УДК 004

А.О. ОСІДАЧ
Національний університет "Львівська політехніка"

РОЗРОБЛЕННЯ АЛГОРИТМУ ВЕРИФІКАЦІЇ ДОКУМЕНТІВ

Встановлено та обґрунтовано необхідність розробки алгоритму верифікації, яка криється у збільшенні кількості інформації, що обробляється, передається і зберігається в автоматизованих системах управління підприємств і організацій, що призведе, в свою чергу, до необхідності вирішення завдань, таких як забезпечення конфіденційності, цілісності, підтвердження авторства; створення захищеного електронного документообігу та ін. Проведено розробку алгоритму верифікації документів, побудованого на складності завдання факторизації, і його застосування в системах захисту документів від підробки. Складено блок-схему процесу верифікації документів. Доведена необхідність застосування криптографічного перетворення інформації для розробки сучасних засобів захисту інформації. Наголошено, що верифікація, або іншими словами перевірка справжності, на сьогодні є головним пріоритетним напрямком інноваційного характеру у криптографії. Описано детально процедуру верифікації, яка описується як звід необхідних правил перевірки справжності операції, що виконується стосовно інформаційного об'єкту в рамках виконання кроку, визначеного як верифікація. Склад виконуваних правил перевірки справжності залежить від групи, типу документа і його поточного статусу. Зазначається, що єдиним результатом виконання процедури верифікації є підтвердження істинності чи хибності логічного виразу. Відокремлено, що зазначена процедура може бути застосована до примірника інформаційного об'єкта, який саме перевіряється.

Практична реалізація наведеного алгоритму верифікації документів накладає додаткові обмеження, які описані на сторінках дослідження. За умови наявності зазначених обмежень, у роботі пропонується забезпечити ряд розробок, що стосуються врахування відповідного переліку користувачів; здійснення прив'язки до засобів електронного цифрового підпису; зміни статусу затвердження документа залежно від стадії верифікації; злиття з операційною моделлю. Зазначається, що механізм формування та перевірки електронного цифрового підпису засновано на асиметричних схемах шифрування, при використанні яких генеруються два математично взаємопов'язаних ключа. Застосування розробленого алгоритму на практиці дає високий рівень захищеності в сучасному інформаційному середовищі.

***Ключові слова: в**ерифікація, алгоритм, документ, електронно-цифровий підпис, ключ, криптографія, підробка, захист інформації, перевірка справжності.*

A.O.OSIDACH
National University "Lviv Polytechnic"

DEVELOPMENT OF DOCUMENT VERIFICATION ALGORITHM

The necessity of development of the verification algorithm is established and substantiated, that lies in the increase of the volume of information processed, transmitted and stored in the automated control systems of companies and organizations leading to the need to address problems such as ensuring confidentiality, integrity, proof of authorship; creation of secure electronic circulation of documents, etc. The document verification algorithm based on the complexity of the factorization task and its use in systems of document protection against forgery was developed. The flowchart of the document verification process was made. The necessity of the use of cryptographic transformation of information for the development of modern information security means was proved. It is emphasized that today verification, or authentication in other words, is a top priority direction of innovative nature in cryptography. We describe in detail the procedure of verification that is a set of necessary rules of authentication carried out regarding the information object within the step of the operation defined as verification. Composition of the carried out authentication rules depends on the group, type of the document and its current status. It is noted that the only result of carrying out the verification procedure is to confirm the validity or falsity of a logical expression. It is singled out that this procedure can be used to the copy of the information object being checked.

Practical implementation of the above document verification algorithm imposes additional restrictions that are described in the research paper. Provided these restrictions, we suggest to provide a number of developments concerning: consideration of the relevant list of users; binding to digital signature means; change of the document approval status depending on the verification stage; merger with the operating model. It is noted that the mechanism of formation and verification of electronic digital signatures is based on asymmetric encryption schemes, using two mathematically related keys when generating them. The use of the developed algorithm in practice gives a high level of protection in the modern information environment.

***Keywords:** verification, algorithm, document, electronic digital signature, key, cryptography, forgery, information protection, authentication.*

Постановка проблеми

Однією з найбільш важливих цінностей, що створені людством, на початку третього тисячоліття, стає інформація. Інформація виникає, створюється, зберігається, розповсюджується і т.д. кожну секунду людського життя у всіх сферах, вона є основним механізмом взаємодії людей між собою. Її роль в сучасному світі настільки велика, що інформаційна індустрія стала однією з провідних галузей наших днів. У свою чергу, поширення інформаційно-обчислювальних систем в повсякденному житті зробило їх привабливими для різного роду інформаційних атак. На основі зазначеного, значно підвищилася актуальність завдання збереження різного роду інформації та її основних властивостей як в процесі зберігання і обробки, так і при передачі відкритими каналами зв'язку. Одним з ефективних варіантів розв'язання задачі, в таких умовах сталого розвитку інформаційних систем, є застосування сучасних методів криптографії.

Актуальність дослідження

Фундаментальною базою сучасних інформаційних технологій виступають сучасні комп'ютерні і телекомунікаційні технології, які надзвичайно інтенсифікували інформаційні процеси в сучасному суспільстві. Проте, ходіння паперових документів і цінних паперів, на сьогодні, у сучасному інформаційному суспільстві, продовжує грати надзвичайно важливу роль і, в доступному для огляду майбутньому, роль паперових документів видається настільки ж значною. Незмірний збиток суспільству завдається таким негативним явищем як підробка документів, цінних паперів та грошових купюр. Це робить актуальним розробку систем випуску і верифікації автентичності паперових документів від підробки. Принципово новий рівень захисту від підробки забезпечується нещодавно запропонованою технологією криптографічного захисту матеріальних об'єктів.

Ступінь дослідження в науковій літературі

Методологічна та теоретична база дослідження проблем верифікації документів, на сьогодні, тільки формується. Окремі проблематичні аспекти, що виникають при створенні, формуванні та впроваджені сучасних криптографічних систем розглядаються на сторінках таких науковців, як О.В. Бабаш, Г.П. Шанкін [1], В.П. Бабак [2], О.М. Бевз, Р.Н. Квєтний [3] та ін.

С.П. Панасенко у своїй праці [4] розглядає алгоритми блокового симетричного шифрування. Подає загальну класифікацію криптографічних алгоритмів. Пропонує більше 50 алгоритмів шифрування: історію створення та використання, основні характеристики та структура, переваги і недоліки. Описує різні види криптоаналітичних атак на алгоритми шифрування і на їх реалізації у вигляді програмних або апаратних шифраторів.

Також варто відзначити роботу С.Г. Баричєва, В.В. Гончарова, Р.Є. Сєрова [5]. На сторінках праці у систематизованому вигляді розглянуті питання створення симетричних і асиметричних криптографічних систем захисту інформації. Описано алгоритми електронних цифрових підписів, системи управління криптографічними ключами, імітозахисту інформації.

Загальну низку робіт у сфері захисту інформації формують праці таких вчених як: Б.Я. Рябко, А.Н. Фіонов [6], А.А. Малюк [7], М.А. Шолохова [8], Г. А. Смирнов [9], А. Круглов, Б.І. Скородумов [10], І.М. Ажмухамедов [11] та ін. Дослідження зазначених праць у сукупності розвиває основні положення щодо загальних механізмів криптографічного аналізу інформації у програмній реалізації, етапи розвитку криптографічного захисту та принципи його вдосконалення в рамках вирішення загальної проблеми забезпечення інформаційної безпеки.

Виокремлення невирішених раніше частин загальної проблеми, яким присвячується означена стаття. Технологія захисту матеріальних об’єктів від підробки, у загальному вигляді, вивчена доволі масштабно. Виходячи з того, що задача декомпозиції об’єктів вимагає високого рівня визначення умов, системи криптографічного захисту є дієвими та надійними, що сприяє їх широкому застосуванню. Проте, практичне застосування зазначених систем, виявило наявність мітки великого розміру, це, у випадку з перевіркою справжності документів, є істотним недоліком.

На основі вищевикладеного, варто зазначити, що дана наукова робота пов’язана з розробкою алгоритму верифікації документів, який є сучасною дієвою криптографічною системою захисту документів, побудованого на вдосконаленні декомпозиції об’єктів, шляхом визначення обмежень та впровадження ряду розробок.

На сторінках даного наукового дослідження розробляється алгоритм верифікації документів від підробки і вирішується питання про підвищення рівня захищеності від широкого спектра атак на систему, що визначає практичну важливість теми дослідження.

Мета дослідження

Здійснити розроблення алгоритму верифікації документів, з метою застосування його в системах захисту документів від підробки. Скласти блок-схему процесу верифікації документів. Обґрунтувати необхідність застосування криптографічного перетворення інформації для розробки сучасних засобів захисту інформації. Сформувати поняття верифікації документів та детально описати процедуру верифікації.

Виклад основного матеріалу

Масштабність інформації представленої в сучасному інформаційному просторі вражає, форми подання документованої інформації, сьогодні, існують дві: аналогова і електронна [6]. Перша форма – це надання інформації в середовищі фізичних об'єктів [7]. Друга – в електронно-цифровій формі [12]. Таким чином, є можливість стверджувати, що процес обробки документів в сучасних системах документообігу носить змішаний характер (електронний та аналоговий) [4, 7].

У процесі життєвого циклу, до кожного документа, постає вимога справжності, тобто особливість документу зберігати свій початковий стан від моменту виникнення до моменту знищення, з можливістю ідентифікації особистих даних (час виникнення, автор, дата виникнення і т.д.). Як наслідок, постає питання забезпечення достовірності та збереження документованої інформації протягом повного життєвого циклу, незалежно від типу та форми документів.

На сьогодні, питання про необхідність застосування криптографічного перетворення інформації для розробки сучасних засобів захисту інформації є очевидним. У сучасних системах конфіденційність та

інформаційна безпека забезпечуються різними методами: правовими, адміністративними, фізичними, інформаційними (використання паролів, ідентифікаційних номерів абонентів, обмеження користувачів і ін.) і криптографічними методами. При цьому роль криптографічних методів продовжує зростати. Збільшення кількості інформації, що обробляється, передається і зберігається в автоматизованих системах управління підприємств і організацій призвело до підвищення актуальності завдань: забезпечення конфіденційності, цілісності, підтвердження авторства; створення захищеного електронного документообігу; забезпечення високої швидкості обробки і підписання.

Підпис документа є головною ідентифікуючою ознакою у аналоговому середовищі. Проте, у разі перетворення документа, зазначені ознаки не відповідають за автентичність.

Електронний підпис застосовується у електронному середовищі, та є гарантом автентичності цифрового документа [6, 7]. Першою і найбільш відомою у всьому світі конкретною системою ЕЦП стала система RSA, математична схема якої була розроблена в 1977 р. Пізніше винайшли систему El Gamal Signature Algorithm (EGSA) розроблену в 1984 р. американцем арабського походження Тахера Ель Гамалем. У 1991р. в США розробили алгоритм цифрового підпису Digital Signature Algorithm (DSA), який був більш досконалим та мав скорочений обсяг пам'яті і час обчислення підпису. Далі було кілька доповнень та вдосконалень але всі вони, у загальному випадку, базувались на трьох попередниках.

Верифікація, або іншими словами перевірка справжності, на сьогодні є головним пріоритетним напрямком інноваційного характеру у криптографії.

Верифікація є однією з основних функцій, яка найбільшою мірою підлягає автоматизації за допомогою програмних засобів. Забезпечення різних видів верифікації на різних етапах життєвого циклу документа є однією з пріоритетних задач при створенні сучасної дієвої криптографічної системи захисту документів.

На сьогодні, у рамках окремого проекту, розрізняють два типи верифікації:

- автоматизована перевірка справжності – перевірка атрибутів документів, на підставі попередньо налаштованих правил в системі;
- користувальницька перевірка справжності – перевірка здійснюється візуально шляхом перегляду користувачем даних форми.

На даний момент не існує єдиної системи для верифікації, а також не виокремлено єдиного підходу до налаштування перевірки справжності для всіх типів документів окремої системи. За допомогою автоматичної верифікації необхідно забезпечити вирішення низки наступних завдань:

- перевірка справжності даних, переданих в даний екземпляр із зовні за допомогою XML файлу;
- перевірка справжності полів форм при введенні документів вручну користувачем;
- перевірка справжності полів документів, що потрапляють в систему за допомогою сканування паперових носіїв;
- перевірка справжності атрибутів документів в таблицях системи на різних стадіях життєвого циклу документа.

Процедура верифікації – звід необхідних правил перевірки справжності, що виконуються стосовно інформаційного об'єкта в рамках виконання кроку операції, визначеного як верифікація. Склад правил перевірки справжності залежить від групи, типу документа, і його поточного статусу. Єдиним результатом виконання процедури верифікації є підтвердження істинності чи хибності логічного виразу, зазначена процедура може бути застосована до примірника інформаційного об'єкта, що перевіряється.

У свою чергу, правило верифікації – це, перш за все, логічний вираз, що визначає який атрибут інформаційного об'єкта, при виконанні яких умов, яким чином і на які дані, що зберігаються у загальній інформаційній системі, повинен бути перевірений щодо справжності.

Алгоритм здійснення верифікації документів наведено на рис. 1.

Рисунок 1 розкриває, за допомогою багаторівневого затвердження у рамках окремої інформаційної системи, перевірку справжності. Також, важливим фактором є те, що дана функціональність інтегрована із засобами електронного цифрового підпису.

На відміну від автоматизованої перевірки справжності твердження виконується в асинхронному відносно до користувача режимі і, отже, не пред'являє серйозних вимог до продуктивності.

Аналізуючи наведений алгоритм, варто наголосити, що специфіка його функціонування накладає додаткові обмеження:

- необхідність роботи з кастомізованими документами;
- необхідність прив'язки електронного цифрового підпису до документа;
- забезпечення правил налаштування не через клієнт-сервер, а за допомогою трирівневої архітектури;
- необхідність інтеграції із загальним підходом щодо реалізації базових функцій верифікації.

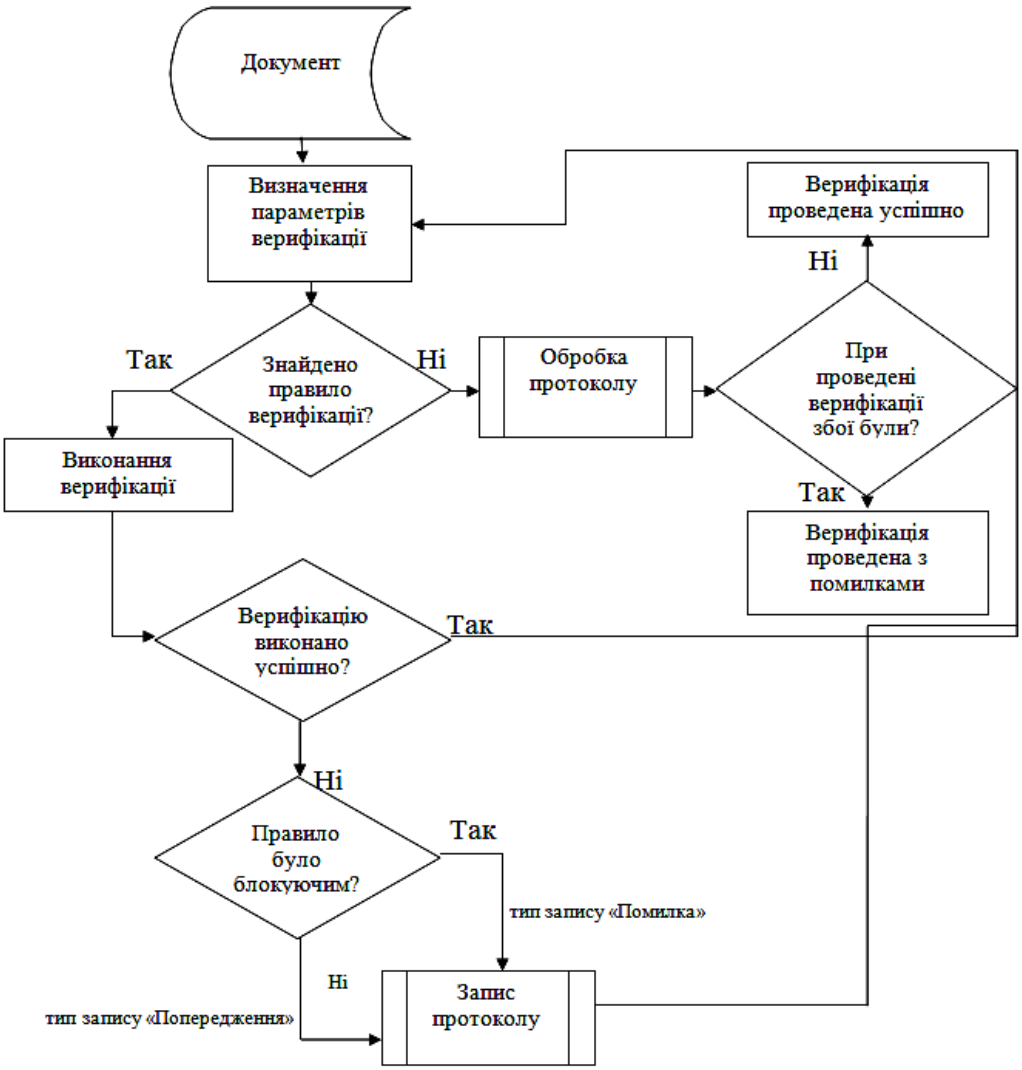

Рис. 1. Алгоритм верифікації документів
Розробка автора на основі [6, 8]

За умови наявності зазначених обмежень пропонується забезпечити ряд розробок, що стосуються:

- врахування відповідного переліку користувачів, що мають безпосереднє відношення до інформаційної системи на підставі попередньо налаштованих правил;
- здійснення прив'язки до засобів електронного цифрового підпису (ЕЦП);
- зміна статусу затвердження документа в залежності від стадії верифікації;
- злиття з операційною моделлю, яка, зокрема, має на увазі автоматичний запуск багаторівневої перевірки справжності після закінчення операції.

Стосовно прив'язки до засобів електронного цифрового підпису, варто враховувати, що даний механізм (формування та перевірки ЕЦП) засновано на асиметричних схемах шифрування, при використанні яких генеруються два математично взаємопов'язані ключі: один з них вважається секретним, інший – відкритим. В основі даного принципу, лежить фундаментальна особливість дієвості, яка полягає у тому, що секретний ключ розкриває відкритий, але не навпаки.

Механізм формування, з математичної точки зору, виглядає наступним чином: повідомлення *P* (блок інформації, файл, таблиця) стискають за допомогою хеш-функції *h ( )* в ціле число *m*:

$$m = h(P) \quad (1)$$

Далі обчислюють цифровий підпис *S* під електронним документом *P*, використовуючи хеш-значення *m* і секретний ключ *D*:

$$S = mD \ (\mathrm{mod}\ N) \quad (2)$$

Наступний крок – відправлення електронного документу P, який є підписний підписом *S*, тобто документ *(P, S)*. У цьому випадку підпис формується власником секретного ключа *D*.

Одержувач відновлює хеш-значення *m'*, застосовуючи криптографічне перетворення підпису *S* з використанням відкритого ключа *E*:

$$m' = S^E \ (\mathrm{mod}\ N). \quad (3)$$

Прирівнюючи вирази (1) та (3), отримуємо:

$$S^E \ (\mathrm{mod}\ N) = h(P), \quad (4)$$

якщо вираз є дійсним, документ є справжнім.

Таким чином, зловмисникові, так як він не володіє закритим ключем автора і не зможе згенерувати коректний підпис, не вдасться непомітно внести зміни у вихідну інформацію. Проте, кожен зловмисник має можливість замінити всі три складові: зашифрувати змінену інформацію власним закритим ключем і прикласти свій відкритий ключ. Попередити та зупинити описаний випадок буде можливим у випадку застосування схеми взаємодії із залученням третього суб'єкта. У якості якого, у більшості випадків, виступає певного роду структура, яка отримує місію забезпечення взаємної довіри між учасниками обміну електронними повідомленнями, підписаними електронним цифровим підписом. Основним документом, що підтверджує наявність криптографічного захисту документа є цифровий документ, який підтверджує відповідність між відкритим ключем і інформацією, що ідентифікує власника ключа. Зазначений документ має назву сертифікат відкритого ключа [3].

Сертифікат відкритого ключа розкриває:

- область дії відкритого ключа;
- загальні відомості про відкритий ключ;
- основні дані про власника відкритого ключа;
- призначення відкритого ключа;
- відомості про структуру відкритого ключа;
- термін дії сертифікату відкритого ключа.

Підсумовуючи вищезазначене можемо стверджувати, що сертифікат відкритого ключа виступає своєрідним гарантом захищеності в сучасному інформаційному середовищі.

Заміна, перетворення або форматування початкового документу автоматично робить електронно-цифровий підпис не дійсним, так як останній є послідовністю символів, що засвідчує справжність документів, отриманий внаслідок перетворення початкового документа. Базуючись на тому, що для підробки електронного цифрового підпису необхідно проведення великого обсягу математичних обчислень, підробка ЕЦП є майже неможливою.

У разі, якщо ЕЦП виробляється на основі самого тексту документа, є можливість встановити факт підміни або редагування документа при передачі. Це говорить про те, що електронний підпис за своєю структурою, є послідовністю символів, пов'язаних з текстом документа так, що при зміні документа порушується задана відповідність між електронним підписом і текстом. Таким чином, для отримання електронного підпису під документом потрібно провести деяке перетворення тексту документа.

Для вирішення різних криптографічних завдань, на сьогодні, існує безліч криптографічних алгоритмів, які є сукупністю операцій, що здійснюються над текстом під час криптографічного перетворення.

Алгоритм отримання зашифрованого тексту полягає у тому, що вихідний текст обов’язково перетворюється так, щоб відновлення вихідного тексту було практично неможливим без знання певної інформації. Одиниці, що володіють цією інформацією, повинні бути в змозі відновити вихідний текст. Очевидно, що інформація, необхідна для відновлення тексту (розшифрування), повинна бути відома тільки адресатам.

На практиці, виникає необхідність здійснити верифікацію документа за допомогою іншого документа, який так само вимагає верифікації. Це можливо, наприклад, коли підпис під документом перевіряється за допомогою сертифіката на відкритий ключ, парний тому секретному ключу, на якому підпис вироблено [5]. Проте, з вищезазначеного випливає, що сам сертифікат – це теж документ, коректність і достовірність якого вимагає перевірки. Підпис під сертифікатом перевіряється на сертифікаті на відкритий ключ підпису того центру, який випустив сертифікат. Сертифікат центру, в свою чергу, теж може бути підписаний електронним підписом і вимагати перевірки.

Кількість таких документів необмежена, вони створюють так звані ланцюги довіри, що говорить про те, що кожен наступний документ перевіряє попередній. Не виникає сумнівів, що в кінці кінців ланцюжок довіри закінчується – в ньому обов'язково існує документ, який неможливо перевірити на іншому документі (як варіант, найперший сертифікат центру). Називаються зазначені документи кореневими, довіреними і т.д. Верифікація останніх залежить від програмного забезпечення, що використовується, і прийнятого регламенту: контрольні записи, цифрові відбитки і т.д. Головною особливістю всіх цих способів верифікації є те, що всі вони є користувальницькими мають на меті застосування паперових документів, тобто не підлягають автоматизації: необхідно, щоб людина порівняла інформацію з електронним документом, що проходить стадію верифікації, з роздрукованим і переконалася у справжності документа. Також вагомим фактором є те, що справжнім документ вважається тільки в тому випадку, якщо всі документи ланцюга довіри справжні та пройшли верифікацію у повному обсязі. З викладено видно, що це складний та довготривалий процес, тому повністю очевидно, що при кожній перевірці підпису, увесь ланцюжок довіри не перевіряється безпосередньо людиною, а у більшості випадків кореневий документ проходить верифікацію при його встановленні на комп’ютер, а далі верифікація ланцюжків довіри, що закінчуються цим документом, відбувається автоматично.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Здійснено розробку алгоритму верифікації документів, побудованого на складності завдання факторизації, і його застосування в системах захисту документів від підробки. Складено блок-схему процесу верифікації документів. Доведена необхідність застосування криптографічного перетворення інформації для розробки

сучасних засобів захисту інформації. Наголошено, що верифікація, або іншими словами перевірка справжності на сьогодні є головним пріоритетним напрямком інноваційного характеру у криптографії. Визначено детально процедуру верифікації, яка описується як звід необхідних правил перевірки справжності операції, що виконується стосовно інформаційного об'єкту в рамках виконання кроку, визначеного як верифікація. Склад правил перевірки справжності, що виконуються, залежить від групи, типу документа, і його поточного статусу. Зазначається, що єдиним результатом виконання процедури верифікації є підтвердження істинності чи хибності логічного виразу. Виокремлено, що зазначена процедура може бути застосована до примірника інформаційного об'єкта, який саме перевіряється.

У подальшому, актуальним напрямком дослідження є автоматизація алгоритму верифікації для різних типів документів з подальшим впровадженням на реальному підприємстві у вигляді додаткового програмного забезпечення.

Література

1. Бабаш А.В. Криптография / А.В. Бабаш, Г.П. Шанкин ; под ред. В.П. Шестюка, Э.А. Применко. – М. : СОЛОН-ПРЕСС, 2007. – 512 с.

2. Бабак В.П. Теоретичні основи захисту інформації : підручник / В. П. Бабак. – Книжкове видавництво НАУ, 2008. – 752 с.

3. Бевз О.М. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню : монографія / О.М. Бевз, Р.Н. Квєтний – Вінниця : ВНТУ, 2010. – 96 с.

4. Панасенко С.П. Алгоритмы шифрования : специальный справочник / С.П. Панасенко. – СПб : БХВ-Петербург, 2009. – 576 с.

5. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е.Серов. – 3-е изд. – М. : Диалог-МИФИ, 2011. – 176 с.

6. Рябко Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. – 2-е изд. – М. : Горячая линия – Телеком, 2013. – 229 с.

7. Малюк А. А. Защита информации: современные проблемы / А. А. Малюк // Безопасность информационных технологий. – 2010. – № 1. – С. 5–9.

8. Шолохова М. А. Процедурный уровень информационной безопасности / М. А. Шолохова // Информационная безопасность. – 2010. – С. 98–99.

9. Смирнов Г. Особенности обеспечения информационной безопасности малого и среднего бизнеса / Г. Смирнов // Small Business Securuty. – 2013. – С. 67–78.

10. Круглов А. А. Об информационной безопасности / А. А. Круглов, Б. И. Скородумов // Вестник Российского нового университета. – 2007. – № 2. – С. 77–78.

11. Ажмухамедов И. М. Принципы обеспечения комплексной безопасности информационных систем / И. М. Ажмухамедов // Вестник АГТУ. Серия: «Управление, вычислительная техника и информатика». – 2011. – № 1. – С. 7–11.

12. Шакалей М.Б. Схема RSAна основе простого числа / М.Б. Шакалей // 52-я Научно-техническая конференция аспирантов, магистрантов и студентов БГУИР : тезисы докладов. – Минск, 2016 – С. 24–25.

Рецензія/Peer review : 21.9.2016 р. Надрукована/Printed : 30.10.2016 р.
Рецензент: д.т.н., проф.. Троцишин І.В.