Добри практики за контрол на обучаемите при тестово изпитване онлайн

Явор Здравков Дечев

Good practices for supervising learners in online test taking

Yavor Zdravkov Dechev

Abstract:
The article presents some good practices for supervising learners in online testing. The technical parameters, potential risks, and options for counteracting unregulated student practices when conducting distance exams in an electronic environment are considered**.**
Keywords: Moodle, test, secure browser, cyber security, video conferencing

For contacts: Yavor Dechev, National Military University - Artillery, Air Defense and CIS Faculty, dechco99@yahoo.com

ВЪВЕДЕНИЕ

Внезапно наложилата се практика да обучение от разстояние в електронна среда (ОРЕС) във всички образователни степени, срещна недостатъчно подготвени преподавателите за противодействие на нерегламентирани опити и практики от обучаемите за въвеждане в заблуда и опити за преписване при неприсъствен и в онлайн-вариант на провеждане на изпитите и оценяването на придобитите знания.

Сертификационни центрове

В средите извън образователната сфера често се посочват сертификационните центрове като образец за компютърно-базирано изпитване. Сравнявайки ги с начините на изпитване в средното и висше образование се посочва, че последните не могат да бъдат използвани за котрол на знанието поради отворения си характер и възможността за преписване в онлайн среда.

Като пример ще се посочи сертификационния център на Pearson Vue. Такъв се намира и на територията на катедра „Информационни технологии“ на ВВМУ „Н.Й.Вапцаров“, гр. Варна. Изграждането и експлоатацията на такъв център задължително трябва да отговарят на строго определени параметри. Изпитваните решават онлайн тестове, но в присъствена форма. Те се намират в изолирана стая, в контролирана среда. Работните места на изпитваните и на администратора на центъра, трябва да отговарят на специфични архитектурни параметри, като се допуска в залата да има максимум 100 работни станции, но най-често те са под 10 работни места за изпитване/оценяване. Като пример може да се посочи, че центърът на Pearson Vue във ВВМУ разполага само с места за обучаеми и едно за администратора. Всички работни станции трябва да притежават специфични хардуерни характеристики и да работят с точно определен софтуер. Достъпът до Интернет трябва да бъде високоскоростен, с определени параметри, които пряко зависят от броя на работните станции. Всеки изпитван работи в среда на защитен браузер, без възможност за контакт с други хора и е наблюдаван минимум чрез две видеокамери.

Pearson Vue предоставя достъп до няколко хиляди онлайн изпити, но те основно са насочени в ИТ сферата и са на определени фирми, които предоставят онлайн обучение (Microsoft, NetApp, Oracle, Cisco, VMware, CompTIA и др.). Не е възможно определено висше учебно заведение да предостави своите изпитни форми.

Сертификационните центрове не могат да бъдат използвани за масово онлайн изпитване на студенти и ученици, поради следните причини:

- изпита се провежда в присъствена форма;
- малък брой работни места;
- строги изисквания към сертификационния център;
- тестове на определени фирми;
- висока цена на изпита (добавена е към сумата, изисквана за определения тест).

Полагането на изпит в подобен център се използва единствено за надграждане на знанията в професионалната сфера и получаване на допълнителни сертификати.

Онлайн изпитване на студенти и ученици

Кризисното преминаване в неприсъствена форма на обучение откроi голяма част от недостатъците на онлайн образованието и в частност на изпитването в онлайн среда.

Някои от откроените най-често срещани затруднения и пропуски могат да се обобщят до следните характеристики: липсва пряк контакт между преподавателя и изпитваните; наличие на негарантирана Интернет връзка; възможност за технически неизправни крайни устройства (компютър, лаптоп, слушалки микрофон, камера и др.); ограничено или липсващо наблюдение на средата около изпитвания, което води до лесно компрометиране на достоверността на изпита; ниска компютърна грамотност и неразбиране технологията на онлайн обучението от част от образователната общност - от академичния и административния състав.

В катедра „Информационни технологии“ на ВВМУ „Н.Й.Вапцаров“ първите семестриални изпити в неприсъствена форма се проведоха през лятото на 2020 г. Електронно-базираното обучение е изградено на базата на общ модел, който интегрира асинхронна система за дистанционно обучение Moodle и синхронната система за видеоконферентни връзки Microsoft Teams [1].

Дългогодишният опит за работа в среда на Moodle и няколкото семестъра, проведени изцяло в онлайн среда, позволиха да се апробират различни варианти и да се изведат редица работещи механизми, чрез които да се противодейства на недобросъвестното поведение на студентите и да не се допускат действия за въвеждане в заблуда и да се преустановят опити за преписване.

Изведените в статията „добри практики“, които могат да бъдат използвани при контрол на знанието при онлайн изпити, са насочени в няколко направления: методическо, техническо и киберсигурност.

По отношение на техническия компонент и предварителните настройки на системата за електронно-базирано обучение, първоначално могат да бъдат посочени някои процедури и настройки, извършвани в LMS Moodle. Могат да се посочат следните стъпки:

1. Създаване на отделен курс в Moodle, в който се намират изпитните тестове или задания. Записването се извършва единствено от преподавателя, водещ дисциплината. Достъп до този електронен курс имат само допуснатите до изпит студенти/курсанти.
2. Интерфейсът на Moodle позволява скриването на курсове или отделни модули в тях. Самият курс с изпитни материали), както и тестът могат да се направят видими за студентите в точно определен период от време, в който да се реализира изпитът едновременно за всички студенти от групата/курса.
3. В настройките на теста могат да бъдат заложени следните ограничения:
   - Тестът да бъде е активен в точно определен период от време.
   - Ограничение в броя на възможните опити за решаване на теста или връщане към предходно даден отговор на въпрос, като по този начин се елиминира възможността студентът да предостави на друг паролата за достъп до своя профил.
   - Задаване на парола за достъп до теста, като е желателно, ако групи със студенти са няколко, паролата да бъде сменяна за всяка от тях.
4. Ако изпитът се провежда в присъствена форма, допълнително в настройките на теста може да бъде зададено ограничение по мрежов адрес, достъпен само от определени компютърни системи в съответната катедра.
5. Инсталиране в Moodle на плъгина за защитен браузер (SEB - safe exam browser или подобен) и използването му към всеки тест.
6. Решаването на примерни тестове за самоподготовка от обучаемите в среда на SEB преди финалния изпит.
7. Включване в Moodle на плъгин за лицево разпознаване и за визуално следене движението на главата на обучаемия.

Използването на защитен браузер, в случая SEB, намалява драстично вероятността студентът да използва компютъра, за да търси и намери верните отговори или да запише въпросите от теста.

Допълнително ограничаване на преписването от страна на студентите е възможно и чрез усложняване на теста. Стандартно, в онлайн тестовете на ИТ фирмите (Microsoft, Cisco, Sun и др.), времето за отговаряне на един въпрос е под 1 минута. Ако въпросът е сложен, мултидисциплинарен, от отворен вид с изискване за написване на текст, тогава времето за изпълнение може да бъде увеличено. Желателно е времетраенето за решаване на целия тест да бъде така разчетено, че студентите да нямат време за опити за търсене на верните отговори в други източници – Internet, предоставени учебни материали в електронен или хартиен формат, чат с други хора.

Включването в изпита на различни типове въпроси провокира студента да мисли в момента, а не да отговаря машинално с маркиране на един радиобутон. Така ще се намали евентуалното оставащо време до приключването на теста, което може да се използва за „преписване“. Разнообразните типове задачи и въпроси в съдържанието на изпитното задание/тестовата диагностична батерия с тестови въпроси и задачи, провокират обучавания и оценяван в момента студент/курсант да извършва сложни мисловни операции (анализ, синтез, дискриминиране, екстраполация на данни и знания и т.н.), което възпрепятства

достигането да правилния/верния отговор чрез преписване или извличане на информация от наличен информационен ресурс.

Създаването на банка с поне 3 пъти по-голям брой въпроси от необходимите за конкретния тест, намалява вероятността за запомняне / снимане на всички възможни въпроси от теста и позволява да се генерират различен уникален вариант на теста за всеки отделен обучаван и оценяван студент/курсант.

Наблюдението на действията на студентите при изпит в онлайн среда се извършва посредством системата за видеоконферентна връзка. За да се осигури по-добра разделителна способност и видимост на обстановката около изпитвания онлайн студент, е желателно на един компютърен екран при преподавателя, на стационарен монитор с диагонал минимум 23 инча, да се визуализират екраните от камерите на максимум 8-10 студенти. Въпреки че някои от платформите да позволяват едновременно свързване към 32-64 камери, то реалният контрол върху студентите в такъв случай е невъзможен. В най-добрият случай може да се наблюдава само дали студентът е пред камерата или дали връзката е прекъсната. При голям брой изпитвани обучаеми се препоръчва изображението от системата за видеоконферентна връзка да бъде разпределено на няколко монитора, разположени един до друг, като всеки от тях визуализира максимум 8 камери. Сам преподавател трудно може да следи повече от 2-3 екрана, като всеки от тях показва информация от камерите на максимум 8 студенти. При нарастване на броя на едновременно изпитваните обучаеми е препоръчително в процеса на изпита да бъдат ангажирани няколко преподаватели, които да осъществяват мониторинг на информацията от камерите на студентите, за да не се допускат нерегламентирани действия, които биха ощетили достоверността на изпитния процес и обективното наличие на знание от студента.

Препоръчва се по време на целия цикъл на онлайн изпит да се извършат следните процедури:

- Запис на сесията във видеоконферентната система (от започването на предварителния инструктаж до напускане на „стаята“ от последния студент).
- Запазване на видеофайла в срок, указан в правилниците на съответното ВУ.
- Задължително наличие от студентите на втори канал за онлайн връзка (смартфон). Той да се използва както за следващата процедура, така и като резервен вариант за контакт с преподавателя.
- По време на теста преподавателя последователно изисква всеки студент да си включи камерата на смартфона (или подвижна камера към компютъра), с която да покаже лицето си, стаята, в която се намира и задължително екрана на компютъра, със стартиран изпитен тест в Moodle.
- След приключване на теста преподавателят, използвайки логфайловете от Moodle, може да провери дали по време на изпита даден акаунт на студент е влязъл в системата от IP адреси. Най-често това се получава, когато студентът е дал достъп на друг човек да му реши теста.
- При съмнение за компрометиране на изпита, е необходимо да се направи допълнителна проверка на видеофайлове от плъгин за лицево разпознаване и за визуално следене движението на главата на обучаемия.

При онлайн обучението съществува голяма вероятност за кибератака на компютъра на преподавателя от страна на студентите. Пробивът в сигурността може да доведе до пълно компрометиране на изпита. Допълнително, студентите могат да имат достъп до лични данни на самия преподавател или на личния състав на катедрата, факултета или ВУЗ, с което да се доведе до дискредитиране на цялото учебно заведение или до изтичане на класифицирана или чувствителна информация.

За се подобри защитата на персоналния компютър на преподавателя могат да бъдат изпълнение следните препоръки [2,3,4]:

- включена антивирусната защита, като редовно се обновяват вирусните дефиниции;
- периодично да се извършва проверка със софтуер против malware;
- задължително да се извършва проверка с антивирусен софтуер на файловете, които са изпратени от студентите;
- да не се предоставя дистанционен достъп на студентите до компютъра на преподавателя чрез системата за видеоконферентна връзка;
- при осъществяване на видеоконферентна връзка, преподавателят да използва отделен десктоп (Windows 10 и по-нови версии на ОС) и браузер само за връзка с обучаеми;
- да се визуализира минимална информация за личния компютър (инсталирани програми, използван софтуер, десктоп);
- да се използва служебен емайл за контакт със студентите;
- по възможност да не се предоставя личен акаунт в социалните мрежи.

Предложените мерки могат да бъдат използвани в ежедневната работа на академичния и на административен състав на учебното заведение. Ако служителят работи в сферата на сигурността или по национални / международни проекти, свързани със сигурността, то предложените практики трябва да бъдат задължителни, а не препоръчителни. Всички те трябва да бъдат разписани в Правилници и Наредби на конкретното ВУ или учреждение. Като пример могат да се посочат няколко учебни заведения (НВУ, ВВВУ, ВВМУ, ВА, Института по отбрана, Академията на МВР), които провеждат онлайн обучение и в същото време участват в изпълнение на дейности по Национална научна програма „Сигурност и отбрана“, боравят с чувствителна информация и имат отговорности, свързани с осигуряване на националната сигурност.

Въпреки множеството си предимства, провеждането на изпити в онлайн формат води и до допълнителни затруднения. Не всички преподаватели имат необходимата техническа и методическа подготовка, както и желание за работа в онлайн среда. Създаването на голям брой въпроси за тестовете изисква допълнително време и ангажираност, които често не могат да бъдат компенсирани финансово. По време на самия изпит преподавателят допълнително се натоварва физически да следи камерите на обучаемите. Проверката на логфайловете в Moodle изисква време. При съмнение за компрометиране на изпита, преподавателят допълнително заделя време за проверка и на видеозаписите от системите за видеоконферентна връзка и за лицево разпознаване. За съхранение на последните е необходимо голямо дисково пространство, при което видеофайлът само от един изпит може да достигне 2-3 GB. Увеличаването броя

на изпитваните, увеличава и броя на отделните файлове от системата за лицево разпознаване. Времето за съхранение на доказателствения материал е различно и зависи от правилата на всяко учебно заведение. Стандартно, то е минимум 1 година за семестриален изпит и 5 години за държавен изпит. Това налага ИТ отдела на ВУ–да задели голямо дисково пространство само за съхраняване на материалите от онлайн изпитите.

Всички изброени техники и процедури са препоръчителни. Използването само на една или няколко не може да доведе до 100 % сигурност, че студентите няма да компрометират изпита. Използването на всички, включени в единен комплекс, може да позволи преподавателят да осъществява максимален контрол върху студентите по време на онлайн изпита и да намали възможността за изтичане на служебна и лична информация към обучаемите.

Заключение

В настоящият момент информационните технологии се развиват с часове. Сега предложена техника или методология може да не бъде ефективна следващият месец. Хилядолетната човешка история е показала, че както за всеки вид оръжие е създадена защита, така и за всяка защита е намерено противодействие. В момента все повече навлизат технологиите за изкуствен интелект и в частност ChatGPT. Докато някои преподаватели дори и не са и чували за него, той вече активно се използва от студентите при изготвяне на реферати, есета и решаване на тестове. За да се намали възможността за компрометиране на изпита, било то в присъствена или онлайн форма, преподавателят също трябва да променя начина си на обучение и оценяване. Изпитните формати и изпитни задания трябва да бъдат обновявани периодично – като съдържание, методика и техническо изпълнение.

Направените наблюдения и предложените препоръки са извършени от автора на статия докато е асистент в катедра „Информационни технологии“ и модератор на системата за електронно-базирано обучение във ВВМУ „Н.Й.Вапцаров“.

ЛИТЕРАТУРА

1. Dechev , Y., Nikolov, B., Rachev, M., 2020. Distance Learning at Nikola Vaptsarov Naval Academy Utilizing Online Platforms during the COVID-19 Crisis. *Information & Security: An International Journal. 46(3)*, 293-303. ISSN 0861-5160

2. ENISA (2016): Cyber Hygiene. [cites 05.05.2023] Available from: <https://www.enisa.europa.eu/publications/cyber-hygiene/@@download/fullReport>

3. Fred Bedrich(2022): A cyber hygiene checklist can help prevent attacks on your business. [cites 05.05.2023] Available from: <https://www.bdc.ca/en/articles-tools/blog/cyber-hygiene-checklist-can-help-prevent-attacks-on-your-business>

4. Kaspersky (2023): Top tips for cyber hygiene to keep yourself safe online. [cites 05.05.2023] Available from: <https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygienehabits>