



КИБЕРСИГУРНОСТ В ЕЛЕКТРОННОТО ОБУЧЕНИЕ: ВАЖНОСТ И ПРЕДИЗВИКАТЕЛСТВА

Фатме Юсеинова Рашидова

Технически университет - Габрово

CYBERSECURITY IN E-LEARNING: IMPORTANCE AND CHALLENGES

Fatme Yuseinova Rashidova

Technical University of Gabrovo

Abstract: *With the increasing use of e-learning, cybersecurity is becoming a key factor in ensuring a safe and effective educational environment. Online platforms and virtual classrooms pose risks from cyber threats such as phishing attacks, malware and personal data leaks. Despite technological advances, many students and teachers do not have sufficient knowledge to protect their digital resources. This report analyzes the importance of cybersecurity in e-learning and highlights the need for digital literacy among educational stakeholders.*

Keywords: *eLearning, Cyber Security, Risks, Educators, Students*

Въведение

Развитието на електронното обучение (ЕО) доведе до значителни промени в образователния процес, като осигури по-голяма достъпност и гъвкавост за обучаващите се. Възможността за дистанционно обучение елиминира географските бариери, позволявайки на ученици и студенти от цял свят да участват в курсове, без да напускат дома си. Онлайн платформите предлагат разнообразни методи за обучение – интерактивни уроци, видеолекции, тестове и дискуссионни форуми, които подпомагат придобиването на знания по един модерен и удобен начин.

Въпреки многобройните предимства на ЕО, цифровизацията на образованието носи със себе си и редица предизвикателства, свързани с киберсигурността [1-4]. Студентите и преподавателите често подценяват рисковете, произтичащи от кибератаки, кражба на лични данни, фишинг атаки и неразрешен достъп до акаунти. Липсата на достатъчна информираност и неефективни мерки за защита могат да доведат до сериозни проблеми, включително компрометиране на учебни материали, загуба на лична информация и дори финансова злоупотреба.

Настоящата работа има за цел да представи основните заплахи за киберсигурността в ЕО, да предложи ефективни стратегии за защита на личните данни и да анализира добрите практики за осигуряване на сигурна дигитална учебна среда. За да се гарантира



безопасността на всички участници в образователния процес, е необходимо институциите, преподавателите и студентите да възприемат проактивен подход към киберсигурността, като прилагат съвременни методи за защита и следват утвърдени политики за информационна сигурност.

Изложение

С развитието на технологиите и навлизането на цифровите платформи в образованието, ЕО се утвърди като основен метод за предаване на знания. Онлайн класовете, виртуалните учебни пространства и облачните платформи предлагат удобство и гъвкавост, но също така крият сериозни рискове, свързани с киберсигурността. За студентите и преподавателите в електронно обучаващата се среда, разбиране на тези рискове и предприемане на действия за защита на личните и професионални данни става все по-необходимо [5-7].

I. Основни рискове за киберсигурността в ЕО

ЕО разчита на онлайн платформи, които предоставят достъп до учебни материали, комуникация между участниците и провеждане на изпити. Въпреки удобствата, те създават потенциални уязвимости, сред които:

- ✓ Фишинг атаки: Киберпрестъпниците могат да изпращат фалшиви имейли, които изглеждат като официални съобщения от образователните институции. Целта е да се откраднат лични данни, пароли и информация за кредитни карти;
- ✓ Зловреден софтуер: Изтеглянето на нелегални материали или посещаване на компрометирани уебсайтове може да доведе до заразяване на компютрите с вируси и други зловредни програми;
- ✓ Изтичане на лични данни: В случай на несигурност на платформата или небрежност при обработка на лични данни, студентите и преподавателите могат да станат жертви на кражба на идентичност или несанкциониран достъп до техните акаунти и записи;
- ✓ Неадекватни пароли и лоши практики за сигурност – слаби пароли и споделяне на акаунти увеличават риска от злоупотреба;
- ✓ DDoS атаки – Дистрибутираните атаки за отказ от услуга (DDoS) могат да блокират достъпа до образователни платформи, което може да наруши учебния процес и да доведе до загуба на ценна информация.
- ✓ Надеждност на облачните услуги – Облачните платформи, използвани за съхранение на учебни материали и данни, също са обект на хакерски атаки. Пробив в сигурността на тези услуги може да доведе до загуба или манипулация на важни учебни ресурси.
- ✓ Заплахи при видеоконферентни връзки (Zoombombing) – Виртуалните класни стаи са уязвими към неоторизирани потребители, които могат да прекъснат лекции, да споделят неподходящо съдържание или да извършват други вредни действия.



- ✓ Неоторизиран достъп и измами при онлайн изпити – Студентите могат да бъдат подложени на измами или опити за манипулация по време на онлайн тестове, а

недостатъчната защита на изпитните платформи може да компрометира целостта на оценяването.

II. Обучение за киберсигурност в образователните институции

С оглед на нарастващите киберзаплахи в ЕО, образователните институции трябва да предприемат целенасочени действия за осигуряване на безопасността на своите потребители. Един от основните начини за намаляване на рисковете е чрез осигуряване на редовни и ефективни обучения по киберсигурност. Това обучение трябва да обхваща няколко ключови области:

- ✓ Запознаване със заплахите – обучението на студентите и преподавателите за основните видове киберзаплахи, като фишинг атаки и зловреден софтуер е основно условие за предотвратяване на киберпрестъпления. Студентите трябва да бъдат обучени да разпознават подозрителни имейли, фалшиви линкове и фалшиви уебсайтове. Това включва както теоретично знание, така и практически примери за разпознаване на такива заплахи. Например, учебни материали и симулации на фишинг атаки могат да помогнат на студентите да придобият умения за откриване на опасни съобщения и да знаят как да реагират при тяхното получаване;
- ✓ Управление на лични данни – важно е студентите и преподавателите да бъдат информирани за важността на личните данни и за начините, по които тези данни могат да бъдат защитени в онлайн среда. Част от обучението трябва да включва правилата и законите за защита на личните данни, като Общия регламент за защита на данните (GDPR) в Европа. Това обхваща осведоменост относно това каква информация се събира и защо, как се съхранява и обработва, както и как да се минимизира излагането на чувствителни данни;
- ✓ Използване на надеждни платформи – образователните институции трябва да насърчават студентите и преподавателите да използват сигурни и редовно актуализирани системи за обучение, които осигуряват високо ниво на защита. Също така, трябва да бъдат препоръчвани платформи и приложения, които предлагат криптиране на данни, защита на комуникацията и други основни сигурностни механизми. При избор на нови платформи или софтуери за обучение, университетите трябва да осигурят проверки за сигурността и да гарантират, че тези решения отговарят на най-високите стандарти за киберсигурност;
- ✓ Създаване на политики за киберсигурност – в допълнение към обучението на студенти, университетите трябва да разработят вътрешни политики и процедури, които да регулират безопасността на данните и да осигуряват подкрепа при инциденти. Това включва стратегии за управление на рисковете, планове за реакция при инциденти (например, когато се случи пробив в сигурността или изтичане на данни) и механизми за уведомяване на всички засегнати участници. Политиките трябва да включват и



регулярни тестове и симулации на инциденти, за да се провери ефективността на съществуващите системи за защита;

✓ Обучение на преподавателите - преподавателите също трябва да преминат през специализирано обучение, което да ги запознае със специфичните рискове, които

съществуват за тях в контекста на преподаването онлайн. Те трябва да разпознават заплахите, свързани с виртуални класни стаи, използване на студенски данни в оценяването и управлението на виртуални групи. Освен това е важно преподавателите да създават безопасни условия за онлайн дискусии и да използват проверени методи за предаване на материали и изпити.

III. Технологични решения за защита на данните

В допълнение към обучението, технологиите играят ключова роля в осигуряването на защита на данните и предотвратяването на киберзаплахи в електронното обучение. Използването на напреднали технологии може значително да повиши сигурността на учебните платформи и да създаде по-безопасна и надеждна среда за студентите и преподавателите. Ето някои от най-ефективните технологични мерки за защита на данни:

✓ Двухфакторна автентикация (2FA) – двухфакторната автентикация (2FA) предоставя допълнителен слой на защита, като изисква от потребителя не само парола, но и втори фактор, например код, изпратен на мобилен телефон или генериран от специално приложение. Това значително намалява риска от неоторизиран достъп до акаунти, дори ако паролата е компрометирана. За електронното обучение, 2FA може да се внедри за всички акаунти на преподаватели и студенти, като така се гарантира сигурността на личните и академичните данни;

✓ Криптиране на данните – криптирането на данни е основна мярка за защита, която осигурява безопасен обмен и съхранение на информация. За платформите за електронно обучение криптирането е задължително за защита на онлайн комуникацията, като например чатове и имейлите, и също така за осигуряване на безопасността на личната информация на студентите;

✓ Антивирусен софтуер и защитни стени – антивирусният софтуер и защитните стени играят основна роля в предотвратяването на проникването на зловреден софтуер. Тези технологии наблюдават и блокират опити за заразяване на системата с вируси, троянски коне, шпионски софтуер и други зловредни програми. За електронните платформи за обучение е от съществено значение те да използват последните версии на антивирусния софтуер и да имат активирани защитни стени, които да предотвратяват всякакви опити за кибератаки или несанкциониран достъп;

✓ Системи за мониторинг и откриване на заплахи – инструментите за мониторинг на трафика и откриването на заплахи са проектирани да анализират и наблюдават интернет трафика в реално време, като идентифицират подозрителни действия и аномалии. Тези системи могат бързо да открият и да реагират на атаки, като например неоторизиран достъп до системата, опити за изтичане на данни или DDoS (Distributed Denial of Service)



атаки. Важно е образователните институции да внедрят тези технологии, за да гарантират незабавна реакция при инциденти с киберсигурността и да предотвратяват сериозни щети;

✓ Редовни актуализации на софтуера – актуализациите на софтуера са жизненоважни за поддържане на сигурността на платформите за ЕО. Често новопубликуваните версии на софтуера съдържат важни поправки на сигурността, които затварят уязвимости и

предпазват от новопостъпващи заплахи. За да се намалят рисковете от атаки, е необходимо редовно да се актуализират както платформите за обучение, така и всички свързани със системата приложения и хардуер. Препоръчва се тези актуализации да бъдат автоматизирани, за да се осигури постоянна защита;

✓ Изолация и сегментиране на мрежата - в образователните институции е препоръчително да се прилага принципът на сегментиране на мрежата, при който чувствителните данни и ресурси се изолират в отделни мрежи с ограничен достъп. Това осигурява по-висока сигурност, като ограничават разпространението на евентуални атаки и рискове в цялата мрежа. Например, студентските данни могат да бъдат съхранявани на отделни сървъри с повишена защита, отделени от общите административни системи;

✓ Периодични тестове за сигурност и симулации на атаки (Penetration Testing) - за да се оцени ефективността на използваните защитни мерки, образователните институции трябва да провеждат редовни тестове за сигурност, включително симулации на кибератаки (penetration testing). Това включва сканиране на мрежата и системите за уязвимости и идентифициране на слабости, които могат да бъдат експлоатирани от хакери. Чрез тези тестове университетите могат да предприемат своевременни корекции, преди да се случи реална кибератака.

Прилагането на тези технологични решения, в комбинация с адекватно обучение на студентите и преподавателите, ще гарантира по-високо ниво на сигурност в ЕО. Това ще създаде по-защитена и надеждна учебна среда, която ще минимизира риска от киберзаплахи и ще гарантира безпроблемното протичане на образователния процес.

IV. Стратегии за защита на личните данни

На индивидуално ниво, както преподавателите, така и студентите трябва да прилагат практики за защита на личните си данни:

- ✓ Редовно обновяване на софтуера – поддържане на сигурността чрез актуализации;
- ✓ Използване на защитени Wi-Fi мрежи – избягване на обществени мрежи без криптиране;
- ✓ Етика на данните – информираност за отговорното използване на лична информация в образователния процес.



Заклучение

В дигиталната ера киберсигурността играе ключова роля в ЕО, като гарантира защитата на личните данни, учебните ресурси и комуникацията между преподаватели и студенти. С нарастващата зависимост от онлайн платформи и дигитални технологии, образователните институции са изправени пред редица предизвикателства, свързани с киберзаплахите. Фишинг атаки, зловреден софтуер, пробиви в сигурността и нерегламентиран достъп до данни са само част от рисковете, които могат да компрометират учебния процес и да застрашат академичната общност.

Осигуряването на сигурна учебна среда изисква координирани усилия между университетите, студентите и преподавателите. Чрез обучения, внедряване на съвременни технологични решения и прилагане на ефективни политики за защита, висшите учебни заведения могат да минимизират киберзаплахите и да повишат осведомеността на потребителите относно потенциалните рискове. Освен това, добрите практики за киберсигурност, като използване на сложни пароли, двуфакторна автентикация и криптиране на чувствителна информация, трябва да бъдат интегрирани в ежедневната работа на всички участници в образователния процес.

Прилагането на систематичен и проактивен подход към киберсигурността ще спомогне за изграждането на устойчиви и надеждни цифрови образователни среди. Само чрез непрекъснато усъвършенстване на защитните механизми и адаптиране към новите киберзаплахи можем да гарантираме безопасността и ефективността на ЕО, което е неразделна част от съвременната образователна система.

Литература

- [1] Рашидов, А., Методи за защита на Web приложения, Сборник доклади от международна научна конференция Унитех'17, Габрово, 2017, vol.2, pp.I-366-I-372. ISSN 1313-230X.
- [2] Запрянов М., А. Рашидов, Методи за защита на информацията в информационни системи от неправомерен достъп, Сборник доклади от международна научна конференция Унитех'14, Габрово, 2014, vol.1, pp.I-331-I-33. ISSN 1313-230X..
- [3] Рашидов, А., Защита на Web-база от данни от неправомерен достъп // сп. Инженерни науки, 2009, кн.1, ISSN 1312-5702.
- [4] Рашидов, А., Приложение на хаотична синхронизация за защитено предаване на данни при Web-базите от данни, Сборник доклади от международна научна конференция Автоматика и информатика '08, София, 2008, том 1. с.X-21-24. ISSN 1313-1850.
- [5] J. Kallberg and B. Thuraishingham, "Towards cyber operations - The new role of academic cyber security research and education," *2012 IEEE International Conference on Intelligence and Security Informatics*, Washington, DC, USA, 2012, pp. 132-134, doi: 10.1109/ISI.2012.6284146.
- [6] G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano and T. J. Tokola, "Poster: The Need for a Collaborative Approach to Cyber Security Education," *2021 IEEE European*



Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021, pp. 719-721, doi: 10.1109/EuroSP51992.2021.00058.

- [7] J. Kallberg and B. Thuraisingham, "Towards cyber operations - The new role of academic cyber security research and education," *2012 IEEE International Conference on Intelligence and Security Informatics*, Washington, DC, USA, 2012, pp. 132-134, doi: 10.1109/ISI.2012.6284146.

За контакт с автора:

гл. ас. д-р Фатме Рашидова

e-mail: fatme@tugab.bg