ЗАПЛАХИ ЗА СИГУРНОСТТА И ОСИГУРЯВАНЕ НА ЗАЩИТА В СИСТЕМИТЕ ЗА ЕЛЕКТРОННО ОБУЧЕНИЕ

Ангел Урилски[1*], Анна Малинова[2], Асен Рахнев[3]

[1, 2, 3] Факултет по математика и информатика, Пловдивски университет „Паисий Хилендарски“, гр. Пловдив, ул. „Цар Асен“ № 24
Имейли: yri@uni-plovdiv.bg, malinova@uni-plovdiv.bg, assen@uni-plovdiv.bg
** Автор за кореспонденция: yri@uni-plovdiv.bg*

Резюме. В тази статия сме представили някои от най-популярните и най-често използвани системи за електронно обучение, като сме разгледали рисковете за сигурността и сме предоставили съвети за подобряване на защитата.

Ключови думи: *защита на информационни системи, информационна сигурност, електронно обучение, e-learning.*

Въведение

Системите за електронно обучение представляват софтуерни платформи за планиране, предоставяне и управление на всички учебни събития в рамките на една организация, включително онлайн обучения, виртуална класна стая и курсове ръководени от лектори. Те могат не само да предоставят съдържание за обучение, а и да управляват учебните дейности на обучаемите, като следят техния напредък и постижения във всички видове обучителни дейности. Обикновено предоставят възможност за създаване на авторски ресурси или импортиране/експортиране на готови такива. Често биват класифицирани като системи за управление на обучението (Learning Management Systems – LMS), виртуални среди за обучение (Virtual Learning Environments – VLE) или системи за управление на учебното съдържание (Learning Content Management System – LCMS). Всички тези системи се използват в процеса на онлайн обучението, но имат някои разлики помежду си. LMS са най-добри за проследяване на напредъка на учениците по учебните цели, докато VLE предлагат на учениците по-задълбочено взаимодействие и ангажираност на учениците. LCMS пък се използват предимно за създаване, съхраняване и организиране на

съдържание за обучение, като в общия случай създаването на съдържание не изисква познаването на специализирани езици. В последните години системите за електронно обучение се развиват с много бързи темпове, авторите им се стремят да предоставят все повече и по всеобхватни функционалности, поради тази причина границите между различните видове започват се размиват.

В следващите секции е направен преглед на най-използваните системи за електронно обучение, като се прави връзка и със стандарти за сигурност и процедури за одит на сигурността, там, където такава информация е предоставена. По-нататък се акцентира на основните заплахи и проблеми за сигурността в платформите за електронно обучение. В последната секция се разглеждат действия, инструменти и техники за подобряване на сигурността, приложими в практиката.

Кратък обзор на системи за електронно обучение

Едни от най популярните системи за електронно обучение и управление на учебното съдържание са:

- Absorb LMS [1] – Изключително богата на функции облачно базирана система за електронно обучение с един от най добрите потребителски интерфейси в класа си. Разполага както с множество готови курсове за самообучение, така и с възможности за интерактивно обучение. Една от интересните функции на системата е платформата ѝ за продажба на авторско съдържание. Системата е насочена по-скоро към корпоративното обучение. Absorb регулярно преминава процедура за одит на сигурността AICPA SOC 2 от тип 2 [46].
- Adobe Captivate Prime LMS [2] – Тази система е интересна със социалното си обучение, базирано на изкуствен интелект. Потребителите да могат да взаимодействат помежду си в среда, подобна на социална медия, като могат да споделят съдържание и пишат коментари, а изкуственият интелект може да насочва съдържанието спрямо индивидуалните интереси. Adobe Captive Prime се хоства в облака на Амазон (Amazon Web Services), следва политиките за сигурност и използва инструментите за сигурност на облака.
- ATutor [3] – Уеб базирана система за управление на учебно съдържание с отворен код. Тя е уникална с това, че е проектирана с множество функции за достъпност и осигурява възможност за пълноценно обучение на учащи със зрителни увреждания и инвалиди.

- Blackboard Learn [4] – Голяма екосистема от образователни инструменти и услуги, която се използва от много академични институции и издатели. Потребителите на Blackboard могат да избират между четири модула, които са персонализирани в зависимост от нуждите от обучение: обучение за училища, за колежи и университети, за държавни институции и бизнес организации. Системата позволява лесна интеграция с редица приложения и бизнес системи. В момента системата може да се използва на собствени сървъри или в облачна SaaS среда, но се планира миграция изцяло към SaaS среда.
- Chamilo [5] – Среда с отворен код за електронно обучение и система за управление на съдържанието, насочена към подобряване на достъпа до образование и знания в световен мащаб. Тази платформа се фокусира върху лекотата на използване, предлагайки ергономичен интерфейс и множество функции благодарение на които правят обучението лесно и ефективно.
- Canvas LMS [6] – Система с отворен код която е насочена специално към нуждите на висшите училища и университетите. Освен стандартните инструменти за онлайн обучение, системата предлага и инструменти за изграждане и управление на обучително съдържание. Използвайки мащабируема облачна SaaS технология, Canvas LMS позволява лесна интеграция на съдържанието, инструментите и услугите. Системата ежегодно преминава процедура за одит на сигурността AICPA SOC 2 от тип 2 [46].
- D2L Brightspace LMS [7] – Отличава се от другите LMS платформи в пълното си прилагане на обучение, основано на компетентности (CBE). За разлика от традиционните онлайн курсове, CBE курсовете позволяват на участниците да демонстрират предишни компетенции под формата на умения или автобиографии. Тези компетенции биват проверявани (най-често проверката се извършва с тестове) и системата позволява учащите да пропуснат частите от курса за които те са показали знания и умения и насочва усилията им към тази част на обучението в което те са показали по-малко знания. Brightspace регулярно преминава процедура за одит на сигурността AICPA SOC 2 от тип 2 [46].
- Docebo [8] – SaaS платформа за електронно обучение използваща услугите на Амазон AWS. Фокусирана е върху професионалното развитие и корпоративното обучение. Амазон AWS използва Docebo като платформа за обучение и сертифициране за своите продукти. Платформата следва политиките за сигурност на AWS и използва инструментите за сигурност на облака.

- Edmodo LMS [9] – Една част образователна LMS и две части академична мрежа от социални медии, Edmodo дава на учителите, учениците и родителите всичко необходимо, за да трансформират традиционните класове в смесени учебни инициативи. Тя има подобен на Facebook интерфейс, като разполага с различни изгледи за учениците, учителите и родителите. Като цяло системата е ориентирана към началните и средните училища.
- Google classroom [10] – Безплатна услуга за онлайн обучение предназначена за учебни заведения и организации с нестопанска цел. Google classroom обединява някои от най-популярните приложения и услуги на Google, като Google Documents, Google Forms, Google Meet, Google Drive и YouTube в опростена среда за обучение. Притежава интуитивен интерфейс, който е лесен и удобен дори за най-малките ученици и е изградена върху една от най-сигурните облачни инфраструктури.
- ILIAS.de [11] – Безплатен софтуер с отворен код, който е мощен и гъвкав инструмент за електронно обучение и сътрудничество. Освен това, той не е тясно свързан с някой конкретен дидактически модел за обучение, повишавайки приспособимостта си към различни приложения и методи. ILIAS поддържа високо ниво на сигурност и има издаден сертификат за сигурност от НАТО. Софтуерът е използван в защитената интранет мрежа на НАТО за споделяне на чувствително учебно съдържание и документи.
- iSpring Learn [12] – Пълнофункционален LMS насочен към автоматизиране на корпоративното обучение и подобряване на представянето на служителите. Потребителите могат да получат достъп до учебни материали от своите смартфони и имат възможност да запазват съдържание директно на своите устройства за гледане офлайн. iSpring Learn е сертифицирана по стандартите за сигурност ISO 27001 и ISO 27701.
- Moodle [13] – Безплатна система с отворен код за електронно обучение. Тя е модулна система, базирана на плъгини, посредством които потребителите могат да изградят персонализирана система за обучение. Опростеният интерфейс, постоянните подобрения, множеството плъгини и огромната общност от потребители правят Moodle атрактивна за използване.
- Schoology [14] – Предоставя лесна за използване и гъвкава образователна платформа насочена основно към началното и средно училище. Средата разполага с множество възможности включително инструмент за създаване и управление на обучителни курсове. Има безплатна версия, в която липсват някои от

функциите, но има всички основни инструменти и функционалности които се използват в процеса на обучение. Schoology се хоства в Амазон (Amazon Web Services), следва политиките за сигурност и използва инструментите за сигурност на облака.

- Sakai Environment [15] – Предоставя гъвкава и богата на функции среда за преподаване, учене, изследвания и друго сътрудничество. Като софтуерен пакет с отворен код, поддържан от голяма общност, Sakai непрекъснато се развива в съответствие с нуждите на студентите, преподавателите и организациите, които обслужва.
- SAP Litmos [16] – Облачна платформа за електронно обучение с богата функционалност, насочена към нуждите за професионално обучение на корпоративните потребители.
- TalentLMS [17] – Платформа, създадена с цел предоставяне на увлекателно онлайн обучение. Тази платформа предлага богата функционалност за създаване на курсове, оценяване на потребители, администриране на процеса на обучение и т.н. Също така е оборудвана с функции за игровизация, посредством които може да направи обучението още по-ангажиращо. TalentLMS се хоства в облака на Амазон (Amazon Web Services), следва политиките за сигурност и използва инструментите за сигурност на облака.
- Tovuti [18] – Универсално, базирано на облак решение, което предоставя на потребителите си всичко необходимо за изграждането на ефективни програми за електронно обучение – от виртуална класна стая и инструменти за създаване на интерактивно съдържание до създаване на събития, включително такива с възможност за заплащане на такса за участие.

Общото между всички по-горе изброени системи е, че всички са уеб базирани и като такива са изложени на потребители, част от които могат да се опитат да нарушат сигурността им. Друга обща характеристика е голямата част от тези системи периодично биват сертифицирани според различни регулации и стандарти за сигурност, като: GDPR [47], ISO 27001 [44] и ISO 27701 [45] и др., или регулярно правят одит на сигурността AICPA SOC 2 от тип 2 [46].

Рискове, свързани със сигурността

Заплахите за сигурността приемат най-различна форма. Рисковете за сигурността на уеб приложенията могат да бъдат обобщени в няколко основни групи [21, 27, 28, 29, 32]:

Рискове от инжектиране на код или команди: Инжектиране на код или команди може да бъде направено, като не валидирани данни се изпращат до интерпретатор като част от команда или заявка. По този начин могат да бъдат изпълнени злонамерени команди или да бъде получен достъп до чувствителни данни. Тези недостатъци са много разпространени, особено в приложения които имат наследствен код. Уязвимости при инжектиране най често се срещат в LDAP, SQL или NoSQL заявки, XML парсери и команди на операционната система.

Отказ от наличност: Едни от най честите заплахи за наличност са DoS и DDoS атаките. Този вид атаки се използват, за да се наруши нормалната операция на дадена система, чрез генериране на огромно количество заявки, което води до претоварване на мрежовите устройства или сървъри, те не могат да обработват подадените им заявки, в следствие на което ги отказват и системата става недостъпна. Според Kaspersky [24] DDoS атаките, насочени към обучителни ресурси през пролетта на 2020 година, са нараснали с над 350% спрямо предходната година. В [35] се изследват DDoS атаките към облачните инфраструктури, като се акцентира на техния ефект върху цялата среда. Представен е подход за идентифициране на DDoS атаки в облака, базиран на различни алгоритми за машинно обучение.

Излагане на чувствителни данни: Излагането на чувствителни данни най често се получава в резултат на неадекватна защита (или липсата на такава) при съхранение и транспортиране на данните. Това включва използване на слабо криптиране или липсата на такова, съхраняване на данни в обикновен текст, липса на хеширане и допълнителни алгоритми при криптиране и пренасяне на данни за идентификация.

Крос-сайт скриптинг (XSS): Този тип уязвимост представлява възможност да бъде инжектиран зловреден код директно в приложението, без той да бъде валидиран. По този начин, когато „жертвата“ отвори съответната страница, този код бива изпълнен върху неговото устройство и дава възможност на атакуващия да се сдобие с чувствителни данни, да бъдат откраднати пароли, сесии, да бъде инсталиран зловреден код или да пренасочат потребителя към злонамерени сайтове.

XML Външни обекти (XXE): XXE атаките експлоатират уязвимости в процесорите за обработка на XML. Използването на остарели версии или лошо конфигурирани XML процесори позволяват използване на препратки към външни обекти. Външните обекти са особено интересни от гледна точка на сигурността, тъй като позволяват обект да бъде дефиниран въз основа на съдържанието на файлов път или URL адрес. Тази уязвимост може да се счита за форма на инжекционна атака и може да се използва за разкриване

на вътрешни файлове, вътрешно сканиране на портове, отдалечено изпълнение на код и атаки за отказ на услуга.

Нарушено удостоверяване: Тази уязвимост обикновено се причинява от лошо внедрени функции за удостоверяване и управление на сесии. Това позволява на нападателите да компрометират сесии, пароли или да използват други недостатъци на внедряването, за да приемат самоличността на други потребители.

Неправилен контрол на достъпа: Неправилният контрол на достъпа често е критична уязвимост която води до тежки последствия. Тя възниква тогава, когато на потребители или процеси е даден достъп до ресурси, до които те нямат изрична необходимост. Злоумишлениците могат да използват тези недостатъци за неоторизиран достъп, промяна или изтриване на информация, промяна на права и т.н.

Неправилно конфигуриране на защитата: Пропуските в конфигурирането на защитите е най-често срещаният проблем. Често се използват конфигурации по подразбиране или конфигурациите се правят повърхностно, като по този начин могат да останат активни ненужни услуги и функционалности, неизползвани функции за обратна съвместимост и т.н. По този начин атакуващите могат да придобият достъп до акаунти по подразбиране, незащитени ресурси, да използват пропуски в сигурността на неизползвани приложения или функции както и допълнителна информация за системата. Трябва да се отбележи, че освен правилното конфигуриране на всяко едно ниво (операционни системи, приложения, рамки, библиотеки и т.н.), много е важна и грижата в последствие – своевременното инсталиране на обновления и кръпките за сигурността.

Несигурна десериализация: Несигурната десериализация е, когато контролирани от потребителя данни се десериализират от уеб приложение. Това потенциално позволява на нападател да манипулира сериализирани обекти, за да инжектира вредни данни в кода на приложението. Несигурната десериализация често води до отдалечено изпълнение на код, атаки за инжектиране и атаки за ескалация на привилегии.

Използване на компоненти с известни уязвимости: Приложения и API, използващи компоненти с известни уязвимости, могат да компрометират защитата на приложенията и да позволят различни атаки и въздействия. Поради тази причина е важно редовно да се инсталират обновления и пачове, които касаят сигурността.

Недостатъчно наблюдение и регистриране и анализиране на събития свързани със сигурността: Липсата на адекватен мониторинг и анализ на поведението на системите, съчетано с неефективно реагиране на инциденти, позволява на нападателите да постигнат целите си, без да бъдат открити. Повечето проучвания за нарушения показват, че нарушенията

обикновено са открити от външни страни, а не от вътрешни процеси или мониторинг системи.

До тук разгледахме рисковете за сигурността на системите за онлайн обучение от гледна точка на външни атаки към самата система. От гледна точка на учебното съдържание и учебния процес обаче съществуват други предизвикателства които трябва да преодолеем. Някои от тях са:

- **Защита на цифрово съдържание от нерегламентирано използване, промяна или разпространение** – често се случва лекции, презентации, видео уроци и други авторски обучителни материали да бъдат разпространявани и използвани без разрешението на авторите. В [37] се представя изследване за прилагането на изкуствен интелект и блокчейн технологии за предотвратяване на промяна на данни, подмяна на изпитни резултати и др. В [39] и [42] също се разглежда приложението на блокчейн архитектура, в комбинация с криптиране, за осигуряване на контрол на достъпа и интегритет на данните.
- **Защита от преписване** – не е тайна че много от учащите се опитват да постигнат по добри резултати на изпитите използвайки нечестни методи и средства. Много е трудно да се избегне напълно нечестното поведение, но е добре да бъде максимално ограничено [42].
- **Удостоверяване на идентичността на обучаемия**, ако/когато това е необходимо – важно е да може бъде установена идентичността на обучаемите особено по време на изпити, при предаване на домашни и курсови работи и други [41, 42]. Модели на „цифрова идентичност“, „цифров отпечатък“ на обучаеми и преподаватели се дискутират и в [38, 43].
- **Защита на личните на данни на обучаемите** – системите за електронно обучение трябва да осигурят защита на личните данни, прогреса, оценките на обучаемите, в синхрон със законодателството в тази област [47]. Това стана още по-актуален проблем предвид повсеместното преминаване към електронно обучение в следствие на Covid19 пандемията [36].

Как да повишим сигурността в системите за електронно обучение?

В отговор на нарастващите заплахи, в системите за електронно обучение трябва да бъдат въведени редица мерки за подобряване на сигурността [28, 30, 33].

Най напред трябва да започнем от сървъра, на който се намира системата. Сървърът трябва да е конфигуриран правилно, без да се използват конфигурации по подразбиране. Трябва да са деинсталирани всички ненужни модули и програми. Достъпите, дадени на хора или на различните части на приложението, трябва да бъдат прегледани и анализирани и да бъдат ограничени само до необходимото. Освен това от съществено значение е редовно да се проверява за актуализации и кръпки на уязвимости на операционната система, на софтуера, на приложението и всички допълнителни модули и рамки които използва то.

Използване на защитна стена за приложения (web application firewall). Защитните стени за уеб приложения (WAF) са различни от мрежовите защитни стени и са критичен компонент за сигурността на приложенията. Основната им задача е да защитават приложенията от уеб базирани атаки в приложния слой. Обикновено WAF защитава уеб приложенията от атаки като крос-сайт скриптинг (XSS), SQL инжектиране, DDoS атаки и дори от пропуски при конфигурацията на сървъра [26].

Използване на системи за откриване и/или предотвратяване на проникване (Intrusion detection system – IDS and Intrusion prevention system – IPS). Защитните стени за уеб приложения са изключително полезен инструмент, но сами по себе си не са достатъчни за пълна защита, а по-скоро са предназначени да се използват заедно с други решения за сигурност като мрежови защитни стени и системи за откриване и предотвратяване на проникване, за да осигурят цялостна защита. IDS системите анализират и наблюдават мрежовия трафик за признаци, указващи опити за проникване и изпращат предупреждения, когато такава активност бъде открита. Те сравняват текущата мрежова активност с база данни с известни заплахи, за да открият поведения като нарушения на политиките за сигурност. Системите за предотвратяване на проникване се разглеждат като разширяване на системите за откриване на проникване, понеже те също извършват наблюдения над мрежовия трафик и изпращат предупреждения, но освен това могат и да предприемат действия за прекратяване на атаката като филтриране на злонамерени пакети или блокиране на трафика идващ от атакуващия IP адрес [33].

Използване на криптиране – за да се избегне излагането на поверителни данни е задължително да се използва криптиране навсякъде където е възможно. В днешно време криптирането играе ключова роля при проектирането и внедряването на почти всички видове информационни системи. Сигурността на една система за електронно обучение определено ще бъде по висока, ако базата данни, в която се съдържат личните данни и оценките на студентите, е криптирана, материалите използвани в обучителните курсове стоят в криптирани хранилища, връзката между потребителите и системата е криптирана (https) и т.н.

Защита при удостоверяване – в системите за електронно обучение едно от най слабите звена са потребителите. Към групата на потребителите можем да причислим не само студентите, а и преподавателите, хората които се грижат за администрирането на самата система, тези които се грижат се за съдържанието, които въвеждат оценки и изобщо всички, които имат достъп до системата. Общото между всички потребители е, че те използват пароли за достъп до системата. Повечето потребители обаче са склонни да създават лесни пароли, рядко ги променят, използват еднакви пароли за различни акаунти, споделят паролите си с други потребители и т.н. Поради тази причина в системата трябва да бъде предвидена функция, която да следи за сложността на паролите. Изборът на сложна комбинация от символи за парола трябва да е задължително условие при регистрацията на всеки потребител независимо от нивото му на достъп. Друго популярно решение за увеличаване на сигурността на акаунтите, което става все по-разпространено напоследък са системите за двуфакторна автентикация (2FA). 2FA добавя още едно ниво на защита. При нея е необходимо, освен въвеждане на парола, да се въведе и допълнителен код за сигурност. Този код се генерира на момента и може да бъде използван само веднъж, така рискът някой друг да злоупотреби с паролата за достъп намалява значително. Допълнително ниво на сигурност може да се добави, ако вместо код за 2FA се използват биометрични показатели (лицево разпознаване, сканиране на ириса или използване на пръстов отпечатък). Същевременно добавянето на биометрични показатели може да помогне при решаването на още един проблем свързан със системите за електронно обучение – удостоверяване на самоличността на обучаемия [43].

Редица изследвания в областта заплахи към сигурността в системите за електронно обучение акцентират и на хардуерните аспекти на осигуряването на защита от атаки. Например, в [34, 40] разглеждат редица проблеми при използването на безжични технологии и средства за достъп до системите за електронно обучение. Предложени са инструменти и протоколи за повишаване на сигурността.

Използване на цифров воден знак и на DRM защити за защита на авторските материали – цифровите водни знаци позволяват да бъдат добавени явни или скрити идентификационни данни в изображения, аудио или видео файлове. Те са инструмент за пасивна защита и посредством тях не може да се ограничи достъпа до данните. Обикновено се използват за идентифициране на собствеността върху авторските права. За тази цел цифровият воден знак трябва да бъде устойчив по отношение на промени на носещия го файл [31].

Digital rights management (DRM) е обобщено понятие на технологиите за контрол на достъпа, копирането и промяната на ресурси, които са компютърно базирани. Те могат да бъдат приложими при системите за

електронно обучение. Съществуват различни възможности за защита на материалите, като например:

- след определена дата материалите да не могат да бъдат отваряни;
- има определен брой отваряния;
- да не може да се променя съдържанието;
- да не може да се печата – всички бутони за печат са неактивни;
- не може да се копира съдържанието с copy-paste и т.н. [25].

На практика всички защити от този тип могат да бъдат надхитрявани и разбивани. Пълната защита материали е много трудна, дори невъзможна. Въпросът е да се направи така, че усилията за разбиването на защитата да са неоправдани.

Защита от преписване – както казахме по-горе, този тип защита е трудно да се направи със сто процентова ефективност, но рискът от нечестно поведение може да бъде намален до приемливи нива. За целта могат да се използват специализирани софтуери за контрол на изпитваните. Те работят сравнително добре, като някои от тях могат да се интегрират в повечето LMS системи, а други могат да работят независимо от това коя LMS система се използва. Някои от тях са:

- Специализирани браузъри.
  - Safe Exam Browser [22] – Този браузър превръща всеки компютър в защитена работна станция: браузърът записва всичко, което студентът прави, но също така ограничава действията му. Студентите не могат да отварят други раздели, за да търсят или проверяват отговорите си, изключват се някои функции като съобщения, клавишни комбинации и др. Някои LMS системи като например Moodle, ILIAS, OpenOLAT предлагат специален изпитен режим който е съвместим със Safe Exam Browser и осигурява допълнителни възможности.
  - LockDown Browser [23] – този браузър е подобен на Safe Exam Browser. Към него обаче може да се включи и допълнителен модул - Respondus Monitor който изисква включване на видеокамера и микрофон, които записват по време на целия изпит. След това проверяващите, ако пожелаят, могат да прегледат/преслушат записа. LockDown Browser се интегрира безпроблемно с Blackboard, Brightspace, Canvas, Moodle, Sakai и Schoology.
- Специализирани системи за проследяване и анализиране на поведението на студентите по време на изпит – съществуват

множество такива системи, които посредством видеокамера (в някои случаи дори две видеокамери и микрофон) в реално време проследяват, анализират и записват студентите, като отбелязват моментите на подозрително поведение. Някои системи имат възможност за следене и анализиране и на компютърния екран, удостоверяване на идентичността на изпитвания и други полезни функции.

- Инструменти за проверка за плагиатство – решения като Turnitin [19] и Unickeck [20] помагат както на изпитващите, така и на изпитваните да проверяват задачите/проектите за следи от плагиатство. Те могат да сравнят тестовете на студентите, за да намерят прилики с други документи или с други ресурси в интернет.

Заключение

Системите за електронно обучение могат да бъдат подложени на всички атаки към сигурността, характерни за всяка една информационна система. В допълнение обаче, е критична и необходимостта от осигуряване на софтуерни инструменти за защита на учебните материали и учебните дейности от неоторизиран достъп, защита от преписване, защита срещу плагиатство и др. Идентифицирането на самоличност се откроi и като един от съществените проблеми, които излязоха на преден план в обстановката на пандемия и глобалното прилагане на електронно и дистанционно обучение във всички степени образование.

Предизвикателствата пред идентифицирането на нови заплахи към сигурността на системите за електронно обучение, както и тяхното отстраняване, ще продължат да са един от ключовите компоненти в ежедневното осъществяване на обучение в електронна среда.

В настоящата статия се направи обзор на едни от най-разпространените заплахи за сигурността на системите за електронно обучение и бяха дискутирани разнообразни варианти за защита, които могат да се прилагат на практика.

Благодарности

Работата е частично финансирана по научен проект ФП21-ФМИ-002 към НПД на Пловдивски университет „П. Хилендарски“ и Национална научна програма „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТвНОС)“, финансирана от МОН.

Литература

[1] Absorb LMS, https://www.absorblms.com/

[2] Adobe Captivate Prime LMS, https://www.adobe.com/bg/products/captivateprime.html

[3] ATutor, https://atutor.github.io/

[4] Blackboard Learn, https://www.blackboard.com/teaching-learning/learning-management/blackboard-learn

[5] Chamilo LMS, https://chamilo.org/en/

[6] Canvas LMS, https://www.instructure.com/en-gb

[7] D2L Brightspace LMS, https://www.d2l.com/

[8] Docebo, https://www.docebo.com/

[9] Edmodo LMS, https://new.edmodo.com/

[10] Google classroom, https://edu.google.com/products/classroom/

[11] ILIAS, https://www.ilias.de/en/

[12] iSpring Learn, https://www.ispringsolutions.com/

[13] Moodle, https://moodle.org/

[14] Schoology, https://www.schoology.com/

[15] Sakai LMS, https://www.sakailms.org/

[16] SAP Litmos, https://www.litmos.com/

[17] TalentLMS, https://www.talentlms.com/

[18] Tovuti LMS, https://www.tovutilms.com/

[19] Turnitin, https://www.turnitin.com/

[20] Unickeck, https://unicheck.com/

[21] OWASP Top Ten , https://owasp.org/www-project-top-ten/

[22] Safe Exam Browser, https://safeexambrowser.org/news_en.html

[23] LockDown Browser, https://web.respondus.com/he/lockdownbrowser/

[24] Kaspersky Lab, https://www.kaspersky.com/about/press-releases/2020_ddos-attacks-against-educational-resources-increased-by-more-than-350-this-spring

[25] G. Agnew, *Digital Rights Management: A Librarian's Guide to Technology and Practise*, Chandos Publishing, Oxford, 2008, ISBN: 978 1 84334 125 3.

[26] Ch. Russell, *Web Application Firewall Securing Modern Web Applications*, O'Reilly Media, Sebastopol, 2018, ISBN: 978-1-492-03228-1.

[27] D. Kim, M. Solomon, *Fundamentals of Information Systems Security*, 4th Edition, Jones & Bartlett Learning, Burlington, 2021, ISBN-13: 978-1284220735.

[28] M. Whitman, H. Mattord, *Management of Information Security*, 6th Edition, Cengage, Boston, 2019, ISBN-13: 978-1337405713.

[29] R. Smith, *Elementary Information Security*, 3rd Edition, Jones & Bartlett Learning, Burlington, 2019, SBN-13: 978-1284153040.

[30] M. Whitman, H. Mattord, *Principles of Incident Response & Disaster Recovery*, 3rd Edition, Cengage, Boston, 2021, ISBN-13: 978-0357508329.

[31] F. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, CRC Press, Boca Raton, 2017, ISBN: 978-1-4987-3876-7.

[32] A. Hoffman, *Web Application Security Exploitation and Countermeasures for Modern Web Applications*, O'Reilly Media, Sebastopol, 2020, ISBN: 978-1-492-08796-0.

[33] R. Das, G. Johnson, *Testing and Securing Web Applications*, CRC Press, Boca Raton, 2020, ISBN: 978-0-367-33375-1.

[34] M. Tigner, H. Wimmer, Disruption and protection of online synchronous learning environments via 802.11 manipulation, *IEEE International IOT, Electronics and Mechatronics Conference*, 2021, DOI: 10.1109/ IEMTRONICS52119.2021.9422484.

[35] A. Nagaraja, U. Boregowda, V. Radhakrishna, Study of detection of DDoS attacks in cloud environment using regression analysis, *ACM International Conference Proceeding Series*, 2021, 166–172, DOI: 10.1145/3460620. 3460750.

[36] P. Sethi, P. Behera, Effective online teaching learning during COVID-19 pandemic, *Journal of Physics: Conference Series*, 2021, DOI: 10.1088/ 1742-6596/1797/1/012068.

[37] N. Hung, T. Phung, P. Hien, D. Thanh, AI and Blockchain: Potential and challenge for building a smart E-Learning system in Vietnam, *IOP Conference Series: Materials Science and Engineering*, 2021, DOI: 10.1088/ 1757-899X/1022/1/012001.

[38] A. Solovov, A. Menshikova, Models for the design and operation of digital educational environments, *Vysshee Obrazovanie v Rossii*, 2021, 144–155, DOI: 10.31992/0869-3617-2021-30-1-144-155.

[39] D. Hamdi, O. Alfandi, Pros and cons of blockchain-based approaches in education, *2021 IEEE Global Engineering Education Conference*, EDUCON, 2021-April, art. no. 9454118, 1558–1564. DOI: 10.1109/ EDUCON46332.2021.9454118.

[40] V. Shapo, M. Levinskyi, Means of Cyber Security Aspects Studying in Maritime Specialists Education, *Advances in Intelligent Systems and Computing*, 2021, 389–400, DOI: 10.1007/978-3-030-49932-7_38

[41] M. Bundin, A. Martynov, A. Minbaleev, Legal Aspects of the Use of Biometric Students' Identification for Distant and Online Learning: Russian

Perspective, *ACM International Conference Proceeding Series*, 2021, 564–566, DOI: 10.1145/3463677.3463758.

[42] C. Cao, X. Zhu, Trusted Data Management for E-learning System Based on Blockchain, *2021 IEEE 13th International Conference on Computer Research and Development* (ICCRD 2021), 2021, 91–94, DOI 10.1109/ICCRD51685.2021.9386354.

[43] D. Korac, B. Damjanovic, D. Simic, A model of digital identity for better information security in e-learning systems, *Journal of Supercomputing*, 2021, ISSN: 0920-8542, DOI 10.1007/s11227-021-03981-4.

[44] ISO 27001, https://www.iso.org/isoiec-27001-information-security.html

[45] ISO 27701, https://www.iso.org/standard/71670.html

[46] AICPA Service Organization Control (SOC), https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

[47] GDPR, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1630230631070

SECURITY THREATS AND PROTECTION IN E-LEARNING SYSTEMS

Angel Urilski[1*], Anna Malinova[2], Asen Rahnev[3]

[1, 2, 3] Faculty of Mathematics and Informatics,
University of Plovdiv "Paisii Hilendarski", 24 Tzar Asen Str., Plovdiv, Bulgaria
Emails: yri@uni-plovdiv.bg, malinova@uni-plovdiv.bg, assen@uni-plovdiv.bg
[*] Corresponding author: yri@uni-plovdiv.bg

Abstract. In this article, we have presented some of the most popular and most commonly used e-learning systems, as well as we have considered the security risks and provided tips for improving their protection.