КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.144157
УДК 004.49

Гарасимчук Олег Ігорович,
К.т.н., доцент, доцент кафедри захисту інформації
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0002-8742-8872
Oleh.harasymchuk@gmail.com

Опірський Іван Романович,
Д.т.н., доцент, професор кафедри захисту інформації
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0002-8461-8996
Iopirsky@gmail.com

Совин Ярослав Романович,
К.т.н., доцент, доцент кафедри захисту інформації
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0002-5023-8442
Yaroslav.r.sovyn@lpnu.ua

Тишик Іван Ярославович,
К.т.н., доцент кафедри захисту інформації
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-1465-5342
Ivan_tysh@i.ua

Штефанюк Євгеній Федорович
Аспірант кафедри захисту інформації
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-0734-6648
Yevhen.sht@gmail.com

ОРГАНІЗАЦІЯ ЗАХИСТУ РЕЗУЛЬТАТІВ КОНТРОЛЮ ЗНАНЬ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Анотація. Робота присвячена розгляду проблем захисту інформації в системах дистанційного навчання (СДН), які набувають широкого розповсюдження в сучасному світі надання освітніх послуг, як одні з найбільш ефективних та перспективних систем підготовки фахівців. Наведені основні відомості про СДН, що існують на українському та зарубіжному освітніх ринках. Розглянуто загальний принцип застосування такого навчання, основні функціональні компоненти та основні суб'єкти взаємодії в рамках СДН. Детально проаналізовані базові проблеми захисту інформації в сучасних системах дистанційного навчання та загрози з точки зору інформаційної безпеки для таких систем, перелічені основні цілі, які може переслідувати зловмисник при реалізації атак на СДН та уразливості через які він здійснює атаки. Оцінено загрози і дестабілізуючі впливи випадкового характеру. Здійснено порівняння найбільш поширених СДН за такими ключовими параметрами, як загрози хибної реєстрації та автентифікації, загрози порушення достовірності результатів контролю знань та загрози впровадження шкідливого програмного забезпечення. Основну увагу приділено підходам до захисту СДН від загроз підміни користувача (як до авторизації так і вже авторизованого користувача), від загроз використання програмних ботів і скриптів (шляхом застосування методу захисту від використання скриптів на основі прихованих елементів та методу захисту на основі аналізу поведінки), а також загроз використання лекцій, електронних довідників та інших сторонніх навчальних матеріалів. Запропоновано механізм захисту від загроз порушення достовірності результатів контролю знань, в якому описано дії користувача СДН та сервера на наступних етапах: реєстрація, вхід в систему, користувач в процесі заповнення анкетних даних, користувач завершив заповнення анкети, користувач приступає до виконання

тесту/завдання та завершує тестування. Такий алгоритм дій може бути використаний у будь-якій системі дистанційного навчання для захисту від загроз порушення достовірності знань, а його новизна полягає у використанні методів автентифікації користувачів та обмеження доступного їм функціоналу.

Ключові слова: системи дистанційного навчання; загрози реєстрації та автентифікації; загрози контролю знань; моніторинг; захист від загроз

1. ВСТУП

В даний час одним з важливих напрямків в глобалізації освітньої галузі та специфіки навчання за умов карантинних обмежень, що існують в світі у зв'язку пандемією короновірусу, є застосування засобів і систем дистанційного навчання (СДН), що дозволяють адекватно і гнучко реагувати на потреби суспільства. Дистанційне навчання є однією з найбільш ефективних і перспективних систем підготовки фахівців.

В англомовній літературі можна зустріти таку абревіатуру СДН [1]:

- LMS − Learning Management System (система управління навчанням);
- CMS − Course Management System (система управління контентом);
- LCMS − Learning Content Management System (система управління навчальним матеріалом);
- MLE − Managed Learning Environment (оболонка для управління навчанням);
- LSS − Learning Support System (система підтримки навчання);
- LP − Learning Platform (освітня платформа);
- VLE − Virtual Learning Environments (віртуальні середовища навчання).

Найбільш поширеними системами дистанційного навчання є LMS і CMS.

Постановка проблеми. Незважаючи на зростання популярності дистанційної форми навчання та її юридичної значимості, в СДН є безліч загроз безпеки, джерелом яких є слухачі (основні користувачі таких систем), від яких практично не здійснюється захист, тому існує потреба в розробленні механізму захисту результатів контролю знань в системах дистанційного навчання.

Аналіз останніх досліджень і публікацій. У зв'язку із значним поширенням в умовах світової пандемії систем дистанційного навчання зростає й інтерес фахівців з безпеки до таких систем. За цією тематикою існує велика кількість праць вітчизняних та закордонних авторів, де основна увага спрямована на усунення різноманітних видів загроз СДН. Зокрема в [2] автори показують, що розробники сучасних СДН не завжди приділяють належну увагу безпеці своїм продуктів. В [3] автори роблять акцент лише на організаційно-адміністративних методах забезпечення безпеки популярної СДН Moodle. У праці [4] акцентовано увагу на надійному отриманні та зберіганні даних СДН шляхом застосування систем шифрування, а інші аспекти захисту не розглядаються. Науковці у [5] поділяють загрози СДН на загальні та специфічні. До загальних відносять загрози, що є властивими для будь-яких автоматизованих інформаційних систем, наприклад, загрози доступності (dos-атаки), підбір паролю, атаки переповнення буфера, SQL-ін'єкції та ін. Автори виходять з того, що ефективне убезпечення від загроз такого типу в СДН можливе з використанням методів та засобів захисту інформації загального призначення, а тому їх не розглядають. Серед специфічних вони виділяють ті, які залежать від реалізації СДН, та ті, які зумовлені взаємодією суб'єктів та об'єктів СДН. У праці [6] ці автори якраз звертають увагу на специфічні загрози які зумовлені взаємодією суб'єктів та об'єктів СДН. Вони є більш

загальними, виявляються через особливості навчального процесу і проявляються в СДН незалежно від того, яким чином вона спроектована, тому автори пропонують підхід лише для виявлення загроз цього типу. Як видно з цих наведених праць, а також в результаті аналізу багатьох напрацювань інших авторів, можна дійти висновку, що вирішення проблем безпеки є комплексною і багатоаспектною задачею, яка повинна охоплювати широке коло можливих загроз СДН та способів їх нівелювання, не створюючи, при цьому, дискомфорту користувачам. Існує багато невирішених задач або ж тих загроз, яким не приділяється належна увага.

Враховуючи недоліки наведені вище ***метою статті*** є розроблення механізму захисту результатів контролю знань в системах дистанційного навчання, як однієї найбільш важливої її складової.

2. ОСНОВНІ ВІДОМОСТІ ПРО СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

В Україні, як і в багатьох провідних світових державах, дистанційне навчання має статус самостійної форми навчання [7]. Забезпечення юридичної значимості СДН можна гарантувати використовуючи розроблені організаціями-ліцензіатами сертифіковані засоби захисту інформації, тобто організаціями, які мають право на створення засобів захисту інформації. Також дуже важливим є вирішення питання про достовірність інформації, що передається. У той же час конфіденційність суттєвої ролі не відіграє, оскільки інформація, використовувана в навчальних матеріалах, не є секретною. Дистанційне навчання у порівнянні з традиційним очним навчанням має більше можливостей для здійснення різноманітних фальсифікацій. Виходячи з цього основна задача інформаційної безпеки дистанційного навчання полягає у грамотній побудові систем ідентифікації та автентифікації особи слухача. На рис. 1 подано загальну структуру використання СДН.

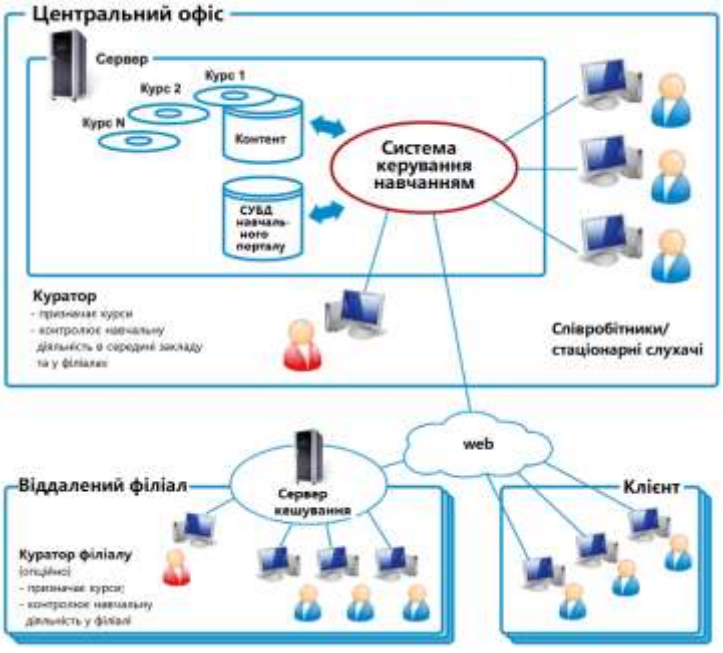

Рис.1. Загальний принцип застосування СДН

Для виявлення ключових проблем організації захисту систем дистанційного навчання, причин і джерел їх виникнення, а також оцінки їх наслідків, необхідно попередньо розглянути типову СДН і виявити в ній найбільш критичні і вразливі місця.

В якості основних функціональних компонентів СДН можна виділити:

1) веб-додаток – зовнішній інтерфейс;

2) база даних, в якій зберігається наповнення навчальних курсів, розміщуються оціночні матеріали, електронні підручники, інформація для студентів;

3) сервер СДН, який є ядром системи і забезпечує: реєстрацію та управління обліковими записами користувачів СДН, розмежування прав доступу до функцій і наповнення СДН, надання доступу до ресурсів як віддаленим користувачам з глобальної мережі, так внутрішнім користувачам локальної мережі навчального закладу, здійснення адміністрування та захист СДН, введення обліку слухачів курсу, створення та імпорт навчальних матеріалів, управління каталогами курсів, відстеження результатів навчання і тестування, реєстрацію інформації про події в СДН, здійснення взаємодії з іншими компонентами внутрішньої інформаційної інфраструктури навчального закладу.

Основними суб'єктами взаємодії в рамках СДН є внутрішні та зовнішні користувачі, яких можна розділити на наступні групи:

1) викладачі навчального закладу;

2) методисти навчального закладу;

3) адміністратори, програмісти, фахівці з інформаційної безпеки інформаційних підрозділів навчального закладу;

4) слухачі (студенти, учні).

3. ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Аналізуючи типовий технологічний процес обробки інформації в СДН можна зробити висновок, що найбільш уразливими з точки зору інформаційної безпеки є процеси:

– передачі ідентифікаційних і автентифікаційних даних користувача СДН;

– обмін даними між браузером віддаленого користувача і веб-сайтом СДН;

– авторизації користувача в СДН (на сервері СДН і в ІС навчального закладу);

– витяг і запис даних в БД СДН і ІС навчального закладу;

– обмін даними між сервером СДН і сервером ІС навчального закладу.

Подібний висновок в першу чергу пов'язаний з тим, що саме в процесі виконання даних дій, найбільш імовірна спроба зловмисника реалізувати атаку на СДН і отримати доступ до її ресурсів, сервісів і даних. Це підтверджується світовою статистикою щодо порушень та інцидентів ІБ, яка показує, що основним джерелом порушень є мережа, включаючи браузер, мережеві ресурси і сервіси, на частку яких доводиться 39,6% всіх порушень. Зловмисник може бути як зовнішнім, так і внутрішнім (переважає зовнішніх) і, при реалізації атаки переслідувати наступні цілі:

– отримання несанкціонованого доступу до ресурсів і сервісів СДН;

– перевищення привілеїв і отримання контролю над СДН;

– отримання через зламану СДН несанкціонованого доступу до внутрішньої ІС навчального закладу;

– крадіжка матеріалів та інтелектуальної власності: навчальних матеріалів, матеріалів оцінювання і матеріалів, що створюються колективно учасниками навчального процесу;

– отримання доступу до персональних даних слухачів та співробітників навчального закладу;

– крадіжка і розголошення персональних даних слухачів та співробітників навчального закладу;

– отримання несанкціонованого доступу та внесення змін до бази даних навчальних відомостей;

– отримання несанкціонованого доступу до внутрішньої службової та іншої конфіденційної інформації, що зберігається і оброблюється в ІС навчального закладу;

– отримання несанкціонованого доступу і крадіжка результатів науково-дослідної та інноваційної діяльності навчального закладу;

– порушення цілісності та/або знищення навчальних матеріалів і даних про навчальний процес;

– порушення доступності веб-сайту і сервера СДН;

– порушення доступності інформації і матеріалів навчальних курсів для користувачів СДН.

Аналіз [8, 9] показує, що при реалізації атак, зловмисник використовує:

– уразливості в веб-додатку і сервісах СДН;

– слабкі паролі і недоліки процесу автентифікації користувачів на сервері СДН;

– помилки в конфігурації і адмініструванні СДН;

– шкідливе програмне забезпечення (віруси, троянські програми, програмні бомби і закладки);

– слабкості системи захисту інформації.

За даними дослідження positivetechnologies [10] більше половини (57%) систем, що зазнали впливів з боку зловмисника містили критичні уразливості, пов'язані з використанням застарілих версій програмного забезпечення і операційних систем.

Найбільшим числом уразливостей, відповідно до [11], що експлуатуються зловмисником при атаці з зовнішньої мережі (наприклад, інтернет), володіють такі види прикладних програм, що активно використовуються в СДН:

– браузери, які використовуються користувачами СДН при доступі до веб-сайту;

– Adobe Reader, Adobe Flash Player і oraclejava, які використовуються при виконанні скриптів, а також читанні і завантаженні документів та мультимедійних файлів.

Крім умисних загроз і атак зловмисника на СДН можуть впливати загрози і дестабілізуючі фактори випадкового характеру. До них відносять катастрофи природного, біолого-соціального та техногенного характеру, збої та відмови програмно-апаратного забезпечення СДН, помилки в діях користувачів.

В системах ДН можна виділити наступні основні загрози:

Таблиця 1.

Загрози систем ДН

Загрози реєстрації і автентифікації		
Загроза	*Реалізація*	*Причина*
Реєстрація додаткових облікових записів з метою вивчення питань тестів	Порушник, за допомогою відкритої форми реєстрації створює новий обліковий запис	Відсутність реєстрації з премодерацією
Перебір пароля	Порушник підбирає пароль до облікового запису викладача/адміністратора по словнику або за допомогою методу «грубої сили»	Відсутність блокування облікових записів при невдалих спробах автентифікації
Перехоплення і аналіз трафіку	Порушник за допомогою атаки «людина посередині» перехоплює і аналізує трафік, що виходить з комп'ютера викладача або адміністратора системи ДН	Передача облікових даних у відкритому вигляді.
Загрози достовірності результатів контролю знань		
Загроза	*Реалізація*	*Причина*
Неповне проходження курсу	Слухач виконує тест або оформляє звіт до завдання без попереднього читання лекційних матеріалів	Відсутність механізмів контролю процесу навчання
Підміна користувача до авторизації	Слухач передає свої облікові дані для авторизації третій особі, яка проходить замість нього окремий етап курсу (тест або завдання) або весь курс повністю	Відсутність механізмів додаткової автентифікації користувачів
Підміна користувача після авторизації	Слухач успішно авторизується в системі ДН і передає комп'ютер в користування третій особі, яка проходить замість нього окремий етап курсу	Відсутність механізмів додаткової автентифікації користувачів в процесі роботи з системою
Використання програмних ботів і скриптів	Слухач використовує програмного бота або скрипт, який проходить за нього окремий етап курсу (тест або завдання)	Відсутність надійних механізмів захисту від програмних ботів і скриптів
Зміна результатів навчання за допомогою підкупу викладачів	Слухач підкуповує викладача, який надалі завищує йому оцінки за виконання тестів і завдань або закриває курс цілком без навчання	Відсутність необхідних організаційних заходів
Використання лекцій і електронних довідників під час тестів і завдань	Слухач використовує лекційні матеріали або електронні довідники для пошуку відповідей на питання з метою підвищити свою підсумкову оцінку	Відсутність механізмів контролю і обмеження дії користувача
Використання звітів інших слухачів для виконання завдань	Слухач використовує звіти інших слухачів під час оформлення звіту до завдання з метою підвищити свою підсумкову оцінку	Відсутність системи анти-плагіат
Використання зовнішніх пристроїв	Слухач використовує зовнішні пристрої для пошуку відповідей на питання з метою підвищити свою підсумкову оцінку	Не існує ефективних механізмів захисту від цього виду загроз
Загрози впровадження шкідливих програм		
Загроза	*Реалізація*	*Причина*
Завантаження шкідливого ПЗ в систему ДН	Слухач завантажує шкідливе ПЗ в систему за допомогою механізмів обміну матеріалами та здачі завдань	Відсутність інтеграції з антивірусним ПЗ
Впровадження програмних закладок в компоненти системи ДН	Адміністратор системи вносить в її компоненти функціональний об'єкт, здатний забезпечити несанкціоновану поведінку	Відсутність спеціалізованого ПЗ для тестування і діагностики компонентів системи
Віддалений запуск	Порушник здійснює запуск завантаженого в	Відсутність

додатків	систему шкідливого ПЗ за допомогою переповнення буфера додатків-серверів або програмних закладок	спеціалізованого ПЗ для тестування і діагностики компонентів системи, а також інтеграції з антивірусним ПЗ
Загрози витоку інформації по технічним каналам		
Загроза	*Реалізація*	*Причина*
Витік акустичної (мовної) інформації	Порушник отримує конфіденційну інформацію безпосередньо з усного мовлення користувача системи або за допомогою функцій її відтворення акустичними засобами системи	Відсутність необхідних організаційних заходів щодо обмеження доступу до приміщень користувачів системи
Оптичний канал витоку	Порушник отримує конфіденційні дані за рахунок перегляду інформації за допомогою оптичних (оптико-електронних) засобів з екранів дисплеїв і інших засобів відображення засобів обчислювальної техніки	Відсутність необхідних організаційних заходів щодо обмеження доступу до приміщень користувачів системи
Витік інформації по каналу ПЕМВН	Порушник отримує конфіденційні дані за допомогою знімання інформації з електромагнітних випромінювань, в основному, монітора і системного блоку комп'ютера	Відсутність необхідних організаційних заходів щодо обмеження доступу до приміщень

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

4.1. Аналіз безпеки сучасних систем дистанційного навчання

З точки зору розглянутих вище загроз проаналізовані сучасні системи ДН на наявність механізмів захисту (Таблиця 2).

Таблиця 2.

Порівняння систем ДН

Механізми протидії загрозам	Системи ДН						
	Sakai	Moodle	Atutor	ILIAS	Canvas	Blackboard	Webtutor
Загрози реєстрації та автентифікації							
Реєстрація з премодерацією	+	+	+	+	+	+	+
Обмеження кількості невдалих спроб автентифікації	+	+	–	–	–	–	–
Захист автентифікаційних даних	–	–	+	+	+	+	+
Шифрування трафіку	+	+	+	+	+	+	–
Механізми додаткової автентифікації	–	+	–	–	–	–	–
Загрози достовірності результатів контролю знань							
Механізми контролю процесу навчання	+	+	+	+	+	+	+
Наявність надійних механізмів захисту від використання програмних ботів та скриптів	–	–	–	–	–	–	–
Механізми обмеження доступу користувача до лекцій та електронних довідників	–	–	–	–	–	–	–
Системи анти-плагіату	+	+	–	+	–	+	–
Загрози впровадження шкідливого програмного забезпечення							
Інтеграція з антивірусами	+	+	–	+	+	–	–
Загальна кількість балів	6	7	4	6	5	5	3

Згідно порівняння систем ДН, наведеним в табл. 1, найбільш захищеною є система Moodle (7 балів), а найменш захищеною – webtutor (3 бали).

4.2. Рекомендації для захисту від загроз достовірності результатів контролю знань

Методи захисту від загроз підміни користувача

1. Підміна користувача до авторизації

Для вирішення проблеми підміни користувача до авторизації можливе використання механізму багатофакторної автентифікації. Для цього на додаток до автентифікації по паролю облікового запису додаються один або кілька таких методів:

А) Одноразові паролі. Для здійснення генерації одноразових паролів, використовуються різні програмні методики. Можлива одностороння і двостороння генерація одноразових паролів. У першому випадку процес генерації пароля буде здійснюватися на стороні сервера, після чого виконується його передача користувачеві, за допомогою електронної пошти або SMS. У другому випадку генерація буде відбуватися одночасно на стороні сервера і клієнта за допомогою генератора псевдовипадкових чисел або на основі тимчасових міток. Зазвичай вона реалізується у вигляді спеціальних пристроїв (etoken) або додатків, однак, як зазначалося раніше, в системах ДН використання спеціальних пристроїв є неможливим. Основний недолік даних методів автентифікації полягає в тому, що паролі які були згенеровані дуже легко передати, що фактично не захищає від навмисної підміни користувача.

Б) Унікальний предмет;

В) Біометричні параметри людини (відбитки пальців, райдужна оболонка, сітківка ока, форма лиця, геометрія рук, рукописний почерк, клавіатурний «почерк», голос).

2. Підміна авторизованого користувача

Для захисту від підміни авторизованого користувача можливе використання механізму прихованого моніторингу і автентифікації. Суть якого полягає в спостереженні за діями користувача і зняття його поведінкової або фізіологічної характеристики, в якості якої може виступати клавіатурний «почерк», «почерк» миші або фотографія.

Методи автентифікації на основі клавіатурного «почерку» і «почерку» миші не вимагають наявності додаткового обладнання, що дозволяє використовувати її для всіх користувачів без винятку. При цьому клавіатурний «почерк» повинен використовуватися при виконанні слухачами завдань, а «почерк» миші при проходженні тестів.

Схема реєстрації та автентифікації для даного методу наведена на рис. 2.

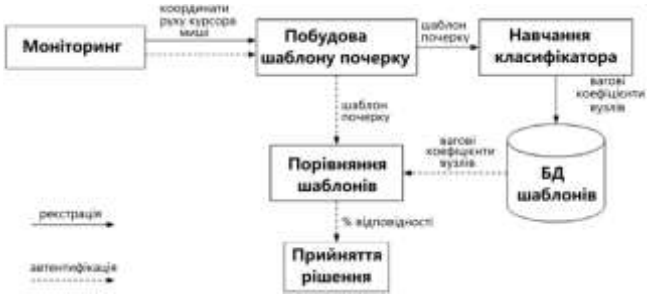

Рис. 2. Схема реєстрації та автентифікації

ISSN 2663 - 4023

При побудові шаблонів «почерку», отримані в процесі моніторингу дані повинні формуватися в набір кривих, які згодом розбиваються на кілька груп, залежно від типу виконаної користувачем дії:

– Переміщення курсору з точки в точку;

– Переміщення курсору з точки в точку, яке закінчується натисканням кнопки миші;

– Відсутність переміщення (тиша).

Основний недолік методів авторизації за "почерком" миші – це використання методів класифікації, які передбачають разове навчання для всіх користувачів. При додаванні нових шаблонів в даному випадку необхідно повне перенавчання класифікатора. Стосовно до систем ДН неможливо повноцінно навчити таку систему за один раз у зв'язку з постійним ростом кількості користувачів.

У випадку застосування клавіатурного «почерку» кінцева система автентифікації повинна складатися з наступних частин:

– Моніторинг дій користувача;

– Побудова шаблонів «почерку» для автентифікації на основі даних моніторингу;

– Навчання класифікатора і подальша автентифікація користувачів.

Завдання моніторингу полягає в тому, щоб надати системі деякий сирий набір даних про затиснуті та віджаті клавіші клавіатури. Сам шаблон «почерку» будується на основі наступних гістограм:

– Гістограми часу утримання клавіш;

– Гістограми часу утримання клавіш при виникненні перекриття;

– Гістограми швидкості друку.

Основний недолік методів авторизації за клавіатурним "почерком"– це час навчання.

Механізм автентифікації на основі форми обличчя застосовується аналогічно, як і у випадку з підміною користувача до авторизації, за винятком того, що знімки з веб-камери необхідно брати або з деякими випадковими інтервалами, або при появі деякого рівня активності в кадрі.

Основним недоліком є підвищення помилок першого роду і необхідність ручного перегляду поданих для автентифікації фотографій, через те, що користувач переважно сконцентрований на роботі з системою навчання, а не на веб- камері.

Методи захисту від використання програмних ботів і скриптів

Оскільки використання програмних ботів і скриптів для виконання завдань є доволі сумнівним то швидше за все не зможе пройти перевірку на плагіат.

А). Метод захисту від використання скриптів на основі прихованих елементів

Даний метод використовують для детектування використання скриптів на основі впровадження в веб сторінку додаткових прихованих елементів.

Б). Метод захисту від використання програмних ботів і скриптів на основі аналізу поведінки

Метод будується на основі методів моніторингу і автентифікації по «почерку» миші, і підходить для детектування як програмних ботів, так і скриптів. Він базується на тому, що боти роблять переміщення курсору на координату за мінімально можливий час. Таким чином шаблон «почерку» миші бота буде характеризуватися відсутністю відхилення від лінійної траєкторії і однаковим часом руху для всіх кривих. Скрипти взагалі не переміщують курсор миші, тому для них шаблон завжди буде порожнім.

Методи захисту від загроз використання лекцій, електронних довідників та інших навчальних матеріалів

ISSN 2663 - 4023

Для унеможливлення використанню лекцій і зовнішніх джерел можливе застосування методу обмеження для користувача функціоналу.

Суть цього методу полягає в створенні обмеження, з якого користувач не може вибратися до закінчення процесу тестування або виконання завдань. Зокрема, ми для захисту від загрози використання лекцій, електронних довідників та інших навчальних матеріалів під час виконання тестів і завдань в веб-орієнтованій системі навчання пропонуємо обмежити наступний функціонал:

– Блокування області переміщення курсора миші – обмеження переміщення курсора рамками вікна браузера;

– Блокування «гарячих клавіш» – перехоплення натискань на такі комбінації клавіш як «Alt + Tab», «Win + d», «Ctrl + Esc» і ін .;

– Закриття сторонніх вкладок браузера;

– Відключення звуку – установка системної гучності на звукових пристроях в значення 0 і блокування мультимедійних клавіш;

– Закриття і блокування подальшого запуску додатків з чорного списку - закриття небажаних програм за допомогою привілеїв відлагоджувача.

4.3. Загальний механізм захисту від загроз достовірності результатів контролю знань

Пропонуємо наступний механізм захисту від загроз достовірності результатів контролю знань:

1. Користувач відвідує центр дистанційного навчання на базі деякого навчального закладу, подає необхідні документи проходить реєстрацію облікового запису в системі дистанційного навчання цього закладу.

2. Повернувшись додому користувач вводить свої автентифікаційні дані в систему ДН.

3. Коли користувач вперше здійснює вхід в систему, то він заповнює певні анкетні дані. Під час цього анкетування у випадкові моменти часу відбувається зняття знімків з веб-камери, які відправляються на сервер для додаткової автентифікації користувача. Також в процесі анкетування здійснюється фіксація координат рухів курсору миші і часу натискань клавіш клавіатури.

4. Після завершення процесу анкетування користувача, дані рухів курсору миші і натискань клавіш клавіатури, що були зафіксовані відправляються на сервер, і, в разі успішної автентифікації користувача за формою обличчя за допомогою захоплених знімків, для нього створюються відповідні шаблони «почерку», які в подальшому будуть використовуватися при автентифікації користувача та наданні йому тих чи інших визначених системою прав.

5. У випадку коли користувач надалі здійснюватиме оформлення звіту до виконуваного завдання чи проходитиме тестування, то системою відбуватиметься обмеження доступного йому функціоналу, а саме: закриття сторонніх вкладок і додатків, блокування області переміщення курсора миші і «гарячих клавіш», а також відключення звуку. Також механізм захисту передбачає фіксацію координат рухів курсору миші і часу натискань клавіш клавіатури в процесі проходження тестування користувачем чи виконання ним контрольних завдань.

Таблиця 3.

Реалізація механізму захисту на окремих етапах роботи користувача

Етапи роботи користувача	*Користувач СДН*	*Сервер*
Реєстрація		Створюється обліковий запис користувача СДН
Вхід в систему	Відправляє свої автентифікаційні дані	Відбувається автентифікація та запускається процес моніторингу
Користувач в процесі заповнення анкетних даних	Відправляються на сервер знімки з веб-камери (1..n) та фіксується функція координат руху курсора миші та часу натискання клавіш клавіатури	Користувач автентифікується за формою лиця та завершується процес моніторингу
Користувач завершив заповнення анкети	Відправляються дані моніторингу	Завершується реєстрація клавіатурного почерку
Користувач приступає до виконання тесту/завдання	Для користувача обмежується користувацький інтерфейс, запускається моніторинг та відправляються на сервер знімки з веб-камер (1..n), фіксується функція координат руху курсора миші та часу натискання клавіш клавіатури	Користувач автентифікується за формою лиця
Тестування завершено	Відправляються дані моніторингу та повертається обмеженого функціоналу	Здійснюється порівняння клавіатурного почерку

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні системи дистанційного навчання набувають останнім часом значної популярності та в свою чергу піддаються все більшому впливу загроз різноманітного характеру. Оскільки основним джерелом порушення цілісності та доступності СДН є дії легальних її користувачів, то акцент щодо забезпечення безпеки СДН необхідно робити саме на захист від загроз пов’язаних з ними.

Запропонований механізм захисту від загроз порушення достовірності перевірки результатів навчання може бути використаний при розробці наступних СДН. Особливість запропонованого підходу для забезпечення інформаційної безпеки СДН полягає у застосуванні в них методів автентифікації користувачів і обмеження доступного їм функціоналу, що значно підвищить достовірність перевірки результатів їх навчання.

Напрямки подальших досліджень можуть бути спрямовані на розробку програмних додатків для реалізації запропонованого механізму захисту СНД від несанкціонованих втручань та подальшої його інтеграції у такі системи, а також подальшої оптимізації та підвищення їх захищеності від багатьох видів загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Богомолов В.А. Обзор бесплатных систем управления обучением / Educational Technology & Society 10(3): 439-454, 2007, ISSN 1436-4522.

[2] Yong Chen, Wu He, Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning 14(5): 108-127, December 2013, Follow journal DOI: 10.19173/irrodl.v14i5.1632

[3] Kassid Asmaa, El kamoun Najib, E-Learning Systems Risks and their Security, International Journal of Computer Science and Information Security (IJCSIS), 14(7): 194-200, July 2016.

[4[Nguyen Huu Phuoc Dai , András Kerti , and Zoltán Rajnai, E-Learning Security Risks and Countermeasures, Emerging Research and Solutions in ICT 1(1):17-25, September 2020, DOI: 10.20544/ERSICT.01.16.P02.

[5] Будік О.О., Чекурін В.Ф. Специфічні загрози інформаційній безпеці систем електронного навчання. // Вісник Національного університету "Львівська політехніка" Автоматика, вимірювання та керування. – 2012. – №741, с.71-76.

[6] Чекурін В.Ф., Будік О.О. Взаємодія об’єктів і аналіз загроз інформаційній безпеці систем електронного навчання. // Вісник Східноукраїнського національного університету ім. В.Даля. – Луганськ, Видавництво СНУ ім. В.Даля, 2011. - №7 (161), Ч1. – С.112-119.

[7] Наказ МОНУ від 25.04.2020 року №466 «Про затвердження Положення про дистанційне навчання» (Із змінами, внесеними згідно з Наказами Міністерства освіти і науки № 660 від 01.06.2013, № 761 від 14.07.2015

[8] Усков А. В. Иванников А. Д. Усков В. Л. Технологии обеспечения информационной безопасности корпоративных образовательных сетей// Образовательные технологии и общество. – 2008. –Т.11, №1. - С. 472 – 479.

[9] Christian Josef Eibl. Discussion of Informtion Security in E-Learning. / Christian Josef Eibl // siegen University, Department of Electrotechnics and Informatics, 2010.

[10] Defta costinelaluminita. Security issues in e-learning platforms. / Defta Costinela-Luminita // World Journal on Educational Technology. – Cyprus, Academic World Education and Research Center, 2011. – Vol.3, issue 3. – pp. 153-167.

[11] Hajwa Hayaati Mohd Alwi, Ip-Shing Fan. E-Learning and Information Security Management. / Hajwa Hayaati Mohd Alwi, Ip-Shing Fan // International Journal of Digital Society. – United Kingdom, Cranfield University, 2010. – Vol. 1, issue 2. – pp. 148-156.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Oleh I. Harasymchuk
Ph.D, Docent, Associate Professor at the Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0002-8742-8872
Oleh.harasymchuk@gmail.com

Ivan R. Opirskyy
Doctor of Science, Professor, Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0002-8461-8996
Iopirsky@gmail.com

Yaroslav R. Sovyn
Ph.D, Docent, Associate Professor at the Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0002-5023-8442
Yaroslav.r.sovyn@lpnu.ua

Ivan Y. Tyshyk
Ph.D, Docent, Associate Professor at the Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0003-1465-5342
Ivan_tysh@i.ua

Yevhenij F. Shtefaniuk
Graduate student at the Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0003-0734-6648
Yevhen.sht@gmail.com

ORGANIZATION OF PROTECTION OF KNOWLEDGE CONTROL RESULTS IN DISTANCE LEARNING SYSTEMS

Abstract. This paper is devoted to the consideration of information security problems in distance learning systems (DLS), which are becoming widespread in the modern world of educational services, as one of the most effective and promising training systems. The basic information about DLS that exist in the Ukrainian and foreign educational markets is given. The general principle of application of such training, the main functional components and objects of interaction within the framework of DLS are considered. The basic problems of information protection in modern distance learning systems and threats from the point of view of information security for such systems are analyzed in detail, the main goals that an attacker may pursue while carrying out attacks on DLS and vulnerabilities due to which he carries out these attacks are listed. Threats and destabilizing effects of accidental nature are also mentioned. The most common DLS's are compared according to such key parameters as threats of corrupt registration and authentication, threats of reliability of knowledge control results and threats of malicious software implementation. The main focus is on the approaches to the protection of DLS from threats of user substitution (both during the authorization and for an authorized user), threats of the usage of software bots and scripts (by applying the method of protection against the use of scripts based on hidden elements and the method of protection based on behavioral analysis), and also threats to the usage of lectures, electronic reference books and other third-party teaching materials. The mechanism of protection against threats to the reliability of knowledge control results is proposed, which describes actions of the DLS user and the server at the following stages: registration, login, user in the process of filling in the questionnaire, user completed the questionnaire, user starts the test / task and completed testing. This algorithm can be used in any distance learning system to protect from threats to the authenticity of knowledge, and its novelty consists in the usage of methods of user authentication and limiting the functionality available to those users.

Keywords:Distance learning systems, registration and authentication threats, knowledge control threats, monitoring, threat protection.

REFERENCES

[1] Bogomolov V.A. (2007). Obzor besplatnyh sistem upravlenija obucheniem [The review of free-of-charge control systems of training]. Technology & Society, 10(3), pp. 439-459.
[2] Yong Chen, Wu He. (2013) Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 14(5), pp. 108-127.
[3] Kassid Asmaa, El kamoun Najib. (2016). E-Learning Systems Risks and their Security. The International Journal of Computer Science and Information Security (IJCSIS), 14(7), pp. 194-200.
[4] Nguyen Huu Phuoc Dai, András Kerti, Zoltán Rajnai. (2020). E-Learning Security Risks and Countermeasures, Emerging Research and Solutions in ICT 1(1), pp. 17-25.
[5] Budik O.O., Chekurin V.F. (2012). Specifichni zagrozi informacijnij bezpeci sistem elektronnogo navchannja [Specific threats to information security of e-learning systems] Bulletin of the National University "Lviv Polytechnic". Automation, measurement and control. No.741, pp. 71-76.
[6] Chekurin V.F., Budik O.O. (2011). Vzaєmodija ob'єktiv i analiz zagroz informacijnij bezpeci sistem elektronnogo navchannja [Interaction of objects and analysis of threats to information security of e-learning systems]. Bulletin of the East Ukrainian National University. Lugansk, Vidavnictvo SNU im. V.Dalja [V. Dahl SNO Publishing House]. 7(161), part1, pp. C.112-119.
[7] Order of the Ministry of Education and Science of Ukraine from 04/25/2020, no. 466. "On approval of the Regulations on distance learning "(As amended in accordance with the Orders of the Ministry of Education and Science number 660 from 01/06/2013, number 761 from 14/07/2015
[8] Uskov A. V. Ivannikov A. D. Uskov V. L. (2008) Tehnologii obespechenija informacionnoj bezopasnosti korporativnyh obrazovatel'nyh setej [Technologies for information security of corporate educational networks]. Educational technologies and society. Vol. 11, no. 1, pp. 472-479.
[9] Christian Josef Eibl. (2010). Discussion of Informtion Security in E-Learning. Siegen University, Department of Electrotechnics and Informatics, p. 160.
[10] Defta Costinela-Luminita. (2011). Security issues in e-learning platforms. World Journal on Educational Technology. Cyprus, Academic World Education and Research Center. Vol.3, issue 3, pp. 153-167.
[11] Hajwa Hayaati Mohd Alwi, Ip-Shing Fan. (2010). E-Learning and Information Security Management. International Journal of Digital Society. United Kingdom, Cranfield University. Vol. 1, issue 2, pp. 148-156.