

Корисна модель відноситься до засобів навчання і може бути застосована для безпечного проведення освіти за дистанційною формою.

Сучасний ринок труда ставить високий рівень вимог до знань та умінь кінцевого спеціаліста, тому освітня організація має забезпечувати достатній контроль знань своїх випускників. Дистанційна освіта є однією з найбільш перспективних форм навчання, однак потребує певних заходів, що забезпечували б належний рівень її якості, зокрема належного її захисту.

Відомо про спосіб дистанційного навчання, за яким передають навчальну інформацію від джерела тим, кого навчають. За допомогою комп'ютера здійснюють тренінг тих, кого навчають, а також проводять контроль рівня засвоєння знань у режимі он-лайн. Учебний матеріал передають особам, яких навчають, у вигляді Web-курсів і/або на електронних носіях, і/або за допомогою он-лайнних телеконференцій, лекцій, семінарів та консультацій з використанням відеоконференцзв'язку в режимі он-лайн, і проводять перевірку результатів теоретичного і практичного засвоєння навчального матеріалу за допомогою тестів або контрольних робіт як в режимі он-лайн (синхронно), так і відстрочено (асинхронно) [Патент UA 17510 U, 15.09.2006]. Вказаний спосіб не бере до уваги можливість підробки результатів виконання учбових робіт. Так, наприклад, контрольні роботи, що будуть виконуватися асинхронно, мають тимчасово зберігати свої результати на комп'ютері учня. Відповідно, виникає загроза підробки цієї звітності. Аналогічна загроза присутня і при он-лайн навчанні, однак тут звітність може бути підроблена безпосередньо перед відправкою на сервер освітньої організації. Можливий також варіант копіювання результатів одного учня на комп'ютер іншого, або перехоплення і копіювання (імітації) інформаційного потоку про виконання роботи, якщо заняття відбувається в режимі он-лайн. Крім того, якщо роботи не матимуть засобів їх надійної ідентифікації, можливий варіант видачі результатів виконання однієї роботи за результат іншої шляхом простої заміни назви виконаної роботи. Вказана загроза в певній мірі стосується і інших типів учбових робіт: лекційних занять (при ознайомленні з якими можна робити певну відмітку), лабораторних робіт (про виконання яких має ставитися певна відмітка), практичних занять (які мають дати певні результати), тощо.

Відомо також про спосіб, за яким розробляють ілюстрований учбовий матеріал, що передається на магнітному носії, або що передається засобами електронного зв'язку, при якому створюють особову електронну сторінку учня, що включає в себе учбовий план по курсам, стандарти за дисциплінами, комплект задач, вправ, завдань, тематики курсових робіт та рефератів, тематики контрольних тестів з дисциплін. Виконують подачу навчального матеріалу у вигляді ілюстрованих аудіолекцій в повному об'ємі курсу з кожної дисципліни. Проводять контроль засвоєння матеріалу учня шляхом контрольних тестів, набір питань в яких створюється комп'ютерною програмою методом випадкових чисел із бази даних питань. При цьому опитування проводять в режимі питання-відповідь, причому в режимі реального часу, а відповіді заносять в особову електронну сторінку учня. Виконують аналіз відповідей учня з метою виявлення поточного рівня його знань з дисципліни, причому на основі цього аналізу створюють програму особових консультацій учня. Із аналізу відповідей всієї учбової групи виявляють складні для засвоєння частини учбової дисципліни та проводять обов'язкові семінари для всіх учнів за допомогою електронних засобів зв'язку з урахуванням запитів учнів. Проводять також індивідуальні консультації учня за його персональними запитам, як в режимі реального часу, так і відстрочено за допомогою електронної пошти, у відповідності з типом запиту. Проводять персональне контрольне тестування учнів, які не пройшли задовільно попереднє тестування. Проводять прийом контрольних робіт учня засобами електронного зв'язку, а результати оцінки робіт заносять в особову електронну сторінку учня. Проводять прийом заліків та екзаменів, причому очно, при обов'язковій явці учня в учбовий центр на екзаменаційну сесію [Патент RU 2002110393 A, 20.01.2004]. За вказаним способом при прийомі контрольних робіт засобами електронного зв'язку можлива підробка результатів їх виконання. Наприклад, результати виконання роботи одним учнем можуть бути розтиражовані на всю учбову групу. При проведенні обов'язкових семінарів (один із видів занять, що можуть бути підроблені) можливе копіювання інформаційного потоку від одного учня до освітньої організації на всю групу. Таким чином, для проведення дистанційного навчання за цим способом також мають бути запроваджені певні заходи для його забезпечення. Зважаючи на ідентичність способу видачі і прийому учбових матеріалів, даний спосіб обирається за прототип.

В основу корисної моделі поставлено задачу удосконалення способу дистанційного навчання шляхом створення захисту від підробки звітності за рахунок застосування криптографічного перетворення над результатом виконання роботи з використанням ідентифікаторів учня та самої роботи, при цьому досягається технічний результат у вигляді підвищення стійкості способу формування звітності в системі дистанційного навчання, а за рахунок цього - значним збільшенням часу, необхідного для її підробки. Стійкість захисту визначається затратами часу, необхідного на його подолання, тобто підробку звітності.

Поставлена задача вирішується тим, що в способі дистанційного навчання, при якому розробляють ілюстрований учбовий матеріал, що передають учневі на магнітному носії або засобами електронного зв'язку, створюють особову електронну сторінку учня, що включає в себе учбовий план по курсам, стандарти за дисциплінами, комплект задач, вправ, завдань, тематики курсових робіт і рефератів, тематики контрольних тестів з дисциплін, та інші необхідні для проведення учбового процесу матеріали в електронному вигляді. Згідно з даною пропозицією кожному учневі, що навчається, присвоюють унікальний ідентифікаційний номер, який надають і зберігають в зашифрованому двоключовим алгоритмом вигляді, а також надають відкритий ключ для його вільного розшифрування. В кожному програмний продукт, що уособлює певну задану роботу, вбудовують унікальний ідентифікаційний номер, який зберігають у програмному забезпеченні в зашифрованому двоключовим алгоритмом вигляді, а з такою такою навчальною роботою поставляють відкритий ключ для розшифровки її ідентифікаційного номеру. При віддаленому виконанні учнем навчальних робіт, що потребують звітності, за допомогою відповідного програмного забезпечення, що уособлює ці роботи, виставляють кінцеву оцінку у вигляді масиву байт, і над виставленою оцінкою проводять криптографічне перетворення з використанням ідентифікаторів учня і роботи. Результат криптографічного перетворення на магнітному носії або засобами електронного зв'язку передають до освітньої організації, де оберненим чином перетворюють його за допомогою пар до ідентифікатора учня і роботи, і заносять оцінку в особову електронну сторінку учня.

У якості коротких відомостей, що розкривають суть корисної моделі, слід відмітити, що технічний результат

досягається за допомогою присвоєння кожному учневі унікального в рамках сукупності усіх учнів ідентифікатора, а також присвоєння унікальних в рамках сукупності усіх робіт ідентифікаторів кожній учбовій роботі, що потребує звітності в процесі навчання. Ідентифікатор учня надається йому та зберігається у його комп'ютері в зашифрованому двоключовим алгоритмом вигляді, причому разом із ним поставляється відкритий ключ для його розшифрування. Таким чином, дізнатися цього едентифікатора учень може, але не може змінити його, бо не знає секретного ключа, за допомогою якого його було зашифровано, ідентифікатори робіт вбудовані в програмне забезпечення, що уособлює кожну окрему роботу, яка потребує звітності, і також зберігаються в зашифрованому двоключовим алгоритмом вигляді. Ключ для їх розшифровки є відкритим і поставляється разом із програмним забезпеченням. Коли учень завершує черговий етап роботи, що потребує звітності, програмне забезпечення, що уособлює цю роботу, виставляє йому певну оцінку. В цю оцінку можуть включатися не лише сам числовий результат, а й необхідні додаткові відомості: час виконання роботи, кількість спроб, і т.д. Тобто оцінка в загальному випадку являє собою сукупність байт. Ці дані мають бути перетворені у незмістовний масив інформації, щоб зломисник не міг його підробити, що виконується за допомогою певного криптографічного перетворення. При цьому перетворенні мають використовуватися ідентифікатори учня і даної роботи, які вбудовуються в зашифрований результат. В перетвореному вигляді результат може зберігатися певний час на комп'ютері учня (при офф-лайн режимі навчання) чи одразу передаватися в освітню організацію (при он-лайн режимі). В освітній організації отриманий результат має бути розшифрованим, тобто над ним виконується обернене криптографічне перетворення, і при цьому використовуються пари до ідентифікаторів учня і роботи. В загальному випадку ці пари функціонально залежать від відповідних ідентифікаторів, наприклад, для симетричного шифрування оцінки ідентифікатором як ключем, пара являє собою сам ідентифікатор, оскільки розшифрування має виконуватися на тому ж самому ключі, що й шифрування. Отримана оцінка і інші необхідні відомості заносяться до особової сторінки учня. Отже, використання криптографічного перетворення оцінки дозволяє попередити її безпосередню підробку. Використання ідентифікаторів учнів дозволяє унеможливити видачу результатів одного учня за результати іншого. Використання ідентифікаторів робіт дозволяє унеможливити видачу результатів виконання однієї роботи за результат іншої. Стьйкість такого методу захисту базується на секретності криптографічного перетворення, алгоритм якого вбудований в програмне забезпечення. При аналізі коду програмного забезпечення для встановлення цього алгоритму трудовитрати повинні оцінюватися біля кількох людино-років. Як приклад криптографічного перетворення можна навести симетричне шифрування на основі ланцюгів Фейстеля масиву байт, що відповідає оцінці, за допомогою ідентифікатора роботи або учня у якості ключа. Аналіз такого складного алгоритму за його асемблерним кодом має займати близько людино-року.

Згідно з запропонованим способом захисту, ідентифікатори студента і роботи є відкритими ключами у двоключовій системі шифрування. Тоді у складі криптографічного перетворення можна виділити два етапи, що вноситимуть залежність зашифрованого результату від відповідних ідентифікаторів: шифрування двоключовим алгоритмом за допомогою ідентифікатора роботи в якості ключа, та шифрування двоключовим алгоритмом за допомогою ідентифікатора учня в якості ключа. В загальному випадку алгоритм вбудовування ідентифікаторів учня та роботи в кінцевий результат може бути довільним. Для забезпечення необхідної криптографічної стійкості вказаний алгоритм має бути двоключовим, що дозволяє унеможливити розшифровку звітності одного учня за допомогою його симетричного ключа, з подальшим зашифруванням цих результатів за допомогою ключа другого учня і видачею чужих результатів за свої. Аналогічно для шифрування ідентифікатором роботи, використання саме двоключового алгоритму не дозволить розшифрувати записаний відмінний результат виконання однієї роботи за допомогою симетричного ключа, замінити назву роботи на необхідну і зашифрувати цю оцінку іншим ідентифікатором роботи, видавши таким чином результат виконання однієї роботи за результат виконання іншої. В якості прикладу двоключового алгоритму можна навести криптосистему RSA, орієнтовний час злому якої на сучасних ПК наближається до тисяч років.

Згідно з запропонованим способом захисту, криптографічне перетворення над отриманою оцінкою проводиться за допомогою спеціально призначеного програмного забезпечення, відокремленого від навчальних робіт. В загальному випадку алгоритм криптографічного перетворення може бути вбудований в кожний програмний продукт, що уособлює окрему навчальну роботу. Такий підхід є незручним на практиці, але головне, що при цьому захищеність реалізації криптографічного перетворення залежить від багатьох прикладних програмістів, що розробляють програмні засоби забезпечення дистанційної освіти. Тому для уніфікації процедури створення звітності і забезпечення належного рівня захищеності всієї системи, алгоритм криптографічного перетворення має бути виведений в окреме програмне забезпечення, наприклад, динамічну бібліотеку.

Здійснення способу дистанційного навчання можна показати на наступному прикладі. Студентові при вступі до навчальної організації присвоюється ідентифікаційний номер і надається доступ до комплексу навчальних матеріалів, що включають ілюстрований учбовий матеріал, учбовий план по курсам, стандарти за дисциплінами, комплект задач або вправ, інших завдань, тематики курсових робіт та рефератів, тематики контрольних тестів з дисциплін, та інші необхідні для проведення учбового процесу матеріали в електронному вигляді. Ці матеріали можуть надаватися через Інтернет за допомогою засобів зв'язку, або, наприклад, можуть надаватися на електронних носіях. Всі навчальні роботи, що потребують звітності (наприклад, усі контрольні роботи), містять вбудовані ідентифікатори. Студент вибирає певну роботу і завантажує відповідне програмне забезпечення, що уособлює цю роботу. Після виконання роботи, програмне забезпечення за своїми внутрішніми алгоритмами оцінювання виставляє студентові певну кількість балів, і формує масив даних про результати виконання даної роботи. В цей масив включається час виконання роботи, номер спроби, кількість правильних відповідей, кількість наданих підказок, тощо. Коротко цей масив даних можна назвати оцінкою. Ця оцінка для унеможливлення її підробки має бути захищена шляхом криптографічного перетворення, першим етапом якого може, наприклад, бути гамування з секретною гаммою. Після цього результат шифрування треба змішати з ідентифікатором роботи, наприклад, зашифрувати двоключовим алгоритмом, використовуючи ідентифікатор студента у якості ключа. Також слід внести залежність результату від ідентифікатора роботи, наприклад, зашифрувати його двоключовим алгоритмом, використовуючи ідентифікатор роботи у якості ключа. Після цього можна виконати додаткові

перетворення результату для підвищення стійкості його захисту. Таким чином, криптографічне перетворення в загальному випадку є складним багатоступінчатим процесом. Отриманий після перетворення результат відправляється до освітньої організації, де він має бути розшифрований. Для цього результат перетворюють в оберненій послідовності, тобто спочатку виконують розшифровування двоключовим алгоритмом, використовуючи у якості ключа пару до ідентифікатора роботи. Потім виконують розшифровування двоключовим алгоритмом, використовуючи у якості ключа пару до ідентифікатора студента. В кінці виконують гамування з заданою гамою, отримуючи масив байт, в якому записані усі результати про виконання даної роботи даним студентом. Ці відомості вносять в базу даних із відповідним відображенням на особовій сторінці студента. Спроба видати чужий результат за свій шляхом підміни ідентифікатора студента потребуватиме значних затрат часу, які, наприклад, при використанні двоключового методу шифрування типу RSA складатимуть тисячі років. Так само спроба заміни ідентифікатора роботи на інший для видачі результату виконання однієї роботи за результат виконання іншої потребуватиме тисяч років при використанні критосистеми RSA. Аналіз всього алгоритму криптографічного перетворення залежатиме від його складності, і для аналізу розглянутого шифру гамування складатиме близько 2-3 людино-місяців. Для більш стійких, наприклад, двоключових шифрів, час аналізу та злому складатиме порядку 1 людино-року. При періодичній заміні окремих етапів криптографічного перетворення такий термін є задовільним для галузі дистанційної освіти.

Таким чином, застосування даного способу дистанційного навчання дозволяє унеможливити підробку звітності за результатами виконання навчальних робіт, підсилює контроль над процесом дистанційної освіти, і тим самим підвищує якість підготовки спеціалістів за дистанційною формою навчання.