпити с високи залози	правната основа за обработка на данни от специални категории
Наблюдение на живо / мониторинг	**Високо**	**Високо**	**Средно**	Изпит с високи залози	Етичните измерения: ученици с увреждания, студенти от по-ниски

Стратегия	Риск от GDPR	Етичен риск	Технически риск	Препоръчителна употреба	
					социално-икономически среди, които споделят жилищни пространства, и студенти в юрисдикции с ненадеждна интернет свързаност
Браузър за заключване	Средно	Средно	Високо	Изпити със среден до висок залог	висок технически рисков профил.
Дизайн на въпроси (рандомизирани пулове)	Ниско	Средно	Средно	Всички видове	най-нисък комбиниран рисков профил
Политики за почтеност и кодекси на честта	Ниско	Средно	Ниско	Всички видове	
Откриване на плагиатство / използване от изкуствен интелект	Средно	Високо	Средно	Университет и професионална кариера	фалшиви положителни резултати

ЗАКЛЮЧЕНИЕ

Измамите с онлайн изпити не са нов проблем, но мащабът, сложността и обществените последици значително са се увеличили в ерата на масовото дигитално оценяване и генеративния изкуствен интелект. Управлението на риска предоставя системен подход и и на тази база може да се дефинира полезна рамка за справяне с този проблем. Чрез прилагане на систематичната логика на идентифициране, анализ, оценка и третиране на риска, институциите могат да вземат принципни, пропорционални решения за това кои контроли да прилагат и на каква цена. Основното заключение на този анализ е, че нито един контрол не е достатъчен. Предотвратяването на измами изисква цялостен подход - нито една стратегия, взета сама по себе си, не е достатъчна.

Към този проблем е възможно да се подходи реактивно (ограничаващо) или активно (мотивиращо). Силно рестктивните стратегии дават своите резултати, но бързо се изчерпват. Изборът на акивни стратегии, промяна на поведението към отказа от измамно такова по време на изпит, е дългосрочното решение на проблема.

ЛИТЕРАТУРА

1. French, S., Dickerson, A., & Mulder, R. A. (2024). *A review of the benefits and drawbacks of high-stakes final examinations in higher education*. Higher Education, 88, 893–918; https://doi.org/10.1007/s10734-023-01148-z

2. Hopkin, P. (2018). *Fundamentals of Risk Management* (5th ed.). Kogan Page.

3. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. Geneva: ISO

4. Newton, P. M., & Essex, K. (2024). *How common is cheating in online exams and did it increase during the COVID-19 pandemic? A systematic review*. Journal of Academic Ethics, 22, 323–343; https://doi.org/10.1007/s10805-023-09485-5

5. HEPI / Kortext. (2025). *Student Generative AI Survey 2025*. Higher Education Policy Institute; https://www.hepi.ac.uk/reports/student-generative-ai-survey-2025/

6. Newton, P. M. (2025*). How vulnerable are UK universities to cheating with new GenAI tools? A pragmatic risk assessment*.*Assessment & Evaluation in Higher Education*,*50*(8),1332–1343.Taylor&Francis, https://doi.org/10.1080/02602938.2025.2511794

7. Meazure Learning. (2024). *By the Numbers: Academic Integrity in Higher Education*. https://www.meazurelearning.com/resources/by-the-numbers-academic-integrity-in-higher-education

8. Scarfe, P., et al. (2024). *A real-world test of artificial intelligence infiltration of a university examination.* University of Reading. Also cited in Turnitin AI Trends Report 2024.

9. Noorbehbahani F, Mohammadi A, Aminazadeh M. *A systematic review of research on cheating in online exams from 2010 to 2021*. Educ Inf Technol (Dordr). 2022;27[6]:8413-8460. doi: 10.1007/s10639-022-10927-7. Epub 2022 Mar 7. PMID: 35283658; PMCID: PMC8898996.)