УДК 004.056.5

Гдадка В.
Салієва О.В.

АНАЛІЗ ІСНУЮЧИХ СИСТЕМ КОНТРОЛЮВАННЯ ДІЙ КОРИСТУВАЧА

Вінницький Національний Технічний Університет

Анотація

У роботі проведено аналіз існуючих систем контролювання дій користувача, які застосовуються для забезпечення безпеки та об'єктивності у процесах тестування й навчання. Особливу увагу приділено сучасним технологіям моніторингу, їх перевагам, обмеженням та можливостям інтеграції з освітніми платформами.

Ключові слова: Захист, контроль дій, інформаційна безпека.

Abstract

The article analyzes the existing systems for monitoring user actions used to ensure security and objectivity in testing and learning processes. Particular attention is paid to modern monitoring technologies, their advantages, limitations, and possibilities of integration with educational platforms.

Key words: Protection, move detection, information security.

Вступ

У сучасному світі цифрових технологій забезпечення об'єктивності та безпеки під час роботи з комп'ютерними системами є важливим завданням. Особливо актуальним це питання стає у сфері тестування знань, де шахрайство та несанкціоновані дії можуть суттєво впливати на якість оцінювання. У роботі розглядаються існуючі системи контролювання дій користувача, їхні технологічні особливості, переваги та обмеження, а також перспективи використання в освітніх і корпоративних середовищах.

Дослідження

ProctorU є сучасною платформою для дистанційного прокторингу, яка спрямована на забезпечення академічної чесності та об'єктивності під час проведення онлайн-іспитів. Ця система поєднує технології штучного інтелекту, відеоспостереження та біометричної ідентифікації, що дозволяє забезпечувати високий рівень контролю за поведінкою користувачів у реальному часі. Однією з ключових функцій ProctorU є живий прокторинг, за якого кваліфіковані проктори контролюють процес іспиту, спостерігаючи за користувачем через вебкамеру, аналізуючи його дії та втручаючись в процес у разі порушень правил. Крім цього, система підтримує автоматизований моніторинг, який базується на використанні алгоритмів штучного інтелекту. Ці алгоритми здійснюють аналіз поведінки користувача, включаючи рухи голови, напрямок погляду та активність на екрані, що дозволяє знизити потребу у безпосередньому людському втручанні [1].

ProctorU також впроваджує перевірку особи користувача перед початком іспиту, використовуючи біометричні дані та перевірку офіційних документів. Окрім цього, система здатна моніторити робоче середовище користувача, аналізуючи відеопотік для виявлення сторонніх осіб або заборонених матеріалів, які можуть порушувати чесність іспиту. Перевагою платформи є її гнучкість, оскільки користувачі можуть проходити тестування з будь-якої локації, що має доступ до мережі Інтернет. Інтеграція ProctorU з популярними системами управління навчанням спрощує процес її впровадження у навчальні заклади та корпоративні середовища [1].

Проте впровадження ProctorU супроводжується низкою викликів. Зокрема, використання біометричних даних та відеоспостереження викликає питання щодо конфіденційності інформації. Технічні вимоги до обладнання та інтернет-з'єднання можуть створювати перешкоди для певних категорій користувачів. Крім того, постійний моніторинг під час іспитів може спричиняти стрес у студентів, що негативно впливає на їхню продуктивність. Незважаючи на ці виклики, ProctorU залишається ефективним інструментом для забезпечення чесності в онлайн-іспитах, демонструючи значний потенціал у впровадженні прозорих і надійних методів оцінювання знань.

Examity – це провідна платформа для дистанційного прокторингу, розроблена для забезпечення цілісності та об'єктивності онлайн-іспитів у навчальних закладах, сертифікаційних організаціях та корпоративних середовищах. Платформа пропонує гнучкі рішення, які поєднують автоматизований та

живий прокторинг, що дозволяє адаптувати процес контролю відповідно до специфічних потреб кожної організації.

Однією з ключових особливостей Examity є її здатність інтегруватися з існуючими системами управління навчанням (LMS), що спрощує процес впровадження та використання платформи. Під час іспиту Examity здійснює автентифікацію особи студента за допомогою багатофакторної перевірки, включаючи ідентифікацію за фотографією, перевірку документів та біометричні дані. Це гарантує, що іспит складає саме той студент, який зареєстрований на курс.

Платформа також забезпечує моніторинг поведінки студента під час іспиту, використовуючи як автоматизовані алгоритми, так і прокторів. Автоматизовані системи здатні виявляти підозрілу активність, таку як несанкціоновані спроби доступу до інших ресурсів або аномальні рухи. У разі виявлення таких дій інформація передається проктору для подальшого аналізу та прийняття рішення.

Examity надає детальні звіти про результати іспитів, включаючи інформацію про будь-які порушення або підозрілі дії, що дозволяє інструкторам та адміністраторам приймати обґрунтовані рішення щодо результатів тестування. Крім того, платформа підтримує глобальний доступ, що дозволяє студентам з різних куточків світу складати іспити в зручний для них час, забезпечуючи при цьому високий рівень безпеки та цілісності процесу [2].

Завдяки поєднанню передових технологій, гнучкості та зручності використання, Examity стала надійним партнером для багатьох освітніх установ та організацій, які прагнуть забезпечити чесність та об'єктивність онлайн-оцінювання.

Respondus – це комплексне програмне забезпечення, призначене для створення, управління та захисту онлайн-оцінювань у навчальних закладах. Основними компонентами є Respondus 4.0, LockDown Browser та Respondus Monitor.

Respondus 4.0 дозволяє викладачам створювати та керувати екзаменами в автономному режимі з використанням знайомого середовища Windows, а також публікувати їх безпосередньо в системах управління навчанням (LMS), таких як Blackboard, Canvas, Moodle та інші. Це значно спрощує процес підготовки та розповсюдження тестових матеріалів, забезпечуючи ефективність та зручність для викладачів.

LockDown Browser – це спеціалізований веб-браузер, який блокує можливість студентам друкувати, копіювати, переходити на інші веб-сайти або запускати інші додатки під час проходження онлайн-іспитів. Це забезпечує контрольоване середовище тестування, мінімізуючи ризики академічної недоброчесності [2].

Respondus Monitor доповнює функціональність LockDown Browser, використовуючи веб-камеру для запису студентів під час складання іспитів. Ця система автоматично аналізує відеозаписи, виявляючи підозрілу активність, що дозволяє викладачам переглядати результати прокторингу та приймати обґрунтовані рішення щодо достовірності виконання роботи.

Інтеграція цих інструментів у навчальний процес сприяє підвищенню академічної доброчесності та забезпечує надійність онлайн-оцінювань. Використання Respondus дозволяє навчальним закладам ефективно впроваджувати дистанційне навчання та оцінювання, зберігаючи при цьому високі стандарти якості освіти [3].

Proctorio – це комплексна платформа для дистанційного прокторингу, яка надає послуги верифікації особи та моніторингу іспитів для понад 4 000 освітніх, корпоративних та державних установ по всьому світу. У 2021 році Proctorio забезпечила проведення більше 30 мільйонів іспитів, демонструючи свою масштабованість та надійність.

Платформа інтегрується з більшістю систем управління навчанням (LMS) та сторонніми платформами оцінювання через розширення браузера, що забезпечує зручність використання для користувачів. Proctorio пропонує набір налаштовуваних опцій, включаючи блокування, запис та верифікацію, що дозволяє адміністраторам іспитів адаптувати рівень безпеки відповідно до потреб конкретного іспиту.

Однією з ключових особливостей Proctorio є низькі вимоги до пропускної здатності інтернет-з'єднання, що робить її доступною для користувачів з обмеженим доступом до швидкісного інтернету. Платформа також пріоритизує конфіденційність та безпеку користувачів, використовуючи наскрізне шифрування для захисту даних [3].

Proctorio надає можливість вибору між автоматизованим та живим прокторингом. Автоматизований прокторинг використовує алгоритми штучного інтелекту для моніторингу поведінки студентів під час іспиту, виявляючи підозрілу активність. Живий прокторинг передбачає безперервний нагляд проктора, який може негайно втрутитися у разі порушень. Крім того, Proctorio пропонує послугу професійного огляду, де співробітники аналізують записи іспитів на предмет порушень цілісності.

Завдяки своїй гнучкості, масштабованості та акценту на конфіденційності, Proctorio є популярним вибором серед освітніх установ та організацій, які прагнуть забезпечити чесність та об'єктивність

дистанційних іспитів. Однак, як і будь-яка технологія дистанційного прокторингу, Proctorio зіштовхується з викликами, пов’язаними із захистом конфіденційності даних та технічними обмеженнями, що вимагають постійної уваги та вдосконалення [4].

У таблиці 1 здійснено порівняння проаналізованих систем.

Таблиця 1 − Порівняння систем контролювання дій

Характеристика	Proctorio	Respondus	Examity	ProctorU
Тип прокторингу	Автоматизований або живий, з можливістю вибору рівня контролю	Автоматизований (LockDown Browser) та живий (Monitor)	Живий, автоматизований або гібридний підхід	Живий прокторинг із автоматизованим моніторингом
Моніторинг оточення	Аналіз відеопотоку для виявлення сторонніх осіб або заборонених матеріалів	Забезпечується через LockDown Browser та відеомоніторинг (Monitor)	Використовує вебкамеру для запису відеопотоку та моніторингу оточення	Виконується через постійний відеозапис і спостереження
Автентифікація	Використовує багатофакторну перевірку: фото, ID, біометрія	Перевірка особи через вебкамеру перед початком тесту	Включає ідентифікацію за фото, перевірку документів та біометрію	Фото, документи та перевірка особи проктором у реальному часі
Інтеграція з LMS	Повна інтеграція з більшістю популярних LMS (Canvas, Moodle, Blackboard тощо)	Інтегрується з усіма популярними LMS	Легка інтеграція з LMS, можливість масштабування для різних платформ	Інтегрується з популярними LMS, включаючи Canvas, Moodle та Blackboard
Конфіденційність	Наскрізне шифрування даних для забезпечення безпеки. Низькі вимоги до пропускної здатності інтернету	Дані зберігаються локально або передаються зашифрованими	Високий рівень захисту даних, однак можуть виникати питання щодо збереження конфіденційності користувачів	Застосовує політики конфіденційності, але потребує зберігання великих обсягів відео та особистих даних
Технології AI	Використовує штучний інтелект для аналізу поведінки, автоматичне виявлення підозрілої активності	Автоматизація через Monitor, але більше залежить від правил тестування, ніж від складного аналізу AI	Поєднання автоматизації та участі проктора, аналіз підозрілих дій здійснюється як проктором, так і алгоритмами	Використовує AI для автоматичного виявлення порушень поряд із живим моніторингом
Можливості кастомізації	Високий рівень кастомізації налаштувань для різних рівнів безпеки	Можливість налаштування політик для тестування, але з обмеженим інтерфейсом	Гнучкі налаштування залежно від потреб організації чи інструктора	Мінімальні опції налаштувань, основний акцент на простоті використання
Глобальне використання	Підтримує багатомовні інтерфейси та адаптацію до різних країн	Використовується переважно у Північній Америці, обмежена адаптація до інших ринків	Широко використовується у США, але доступна для користувачів у всьому світі	Глобально розповсюджена платформа з підтримкою різних часових зон
Переваги	Висока масштабованість, низькі технічні вимоги, можливість автоматизації процесу	Блокування доступу до сторонніх ресурсів через LockDown Browser, простота використання	Інтеграція живого прокторингу з автоматизованими системами, гнучкість у налаштуваннях	Простота використання, високий рівень довіри до системи завдяки участі кваліфікованих прокторів
Недоліки	Висока залежність від інтернет-з'єднання, можливі питання конфіденційності	Складнощі з інтеграцією складних AI-рішень, відсутність моніторингу поза екраном	Можливі технічні проблеми з відеоспостереженням та приватністю даних	Високі технічні вимоги, можливість стресу у користувачів через постійний контроль

Різноманітність проаналізованих систем відображає широкий спектр підходів до забезпечення безпеки, кожен з яких орієнтований на вирішення конкретних завдань.

Висновок

Досліджувані платформи – Proctorio, Respondus, Examity та ProctorU є ефективними інструментами для забезпечення чесності та об'єктивності під час онлайн-іспитів. Вони відрізняються підходами до прокторингу, рівнем інтеграції з LMS, можливостями кастомізації та використанням технологій штучного інтелекту. Proctorio і Examity вирізняються гнучкістю та широкими можливостями налаштувань, тоді як Respondus забезпечує надійність завдяки спеціалізованому браузеру LockDown. ProctorU пропонує живий прокторинг із високим рівнем довіри. Вибір платформи залежить від потреб організації, доступних ресурсів та вимог до безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Understanding Multi-Factor Authentication (MFA) Principles [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.securitymagazine.com/mfa-principles-guide/.
2. Implementing Biometric Authentication for Enhanced Security [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.biometricupdate.com/authentication-implementation.
3. Advances in Public Key Infrastructure (PKI) Systems [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.cybersecurityjournal.org/modern-pki-systems.
4. Encryption Techniques in Cloud-Based Authentication [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.cloudsecurityalliance.org/encryption-authentication-guide/.

Гадка Вікторія – студентка групи КІТС-23М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: gladka.viktoria@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Gladka Viktoria. – student of KITS-23M group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail gladka.viktoria@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com