УДК 004.9

Х. Ю. Іванюк
Львівський інститут банківської справи
Університету банківської справи
Національного банку України,
кафедра економічної кібернетики

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ПІДВИЩЕННЯ КОМПЕТЕНТНІСНИХ ХАРАКТЕРИСТИК ТА ОЦІНЮВАННЯ РІВНЯ ЗНАНЬ АУДИТОРІВ

Безперервний розвиток аудиторів є дуже важливим та водночас складним завданням. Упровадження новітніх технологій та автоматизація процесу навчання значно спрощує та навіть здешевлює це завдання. Проте автоматизація процесу підвищення компетентності аудитора спричиняє загрози, що стосуються несанкціонованого доступу, пошкодження чи викрадення інформації, що міститься в системі. В процесі проектування системи компетентнісної діагностики та підвищення рівня знань аудиторів розроблено низку заходів, що сприяють розпізнаванню користувачів, розподілу їх прав, а також забезпеченню цілісності інформації. В майбутньому планують розширювати засоби захисту інформації у системі компетентнісної діагностики та підвищення рівня знань аудиторів.

Ключові слова: автоматизована система, цілісність інформації, конфіденційність інформації, авторизація, автентифікація, шифрування.

INFORMATION PROTECTION IN THE SYSTEM OF COMPETENCE-BASED CHARACTERISTICS INCREASING AND EVALUATION OF AUDITOR'S KNOWLEDGE LEVEL

Continuous increasing knowledge of auditors is very important and yet difficult task Implementation of new technologies and automation of the learning process much easier and even cheaper this task. However, the automation of the process increasing the competence of auditor entails a number of threats related to unauthorized access, damage or theft of the information contained in the system. In the design process of system for competence diagnostic and increasing knowledge of auditors developed a number of measures to facilitate the recognition of users, the distribution of their rights, and to ensure its integrity. In the future it is planning to expand data protection system competence diagnosis and increased knowledge of auditors.

Key words: automated system, integrity of information, confidentiality, authorization, authentication, encryption.

Вступ

Розвиток персоналу є системою взаємопов'язаних дій, найважливіші елементи якої: розроблення стратегії розвитку персоналу; прогнозування і планування необхідності залучення персоналу певного кваліфікаційного рівня; управління кар'єрним ростом. Можливість навчання та розвитку повинна надаватись усім працівникам, адже це не лише підвищує ефективність праці, але й покращує моральний клімат, спрощує процес делегування повноважень та задач і, в результаті, підвищує гнучкість управління [1].

Що стосується аудиторських фірм, то питання підвищення кваліфікації та підтримання її на належному рівні стає дедалі важливішим, з огляду на посилення конкуренції на ринку аудиторських послуг [2].

Для внутрішніх аудиторів особливо важливі наявність знань, умінь, навичок та інших компетенцій, необхідних для виконання їх обов'язків. Також важливим є отримання професійної сертифікації та відповідних кваліфікацій, для кращої демонстрації професійної компетенції [3]. Зважаючи на це, всі аудитори України, які займаються професійною діяльністю, зобов'язані покращувати свої професійні знання щороку протягом сорока навчальних годин [4].

Побудова моделі посадових компетенцій є якісно новим підходом до підвищення рівня знань, умінь та навичок. З іншого боку, для якісної реалізації такого підходу необхідно використовувати автоматизовані інформаційні системи для навчання та підвищення рівня знань.

Використання обчислювальної техніки в навчальному процесі дає змогу значно покращити якість підготовки, зокрема, шляхом раціонального розподілу матеріалу, що вивчається, та контролю над самостійною діяльністю осіб, які навчаються, істотно розширює можливості індивідуалізації навчання, стимулює потяг до знань, дозволяє зробити процес навчання ефективним і захопливим [5].

Аналіз досліджень та публікацій

На ринку існує декілька лідерів серед компаній, що розробляють програмне забезпечення, призначене для проектування курсів електронного навчання. Серед них найпопулярніша в світі система із закритим вихідним кодом Blackboard і дві найпопулярніші системи з відкритим кодом – Moodle і Sakai [6]. Проте ці системи мають також недоліки. Зокрема, в системі Moodle використовується велика кількість сторонніх додатків, що ускладнює оновлення системи до нових версій. Часто виникають труднощі під час спроб інтегрувати систему Sakai з іншими системами на підприємстві. А основним недоліком обох цих систем є відсутність повного набору інструментів для реалізації компетентнісного підходу [7]. З іншого боку, система Blackboard позбавлена більшості цих недоліків, проте вона дуже громіздка та потребує значних затрат апаратних засобів. Інтерфейс цієї системи дуже заплутаний та містить велику кількість надлишкових зв'язків. Ще одним вагомим недоліком є велика вартість системи, яка постійно зростає з розширенням системи [8].

Питання захисту інформації в автоматизованих системах широко розглядали такі вчені: М. В. Гайворонський, В. С. Галатенко, О. М. Новіков, А. Ю. Щеглов та ін. Науковці С. Л. Литкін, А. М. Береза, А. І. Власов, В. Л. Яковлєв та ін. досліджували проблеми проектування та розроблення автоматизованих систем.

Постановка завдання

Отже, використання новітніх технологій у процесі підвищення кваліфікації має істотні переваги порівняно з традиційним навчанням [9]. З іншого ж боку, інформатизація процесу навчання спричиняє певні загрози, зокрема загрозу втрати, пошкодження чи викрадення інформації.

Автоматизована інформаційна система компетентнісної діагностики та підвищення рівня знань аудиторів містить конфіденційну інформацію про кожного користувача, а саме його прізвище, ім'я, посаду, відділ, в якому він працює, тощо. Також у системі міститься інформація про навчання кожного аудитора, його успішність та слабкі сторони. Вся ця інформація потребує захисту від несанкціонованого доступу. А також постає необхідність розмежовування доступу між різними користувачами та забезпечення можливості розподілу доступу між викладачами та користувачами цієї системи. З іншого боку, в системі збережена велика кількість навчальної інформації, даних для тестування та зв'язків між ними. Особливу увагу в цьому випадку необхідно приділити цілісності даних, оскільки найменше пошкодження може спричинити значну втрату необхідної інформації.

Виклад основного матеріалу

Першим етапом захисту інформації в автоматизованій системі підвищення компетенцій аудиторів прийнято ідентифікацію та автентифікацію. Ідентифікація – це процедура, що дозволяє здійснювати розпізнавання користувача в системі. Зазвичай для цього використовується наперед визначене ім'я (ідентифікатор) чи інша інформація про нього, яку сприймає система. Фактично ідентифікація – це встановлення особистості користувача. Автентифікація – це процедура перевірки

відповідності ідентифікатора користувачу системи. За допомогою автентифікації система повинна пересвідчитись, що користувач той, за кого себе видає [10].

Існує декілька способів ідентифікації та автентифікації.

Можна виділити три найпоширеніші види ідентифікації [11]:

- парольна ідентифікація – всі зареєстровані користувачі системи повинні отримати персональні реквізити;
- апаратна ідентифікація – користувач визначається за певним ключем, що є його особистою річчю.

Однофакторні методи можна поділити на [11]:

- логічні, до них належать ключові фрази, паролі, що вводяться з клавіатури;
- ідентифікаційні, ключова інформація зберігається на зовнішньому носії: дискета, штрихкартка, магнітна картка тощо;
- біометричні, їх особливістю є використання унікальних характеристик людини, таких як: сітківка ока, відбитки пальців, голос тощо.

У розробленій автоматизованій системі розвитку компетенцій аудиторів прийнято використовувати парольну ідентифікацію та логічну автентифікацію, а саме пари логін-пароль (рис. 1). Для підвищення ефективності захисту процедури автентифікації прийнято рішення здійснювати шифрування паролів користувачів.

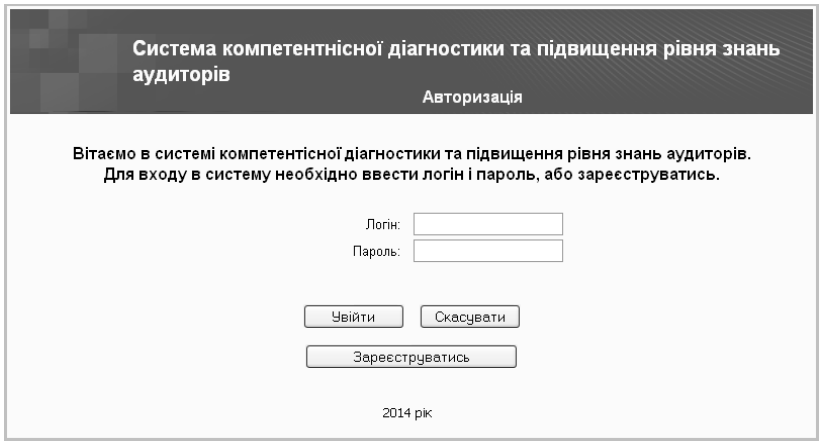

Рис. 1. Авторизація користувачів у системі компетентнісної діагностики та підвищення рівня знань аудиторів

Методом шифрування називається алгоритм, який визначає порядок трансформації вхідного повідомлення у вихідне. Ключем шифрування є набір параметрів, що використовується для застосування методу [12].

Для шифрування паролів вирішено застосовувати алгоритм MD5. Цей алгоритм розробив у 1991 р. професор Рональд Л. Рівест. Головною перевагою MD5 є те, що зашифровані дані неможливо відновити [13]. За допомогою цього алгоритму в базу даних паролі потрапляють вже в зашифрованому вигляді, їх викрадення не дає жодної користі зловмисникові (рис. 2).

Edit Data - PostgreSQL 9.0 (localhost:5432) - tbl_portal - tbl_user

File Edit View Tools Help

No limit

	id [PK] integer	login character	password character varying(200)	last_login_date date	start_page character varying(	name character var	last_name character v	father_name character var	securitylevel numeric	catego numeri
1	1	root	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	adm_start_new.jsp	Адміністратор	"	"	1	1
2	2	user1	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Test	User	1	3	2
3	3	user2	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Test	User	2	3	2
4	125	igor	1562eb3f6d9c5ac7e159c04a96ff4dfe	2013-11-27	test_testing_begin.jsp	Ігор	Пиріг	Миколайович	3	1
5	129	ist	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Сергій	Іванців	Тарасович	3	1
6	130	makhn	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Олег	Махнюк	Михайлович	3	1
7	136	KD	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Христина	Джала	Юріївна	2	2
8	5	ivan2	c4ca4238a0b923820dcc509a6f75849b	2013-11-27	test_testing_begin.jsp	Христина	іванців	Зіновіївна	2	2

Рис. 2. Частина таблиці, що містить дані про користувача, зокрема його логін та пароль

Для ґрунтовнішого розмежування користувачів системи прийнято використовувати вибірковий метод захисту даних у системі. Вибірковий метод захисту визначає різні права доступу для користувачів до різних або однакових даних у системі [14].

В автоматизованій системи компетентнісної діагностики та підвищення рівня знань аудиторів визначено три групи користувачів з різними правами доступу, зокрема: адміністратор, менеджер тестування та користувач (рис. 3).

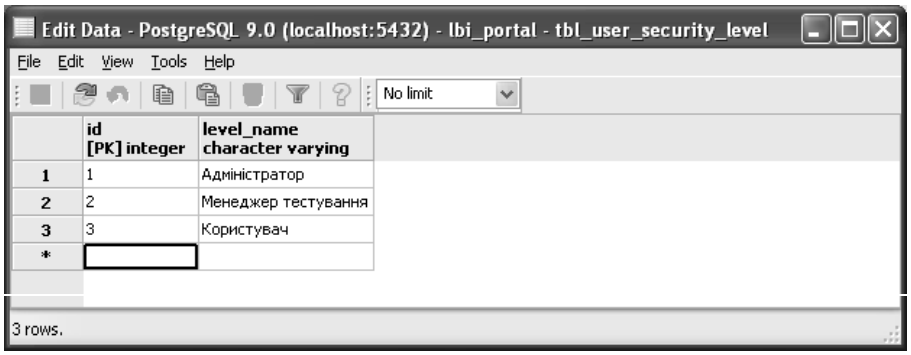

Рис. 3. Таблиця, що визначає права доступу, які можуть надаватись користувачам

Адміністратор має доступ до всіх даних, що містяться в системі. Він має права для створення, видалення та редагування алгоритмів тестувань, категорій користувачів, рівнів складності, типів питань, тем, типів відповідей, рівнів доступу користувачів, категорій користувачів, додавання, видалення користувачів та редагування їх даних тощо. Права адміністратора є найширшими, адміністратор має змогу надавати права доступу іншим користувачам, зокрема права адміністратора та укладача тестування (рис. 4).

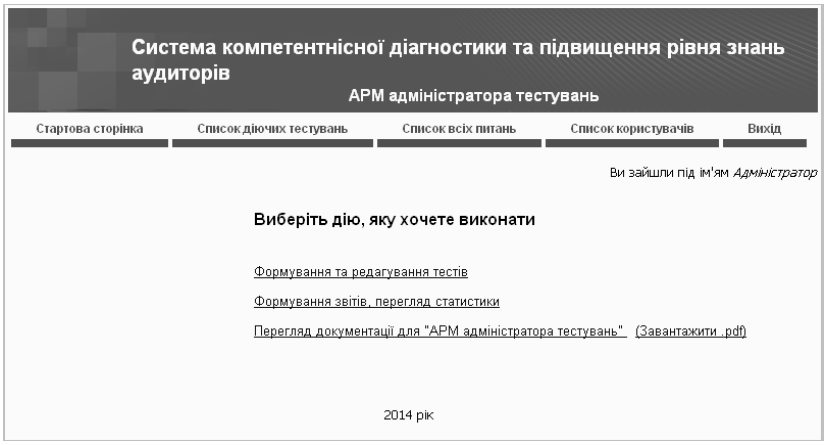

Рис. 4. Автоматизоване робоче місце адміністратора тестувань

Менеджер тестувань має доступ до тестувань, які він створив, а також можливість створювати нові тестування та додавати нові питання в систему. Менеджер тестування також долучає користувачів до тестування та визначає кількість спроб, які вони можуть використовувати для проходження тестування. Крім того, він має змогу переглядати звіти з тестувань як для окремого користувача, так і для групи користувачів (рис. 5).

Користувач має доступ лише до інформаційної частини системи. Він може проходити тестування, вивчати терміни, ознайомлюватись з нормативними документами, статтями, підручниками, відео- та аудіоматеріалами тощо (рис. 6).

Рис. 5. Автоматизоване робоче місце менеджера тестувань

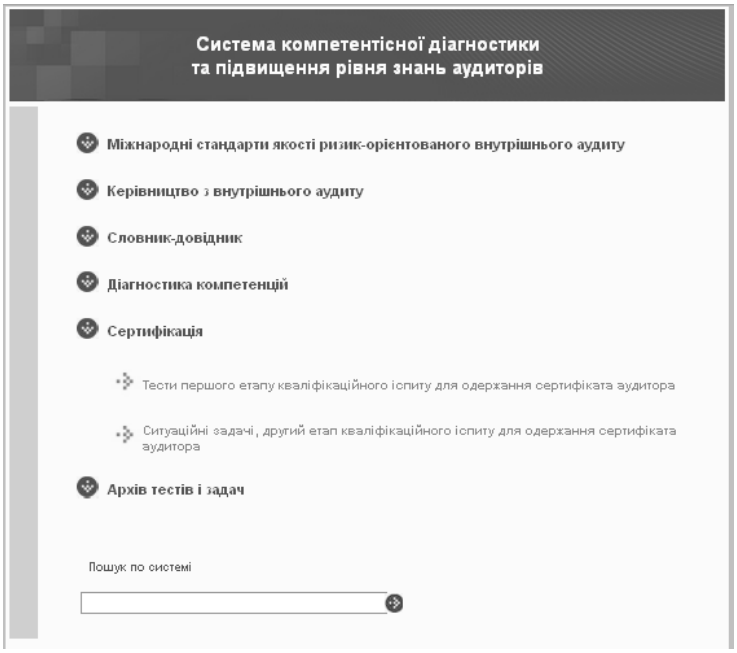

Рис. 6. Автоматизоване робоче місце користувача

Ці засоби забезпечують розмежовування інформації, адже кожен користувач, який здійснює вхід у систему, отримує доступ лише до інформації, доступ до якої йому передбачений. Також база даних розроблена так, щоб ускладнити отримання відповідей на питання, у випадку викрадення інформації, що міститься в базі даних. Це забезпечується двома способами: по-перше, ніхто з користувачів системи не має прямого доступу до бази, а лише за допомогою WEB-інтерфейсу автоматизованого робочого місця адміністратора та автоматизованого робочого місця менеджера тестування (рис. 4, 5). По-друге, питання та відповіді на них, а також вся інформація про питання зберігаються в різних таблицях, тому зловмиснику, не знаючи будови бази даних, дуже складно отримати користь з викраденої інформації (рис. 7).

Проте невирішеною залишається проблема цілісності даних, адже пошкодження найменшої частини даних чи зв’язків між ними може вивести з ладу певний модуль чи навіть всю систему. Щоб запобігти цій загрозі, створено програмний комплекс, який здійснює періодичну архівацію усіх даних системи. Також цей модуль може запустити адміністратор системи, для додаткового проміжного збереження даних. Він дає змогу зберегти поточний варіант бази даних, з поточною датою та часом проведення операції. Отже, якщо виникне проблема з цілісністю даних, достатньо лише розгорнути останню збережену версію чи, за необхідності, будь-яку версію бази даних.

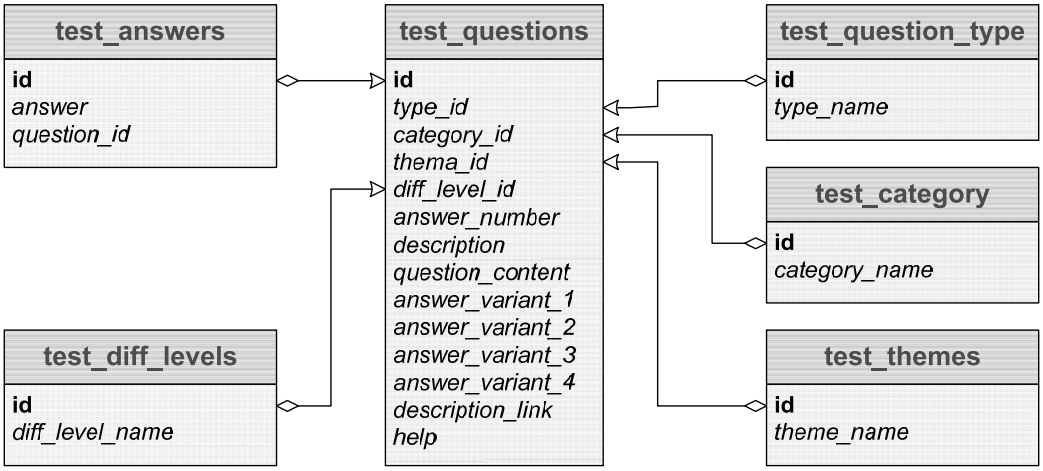

Рис. 7. Частина структури бази даних, що відображає спосіб збереження питань у БД

Проте надійний захист інформації можна забезпечити лише комплексним використанням різних заходів. У сукупність засобів та методів захисту інформації входять апаратні та програмні засоби, організаційні заходи та захисні перетворення [12].

- Апаратний, чи схемний, захист полягає у наявності в приладах ЕОМ чи інших технічних засобах для обробки та передавання інформації спеціальних схем, розроблених для захисту та контролю інформації.
- Програмні методи захисту є сукупністю програм та алгоритмів, що розроблені для розмежування доступу, спрямованого на запобігання несанкціонованому використанню інформації.
- Суть методу захисних перетворень полягає у подаванні інформації, що зберігається в системі та передається каналами зв'язку, в закодованому вигляді, щоб унеможливити використання цієї інформації.
- Організаційні засоби захисту інформації являють собою сукупність дій, спрямованих на перевірку та підбір персоналу, що задіяний у підготовці та експлуатації інформації та програм.

Висновки

Одним з важливих етапів розроблення системи компетентнісної діагностики та підвищення рівня знань аудиторів є розроблення засобів, спрямованих на захист інформації, збереженої в системі. Зокрема, розроблено заходи, які забезпечують розмежування даних між користувачами. Тобто кожен користувач може бачити лише свої персональні дані та працювати за власним навчальним планом. Ці засоби реалізовано за допомогою використання процедур ідентифікації та автентифікації. Також у системі розроблено модуль, спрямований на періодичне збереження інформації, що міститься в системі, для швидкого відновлення цієї інформації, у разі її пошкодження чи втрати.

У майбутньому планується розвиток цієї системи в змістовому та логічному напрямах, а також поглиблення захисту системи від несанкціонованих втручань.

1. Красношапка В. В. Управління людськими ресурсами: курс лекцій. – К.: К., 2004. – 42 с. 2. Tom Campbell, Keith A Houghton. Ethics and auditing. – Canberra: ANU E Press, 2005. 3. Міжнародні стандарти професійної практики внутрішнього аудиту. The Institute of Internal Auditors, 2013. 4. Етичні вимоги до професії аудитора // Вісник бухгалтера і аудитора України. № 15–16, серпень 2007 р. 5. Теория и практика управления персоналом: учеб.-метод. пособ. / Авт.-сост. Г. В. Щёкин. – 2-е изд., стереотип. – К.: МАУП, 2003. – 280 с. 6. Boroch D. Student Success in Community Colleges: A Practical Guide to Developmental Education / Deborah J. Boroch, Laura Hope, Bruce M. Smith, Robert S. Gabriner, Pamela M. Mery, Robert M. Johnstone, Rose Asera. – San Francisco: Jossey-Bass Publishers, 2010. 7. Monarch Media Inc. Business white paper open–source

learning management systems:Sakai and Moodle, 2010. www.Monarchmedia.com. 8. Дьяченко А. В. Построение информационных систем непрерывного образования на основе интернет-технологий / А. В. Дьяченко, В. Г. Манжула, А. Э. Попов, И. Н. Семенихин, А. П. Толстобров. – Академия Естествознания, 2010. 9. Obringer, Lee Ann. How E-learning Works. 01 October 2001. HowStuffWorks.com. 10. Гайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.. 11. Охота Д. Б. Технології комп'ютерної безпеки [Текст] / Д. Б. Охота. – Рівне: МЕГУ, 2011. – 97 с. 12. Митні інформаційні технології: навчальний посібник / за ред. П. В. Пашка. – К.: Знання, 2011. – 391 с. 13. Руслан Коржик. Алгоритм шифрования MD5 // Компьютерная газета № 18, 2006 г. http://www.nestor.minsk.by/kg/. 14. Організація баз даних та знань: підручник / В. В. Пасічник, В. А. Резніченко. – К.: Видавнича група BHV, 2006. – 384 с.

УДК 681.3

А. О. Ігнатович
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

МЕТОД АДАПТИВНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

За результатами аналізу особливостей захисту інформації в комп'ютерних мережах обґрунтована потреба застосування біометричних даних у сервісах аутентифікації користувачів. Запропоновано метод адаптивної автентифікації користувачів у ступеневій системі захисту інформації у комп'ютерній мережі на основі біометричних даних – відбитків пальців.

Ключові слова: захист інформації, аутентифікація, комп'ютерна мережа, біометричні дані, відбитки пальців.

BIOMETRIC DATA BASED METHOD OF ADAPTIVE USER AUTHENTICATION IN COMPUTER NETWORKS

According to the analysis of peculiarities of data protection in computer networks the necessity of usage of biometric data in user authentication services is founded. Adaptive method of user authentication in multilevel data protection system of computer network based on biometric data of fingerprints is introduced.

Key words: data protection, authentication, computer network, biometric data, fingerprints.

Вступ

Проблема захисту інформації від суб'єктів, які не мають на це права, має багатолітню історію. Особливо актуальною стала ця проблема тепер, під час масового застосування комп'ютерних технологій. Велика кількість вчених та дослідників працюють над ефективним розв'язанням цієї багатогранної проблеми. За результатами цих досліджень сформувалися такі напрями наукових досліджень, як криптографія та захист інформації. Багато розроблених методів,