УДК 372.833

# МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО ДОСТУПУ ДО СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ

**Тертиця Д.М., Люта М.В.**
Київський національний університет технологій та дизайну
**Розломій І.О.**
Черкаський національний університет імені Богдана Хмельницького

Використання автоматизованих систем у всіх сферах діяльності людини, заснованих на застосуванні сучасних інформаційно-комунікаційних технологій, висунуло цілий ряд проблем перед розробниками і користувачами цих систем. Одна з найбільш гострих проблем – проблема інформаційної безпеки, яку необхідно забезпечувати, контролювати, а також створювати умови для її управління. Стаття присвячена розгляду засобів конфіденційності інформації, яка міститься в документованому середовищі систем дистанційного навчання. В статті запропоновані способи поліпшення надійності та захищеності документованої інформації, які базуються на захисті доступу до певної інформації та ідентифікації дозволеного користувача.
**Ключові слова:** системи дистанційного навчання (СДН), інформаційна безпека, аутентифікація, електронний цифровий підпис (ЕЦП), цифровий водяний знак (ЦВЗ).

**Вступ.** Життя сучасного суспільства неможливе без повсякденного застосування інформаційних технологій. В даний час комп'ютерні системи і телекомунікації визначають надійність систем оборони і безпеки країни, реалізують сучасні інформаційні технології, забезпечуючи обробку і зберігання інформації, автоматизують технологічні процеси.

Масове використання комп'ютерних систем, яке дозволило вирішити проблему автоматізації процесів виробництва, обробки і зберігання інформації, зробило вразливим ці процеси, в результаті чого з'явилася нова проблема – проблема інформаційної безпеки. Захищеною називають інформацію, яка не змінилась в процесі передачі, зберігання і зберегла достовірність, повноту і цілісність даних. Одним з рішень проблеми інформаційної безпеки є розгляд та вибір методів захисту інформаційної системи. Під захистом інформаційної безпеки розуміється сукупність норм і правил, що регламентують процес обробки інформації, виконання яких забезпечує захист від певної кількості загроз і становить необхідні умови безпеки системи.

**Постановка проблеми.** Широке активне впровадження систем дистанційного навчання зумовило не менш активний розгляд впровадження надійних та практичних методів захисту особистої інформації, яка може зберігатись в електронній формі. З активнішим розвитком технологій, існуючі сьогодні методи захисту інформації потребують постійного доопрацювання та підвищення надійності. Враховуючи досвід впровадження старих та інноваційності сьогоднішніх методів захищеності можна запропонувати найпрактичніші методи захисту для систем дистанційного навчання.

**Аналіз останніх досліджень та публікацій.** Пошуком надійнішого методу захисту або ж просто аутентифікації в мережі Інтернет займається чимало IT-компаній, особливо слід відмітити компанії GOOGLE та Microsoft як одних з лідерів по впровадженню надсучасних систем захисту інформації не тільки в мережі, а й на різноманітних носіях, будь то чіпи чи flash-карти.

**Формулювання цілей статті.** Метою роботи є впровадження методу захисту для систем дистанційного навчання, який буде відповідати таким критеріям: надійність, практичність, доступність.

**Виклад основного матеріалу.** Одним із завдань сучасного навчального закладу є підвищення різноманіття видів і форм організації навчальної діяльності учнів та студентів. Навчальна діяльність в дистанційному режимі служить активному розвитку у студента специфічних умінь, необхідних йому для вирішення поставлених навчальних завдань з допомогою засобів телекомунікацій і ресурсів мережі Інтернет. Більшість сучасних студентів активно використовують комп'ютер і Інтернет в своєму житті та освіті. Впровадження в практику роботи вчителя технології дистанційного навчання робить навчальний процес цікавим і індивідуальним, відкриває нові можливості для творчого самовираження студента.

Якщо розглянути особисту інформацію як цінність, що може зберігатись в особистому кабінету користувача, то в цілому можна прийти висновку, що 90% цієї інформації є документована інформація, яка найвірогідніше всього майже не є захищеною від несанкціонованого доступу в разі отримання доступу до особистих даних певних зацікавлених осіб.

Документи, що найчастіше зберігаються в особистих кабінетах та являють найбільшу цінність:

1) інформація про успішність;
2) навчальні посібники;
3) відомості про учнів;
4) приватні рукописи, заготовки текстів – інтелектуальна власність;
5) статті з обмеженням у вільному доступі чи куплені за кошти;
6) списки та переліки спеціалізованої літератури;
7) спеціально заготовлені контрольні тексти та запитання.

Перераховані вище документи можуть мати такі формати: DOC, DOCX, ODT, RTF, TXT, PDF, HTML, EPUB, XPS, DjVu тощо.

Якщо розглянути вірогідні загрози доступу до перерахованих вище документів, то слід відмітити, що загрози самі по собі не виявляються. Всі загрози можуть бути реалізовані тільки при наявності яких-небудь слабких місць – вразливостей, притаманних об'єкту інформатизації.

Уразливість – певна слабкість, яку можна використовувати для порушення інформаційної автоматизованої системи або інформації, яка в ній міститься. Особлива увага при розгляді безпеки інформації повинна приділятися джерелам загроз, в якості яких можуть виступати як суб'єкти (особистості), так і об'єктивні прояви. Причому самі джерела загроз можуть перебувати як всередині об'єкта інформатизації – внутрішні, так і поза ним – зовнішні. Однак найбільшої шкоди інформації та інформаційним системам наносять неправомірні дії певних осіб і комп'ютерні віруси.

З розвитком мережевих інформаційних технологій віруси стали представляти реальну загрозу для користувачів мережевих і локальних комп'ютерних систем.

Типовими причинами порушення інформаційної безпеки та цілісності особистих даних є: помилки осіб або неточні їх дії; несправність і (або) відмова використовуваного обладнання; непередбачувані і неприпустимі зовнішні прояви; несправність і (або) відсутність необхідних засобів захисту; випадкові і навмисні дії на інформацію, що захищається.

Аналіз і оцінка можливостей реалізації загроз повинні бути засновані на побудові моделі загроз, класифікації, аналізі та оцінки джерел загроз, вразливостей і методів реалізації. Моделювання процесів порушення інформаційної безпеки може здійснюватися на основі розгляду логічного ланцюжка: загроза – джерело загрози – метод реалізації – вразливість – наслідки.

Загрози класифікуються за можливостями нанесення шкоди при порушенні цілей інформаційної безпеки; джерела загроз – за типом і місцем розташування носія загрози; уразливості – за належністю до джерела вразливостей, можливих проявів. Класифікація атак являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки.

У сучасній літературній діяльності більшість авторів публікацій ототожнюють загрозу безпеці інформації або з характером (видом, способом) дестабілізуючого впливу на інформацію, або з наслідками (результатами) такого впливу у вигляді збитків, яких зазнали суб'єктом в результаті порушення його прав.

В даному випадку до таких злочинів можна віднести:

– розкрадання – вчинені з корисливою метою протиправні безплатне вилучення і (або) звернення чужого майна на користь винного або інших осіб, які заподіяли збитки власнику чи власнику майна;

– копіювання комп'ютерної інформації – повторення і стійке запечатление інформації на машинному чи іншому носії;

– знищення – зовнішній вплив на майно, в результаті якого воно припиняє своє фізичне існування або приводиться в повну непридатність для використання за цільовим призначенням.

– знищення комп'ютерної інформації – стирання її в пам'яті ЕОМ;

– пошкодження – зміна властивостей майна, при якому істотно погіршується його стан, втрачається значна частина його корисних властивостей і воно стає повністю або частково непридатним для цільового використання;

– модифікація комп'ютерної інформації – внесення будь-яких змін, пов'язаних з адаптацією програми для ЕОМ або баз даних;

– блокування комп'ютерної інформації – штучне ускладнення доступу користувачів до інформації, не пов'язане з її знищенням;

– несанкціоноване знищення, блокування, модифікація, копіювання інформації – будь-які недозволені законом, власником або компетентним користувачем зазначені дії з інформацією;

– обман (заперечення автентичності, нав'язування неправдивої інформації) – навмисне перекручування або приховування істини з метою ввести в оману особа, у веденні якого знаходиться майно, і таким чином домогтися від нього добровільної передачі майна, а також повідомлення з цією метою введення в оману.

Узагальнюючи викладене, в подальшому під загрозами можна розуміти потенційну або реально існуючу небезпеку вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту, що завдає шкоди власнику (власнику, користувачеві) інформаційних ресурсів, який проявляється в небезпеці спотворення і/або втрати інформації, будь-якої неправомірності її використання.

Розглянувши питання загроз безпеки інформації, слід перейти до питання захисту документованої інформації в системах дистанційного навчання. Щоб захистити потрібну вам інформацію в інформаційному середовищі можна вдатися до великого різноманіття захисних систем, але впевнене місце в інформаційному захисті посідає цифровий водяний знак та електронний цифровий підпис.

Однією з важливих проблем інформаційної безпеки є організація захисту електронних даних і електронних документів. Для їх кодування, з метою задоволення вимог забезпечення безпеки даних від несанкціонованих впливів на них, використовується електронний цифровий підпис.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. ЕЦП як спосіб ідентифікації підписувача електронного документу, дозволяє однозначно визначати походження інформації (джерело інформації), що міститься у документі. Завдяки цьому ЕЦП є також надійним засобом розмежування відповідальності за інформаційну діяльність у суспільстві, зокрема, відповідальності за дезінформування.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа. За умови правильного зберігання власником секретного (особистого) ключа його підробка неможлива. Електронний

документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть миттєво виявлені.

9. Задля забезпечення більшої надійності цілісності документу, особливо на прикладі впровадження його в системи дистанційного навчання, слід використовувати цей метод на будь-якому етапі роботи з документообігом.

Слід розуміти, що при підписанні електронного документу його початковий зміст не змінюється, а додається блок даних, так званий Електронний цифровий підпис. Отримання цього блоку можна розділити на два етапи:

На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest).

Цей відбиток має такі особливості:

· фіксовану довжину, незалежно від довжини повідомлення;

· унікальність відбитку для кожного повідомлення;

· неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться при перевірці Електронного цифрового підпису.

На другому етапі відбиток документу шифрується за допомогою програмного забезпечення і особистого ключа автора.

Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна тільки використовуючи Сертифікат відкритого ключа автора.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документу. Нижче можна розглянути ілюстрацію цифрового підпису даних.

Наступним, не менш важливим методом захисту документованої інформації, який може бути використаним задля забезпечення надійності цілісності документів при роботі з системами дистанційного навчання є цифровий водяний знак (ЦВЗ). Щоб комп'ютерний файл, який представляє собою об'єкт авторського права, не міг бути змінений без відома автора, щоб він містив всю необхідну інформацію про правомірне використання, застосовуються стеганографічні вставки, або цифрові водяні знаки (ЦВЗ). Якщо твір піддається якимось змінам, то разом з ним змінюється і видимий водяний знак.

Видимі ЦВЗ досить просто видалити або замінити. Для цього можуть бути використані графічні або текстові редактори. Невидимі ЦВЗ є вбудовані в комп'ютерні файли вставки, які не сприймаються людськими органами зору або слуху. Тому ЦВЗ повинні відповідати наступним вимогам:

– непомітність для користувачів;

– індивідуальність алгоритму нанесення (досягається за допомогою стеганографічного алгоритму з використанням ключа);

– можливість для автора виявити несанкціоноване використання файлу;

– неможливість видалення неуповноваженими особами;

– стійкість до змін носія-контейнера (до зміни його формату і розмірів, до масштабування, стиску, повороту, фільтрації, введення спецефектів, монтажу, аналоговим і цифровим перетворенням).


**Рис. 1. Ілюстрація цифрового підпису даних**

Для підвищення захищеності файлів пропонується підписувати весь контейнер (електронний документ або об'єкт авторського права) з впровадженими ЦВЗ і електронним цифровим підписом, отриманої з використанням закритого ключа автора документа.

Кожен легальний користувач може за допомогою відкритого ключа перевірити справжність і незмінність файлу. Цифровий водяний знак є гарантією того, що навіть якщо зловмисник підпише файл від свого імені, результати перевірки його електронного підпису і ЦВЗ не співпадуть і можна буде встановити порушення. ЦВЗ виступає в якості додаткового рівня захисту, який іноді важко навіть виявити, а тим більше обійти. Цей рівень захисту дозволяє довести авторство при експертизі.

Одночасне незалежне використання декількох технічних заходів захисту ЦВЗ та ЕЦП підвищує рівень захищеності електронного документа в системі. Потрібно витратити чимало коштів (місяці і навіть роки, тисячі і мільйони доларів), щоб підібрати цифровий підпис до електронного документа.

**Висновок.** В статті було розкрито питання захисту документованої інформації, зокрема за допомогою дворівневої аутентифікація, цифрового водяного знаку та електронного цифрового підпису. Таким чином було запропоновано одночасне використання відразу трьох методів захисту інформації, які можна впровадити в системи дистанційного навчання аби надійно зберігати цінну інформацію з простим доступом лише ідентифікованого користувача. Важливо знати, що характерною особливістю електронних даних є можливість легко і непомітно спотворювати, копіювати або знищувати їх. Тому було розглянуте питання безпечного функціонування даних в будь-яких інформаційних системах з використання найнадійніших методів захисту інформації.

## Список літератури:


1. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.
2. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стегоанализ. – М.: Вузовская книга, 2009. – 220 с.
3. Cox I.J. Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco: Morgan Kaufmann Publishing, 2008. – 624 p.
4. Балакин А.В. Использование стеганографических методов для защиты текстовой информации / А.В. Балакин, А.С. Елисеев // Спецвузавтоматика. Спецвыпуск. – 2009. – С. 183-184.
5. Сагайдак Д.А. Способ формирования цифрового водяного знака для физических и электронных документов / Д.А. Сагайдак, Р.Т. Файзуллин // Компьютерная оптика. – 2014. – № 1(38). – С. 94-104.
6. Очнев Д.В. Цифровые водяные знаки как метод защиты текстовых печатных документов / Д.В. Очнев, Е.С. Чиркин // Психолого-педагогический журнал Гаудеамус. – 2012. – № 2(20). – С. 148-149.



**Тертица Д.М., Люта М.В.**
Киевский национальный университет технологий и дизайна
**Розломий И.А.**
Черкасский национальный университет имени Богдана Хмельницкого


## МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОЙ ЗАЩИТЫ ДОСТУПА К СИСТЕМАМ ДИСТАНЦИОННОГО ОБУЧЕНИЯ


**Аннотация**
Использование автоматизированных систем во всех сферах деятельности человека, основанных на применении современных информационно-коммуникационных технологий, выдвинуло целый ряд проблем перед разработчиками и пользователями этих систем. Одна из самых острых проблем – проблема информационной безопасности, которую необходимо обеспечивать, контролировать, а также создавать условия для ее управления. Статья посвящена рассмотрению средств конфиденциальности информации, содержащейся в документированной среде систем дистанционного обучения. В статье предложены способы улучшения надежности и защищенности документированной информации, основанные на защите доступа к определенной информации и идентификации разрешенного пользователя.


**Ключевые слова:** системы дистанционного обучения (СДО), информационная безопасность, аутентификация, электронная цифровая подпись (ЭЦП), цифровой водяной знак (ЦВЗ).

**Tertitsa D.M., Lyuta M.V.**
Kiev National University of Technology and Design
**Rozlomyi I.A.**
Cherkasy National University named after B. Khmelnitsky

## METHODS OF PROVIDING RELIABLE ACCESS TO REMOTE TRAINING SYSTEMS

**Summary**
The use of automated systems in all spheres of human activity, based on the use of modern information and communication technologies, has raised a number of problems for developers and users of these systems. One of the most acute problems is the problem of information security, which must be provided, monitored, and create conditions for its management. The article is devoted to the consideration of the means of confidentiality of information contained in the documented environment of distance learning systems. The article suggests ways to improve the reliability and security of documented information, based on protecting access to certain information and identifying an authorized user.
**Keywords:** distance learning systems (DLS), information security, authentication, electronic digital signature (EDS), digital watermark (CEH).