DOI: 10.18372/2225-5036.30.18615

СИСТЕМАТИЗАЦІЯ ОЗНАК НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ

Олена Криворучко, Юлія Костюк, Альона Десятко

Державний торговельно-економічний університет, Україна

КРИВОРУЧКО Олена Володимирівна, д.т.н., професор
Рік та місце народження: 1969 р., м. Київ, Україна.
Освіта: Київський національний торговельно-економічний університет.
Посада: професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки.
Наукові інтереси: управління проектами і програмами, інформаційні технології, інформаційні системи, хмарні технології, стандартизація, інформаційний простір ЗВО.
Публікації: більше 70 наукових публікацій, серед яких монографії, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: kryvoruchko_ev@knute.edu.ua.
Orcid ID: 0000-0002-7661-9227.

КОСТЮК Юлія Володимирівна, PhD
Рік та місце народження: 1980 р., м. Київ, Україна.
Освіта: Державний торговельно-економічний університет.
Посада: старший викладач кафедри інженерії програмного забезпечення та кібербезпеки.
Наукові інтереси: комп'ютерні мережі, інформаційно-інтелектуальні системи, хмарні технології, кібербезпека.
Публікації: більше 30 наукових публікацій, серед яких наукові статті та тези, матеріали доповідей на конференціях.
E-mail: kostyuk_yu@knute.edu.ua.
Orcid ID: 0000-0001-5423-0985.

ДЕСЯТКО Альона Миколаївна, PhD, доцент
Рік та місце народження: 1976 р., м. Ржищів, Київська область, Україна.
Освіта: Київський національний торговельно-економічний університет.
Посада: доцент кафедри інженерії програмного забезпечення та кібербезпеки.
Наукові інтереси: хмарні технології, інформаційні системи, кібербезпека, Product IT, Project IT, архітектура ПЗ.
Публікації: більше 60 наукових публікацій, серед яких монографії, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: desyatko@knute.edu.ua.
Orcid ID: 0000-0002-2284-3418.

Анотація. *Останнім часом виявлено збільшення інцидентів несанкціонованого доступу до корпоративної інформації. У статті розглядається підхід, спрямований на вирішення питання щодо розробки методу, основною метою якого є запропонована схема захисту корпоративної інформації від будь-якого несанкціонованого доступу, використовуючи криптографічний алгоритм. Надійність алгоритму досягається за рахунок поєднання криптографічного алгоритму із секретним ключем. Реалізація двійкового шаблону як секретного ключа, який інтегрується в процес генерації хеш-значення, за допомогою алгоритму хешування MD5, відзначається відносно високим ступенем стійкості та надійності. Подальше порівняння отриманого хеш-значення зі збереженим відбувається з метою ефективного управління доступом до корпоративної інформації. Застосування прихованого ключа в алгоритмі хешування полягає у тому, що дані використовуються як додатковий вхід для односторонньої функції, яка хешує пароль. Таким чином, метод обраної криптографічної схеми демонструє ефективність в забезпеченні конфіденційності, цілісності та доступності корпоративної інформації.*

Ключові слова: *несанкціонований доступ, криптографічні методи захисту, алгоритм хешування, хеш-значення, прихований ключ, стійкість.*

Постановка проблеми

У сучасному цифровому світі, де корпоративна інформація є важливим ресурсом для успішної діяльності підприємств, проблема несанкціонованого доступу до цієї інформації стає все більш актуальною. Найпоширенішими методами для забезпечення конфіденційності даних, що циркулюють у різних інформаційних системах, є методи шифрування інформації. До цих методів, незалежно від технологічного виконання, пред'являються високі вимоги, які зумовлені стрімким розвитком радіотехнічних засобів, зокрема обчислювальних. Посилення вимог до стійкості зумовлено різнобічним використанням криптографії та більш широкими можливостями для атак, враховуючи конкретні умови функціонування шифру [1-3].

Основним видом алгоритмів спеціальної обробки даних для захисту корпоративної інформації від загроз порушення конфіденційності та цілісності оброблюваної в них інформації є криптографічні алгоритми, серед яких величезне значення мають симетричні криптографічні алгоритми, такі як алгоритми потокового шифрування, алгоритми блокового шифрування, криптографічні хеш-функції тощо [1-2, 4-7, 12-19]. Нині відома досить велика кількість таких алгоритмів. Серед них є як універсальні, так і орієнтовані або на програмну, або на апаратну реалізацію. Такі алгоритми розробляли багато вчених, серед яких Д. Бернштайн, Й. Даймен, Л. Кнудсен, Р. Меркль, Дж. Мессі, Б. Пренель, Р. Рівест, В. Реймен, Н. Фергюсон, Х. Фейстель, Б. Шнайєр та ін [1-6, 8, 10-11, 15-18]. Таким чином, незважаючи на існування досить великої кількості симетричних криптографічних алгоритмів, розробка нових криптоалгоритмів, спрямованих на досягнення високої продуктивності як при апаратній реалізації, так і для низько-ресурсних апаратних реалізацій, залишається актуальною на сьогоднішній день [2, 7-11, 14-17, 19].

Підвищені вимоги до шифрування пов'язані з необхідністю забезпечення високої продуктивності інформаційних систем після вбудовування в них механізмів захисту [16-17]. У той же час, відзначено, що найбільш поширеними технічними аспектами атак є зовнішні впливи на пристрій шифрування з метою викликати випадкові апаратні збої, вимірювання споживаної потужності та визначення часу обчислень [2-5, 8, 9, 11-13].

Отже, інформаційна безпека вимагає постійного вдосконалення методів шифрування та усунення потенційних вразливостей, забезпечуючи при цьому ефективний захист конфіденційності даних в умовах стрімкого технологічного розвитку.

Захист конфіденційних даних від кіберзагроз вимагає вдосконалених стратегій та технологічних рішень [1, 3, 8-11, 14-16]. Серед різноманітних заходів захисту інформаційних ресурсів, важливе місце займають криптографічні методи, які використовуються для запобігання несанкціонованому доступу до корпоративної інформації. Сучасні загрози кібербезпеки можуть включати в себе високотехнологічні атаки, такі як використання вразливостей безпеки, методи соціальної інженерії або використання шкідливого програмного забезпечення для здобуття несанкціонованого доступу до системи.

Однією з ключових складових вирішення проблеми є систематизація ознак несанкціонованого доступу. Застосування криптографічних методів захисту дозволяє створити ефективну систему, що забезпечує конфіденційність, цілісність та доступність корпоративної інформації. Систематизація ознак несанкціонованого доступу включає в себе аналіз різноманітних векторів атак, таких як перехоплення даних, несанкціоноване копіювання, модифікація і видалення інформації. Розуміння цих ознак є важливим кроком у створенні ефективної системи захисту [2-9, 13-15]. Використання криптографічних методів захисту не повинно лише гарантувати конфіденційність і цілісність, але й необхідно забезпечувати доступність інформації для авторизованих користувачів. Вирішення цієї проблеми включає в себе розробку ефективних ключів, управління доступом і стійких криптографічних алгоритмів.

Захист інформаційних ресурсів від таких загроз базується на використанні різноманітних криптографічних алгоритмів та методів шифрування. Ключовою метою є забезпечення конфіденційності, цілісності та доступності корпоративної інформації. Застосування криптографічних методів захисту дозволяє відвернути атаки та зберегти конфіденційні дані від несанкціонованого доступу. Але важливо вдосконалювати та модернізувати криптографічні засоби для ефективного протистояння зростаючим загрозам [3-7, 9, 10]. Розробка та застосування нових криптографічних алгоритмів стає необхідністю для забезпечення високого рівня захисту корпоративної інформації в умовах сучасного кіберсередовища.

Аналіз останніх досліджень і публікацій

Традиційні методи забезпечення цілісності інформації стають неефективними у випадку спрямованих інформаційних атак. На сьогоднішній день проблема забезпечення стійкого контролю цілісності інформації залишається невирішеною і вимагає розробки нового методу. Оригінальна сигнатура виявлення несанкціонованого доступу до корпоративної інформації об'єднує в собі хеш-функцію з відповідним підписом, ґрунтуючись на хеш-функції та контекстній інформації [1, 3, 4-8, 17-19]. Оригінальна сигнатура для виявлення несанкціонованого доступу до корпоративної інформації представляє собою високотехнологічний метод, який об'єднує в собі хеш-функцію разом із відповідним підписом, покладаючись на ефективність хеш-функцій та контекстну інформацію. Цей метод визначення несанкціонованого доступу призначений для створення ефективної системи, яка забезпечує конфіденційність, цілісність та доступність корпоративних даних.

Хеш-функція, використовуючи складний алгоритм, перетворює корпоративну інформацію у вигляд унікального «відбитка», який є неможливим або

практично неможливим відтворити [1-5, 11, 18-19]. Цей відбиток слугує унікальним ідентифікатором для кожного блоку даних, гарантуючи їхню унікальність та відсутність змін у випадку навіть мінімального втручання. Відповідний підпис, створений на основі цього відбитка, фактично є електронним підтвердженням автентичності та недоторканності інформації. Контекстна інформація, врахована при формуванні сигнатури, включає в себе різноманітні параметри, такі як час, місце зберігання, та структуру даних. Це дозволяє системі бути більш адаптивною до змін в умовах оточення та в робочих процесах, забезпечуючи надійність і стійкість [6, 8-12, 19].

Поєднання цих компонентів створює адаптивний фільтр сигналізації, який виявляє потенційні атаки на основі ретельного аналізу хеш-функцій та контекстуальних умов. Цей фільтр реагує на невизначеність та забезпечує вчасне виявлення будь-яких спроб несанкціонованого доступу до важливих корпоративних даних, забезпечуючи високий рівень безпеки [13-15].

Оригінальна сигнатура визначення несанкціонованого доступу виготовляє систему, що оптимізована для забезпечення найвищого рівня безпеки. Вона не лише захищає інформацію від небажаних втручань, але й гарантує конфіденційність та невразливість важливих корпоративних даних, що є надзвичайно важливим у сучасному цифровому середовищі.

Систематизація ознак несанкціонованого доступу та використання криптографічних методів захисту є необхідною умовою для підтримки кібербезпеки корпоративної інформації [16]. Нинішній рівень розвитку технологій вимагає постійного вдосконалення методів та стратегій для ефективного захисту конфіденційної інформації від небажаних кіберзагроз.

Мета та постановка завдання

Мета роботи полягає в систематизації ознак несанкціонованого доступу до корпоративної інформації на основі застосування криптографічних методів захисту. Однією з ключових задач є розробка та впровадження ефективних стратегій забезпечення конфіденційності, цілісності та доступності корпоративної інформації. Дослідження спрямоване на розробку криптографічних рішень, спроможних відвертати загрози. В рамках дослідження приділено особливу увагу криптографічним аспектам, таким як механізми автентифікації, застосування хеш-функцій, та вивчення різноманітних криптографічних алгоритмів. Дослідження покликане визначити ефективні стратегії використання цих методів для запобігання несанкціонованому доступу та забезпечення високого рівня конфіденційності та цілісності корпоративної інформації. Розглянемо процес автентифікації, роль хеш-функцій у забезпеченні цілісності даних, а також аналізуємо криптографічні алгоритми для їх впровадження в системи захисту. Таким чином, дослідження спрямоване на розробку ефективної системи, яка забезпечить відповідний рівень захисту корпоративних даних від несанкціонованого доступу. Застосування криптографічних методів у роботі спрямоване на створення надійних механізмів, що гарантують конфіденційність, цілісність та доступність корпоративної інформації, у той час забезпечуючи ефективність в процесі обробки даних.

Виклад основного матеріалу дослідження

Багаторівнева аутентифікація − це метод, при якому користувач повинен пройти кілька різних рівнів ідентифікації, щоб отримати доступ до системи чи ресурсів. Цей підхід спрямований на забезпечення вищого рівня безпеки, ускладнюючи процес несанкціонованого доступу через послідовність етапів перевірки, але і дозволяє адаптуватися до різних сценаріїв та загроз, зменшуючи ризик несанкціонованого доступу, особливо в умовах ростучих кіберзагроз [11, 14, 16-18]. У випадку виявлення аномальної активності чи спроб несанкціонованого доступу, система може вжити відповідних заходів безпеки на різних рівнях. На першому рівні багаторівневої аутентифікації використовуються основні методи ідентифікації, такі як паролі чи пін-коди.

Однак, з огляду на ризики, пов'язані із використанням традиційних засобів, важливо впроваджувати криптографічні алгоритми для надійного захисту цих ідентифікаційних даних від несанкціонованого доступу. Другий рівень включає в себе біометричну аутентифікацію, яка базується на унікальних фізіологічних чи поведінкових рисах особи, таких як відбиток пальця, розпізнавання обличчя чи голосу. Використання криптографічних методів на цьому рівні дозволяє захистити біометричні дані від можливого витоку та забезпечити їх конфіденційність. На третьому рівні використовується електронний ключ або смарт-карта, які також піддаваються криптографічному захисту. Ці засоби аутентифікації забезпечують додатковий шар безпеки та ускладнюють завдання потенційного зловмисника [1, 7, 19].

Застосування багаторівневої аутентифікації, що базується на криптографічних методах захисту, дозволяє структурувати та аналізувати ознаки несанкціонованого доступу. Цей підхід зробить систему більш адаптивною до змінних загроз, забезпечуючи високий рівень захисту корпоративної інформації. Криптографічні методи використовуються для створення стійких цифрових підписів та генерації хеш-значень, що сприяє конфіденційності та цілісності даних [5-8, 10-12].

Такий підхід дозволяє системі ефективно протистояти різноманітним загрозам, що можуть виникнути в корпоративному середовищі. Розглянута система базується саме на комплексній багаторівневій аутентифікації, використовуючи криптографічні методи захисту, що дозволяє не лише ідентифікувати користувача, але й забезпечити стійкий захист корпоративної інформації.

Процес відбувається таким чином [1-5, 9]. Спочатку, в системі використовується двійковий шаблон, який інтерпретується як секретний ключ (SALT). Цей

ключ служить основою для генерації стійких хеш-функцій, використовуючи, наприклад, алгоритм MD5. Паралельно враховується чотиризначний пін-код, що є додатковим параметром для алгоритму хешування MD5. Після введення пін-коду і генерації хеш-значення відбувається порівняння отриманого хешу зі значенням, що вже зберігається в пам'яті віддаленого пристрою [1-3, 7-11, 13, 15]. У випадку збігу значень, система надає доступ, підтверджуючи ідентичність ініціатора. Загроза можливості розкриття кодів або сигналів полягає в можливості визначення параметрів, використовуючи зовнішній вплив на пристрій шифрування. Це може включати в себе атаки на апаратні збої, вимірювання споживаної потужності, а також визначення часу обчислень.

Ці атаки спрямовані на отримання інформації про ключ та параметри шифрування. Враховуючи ці загрози, система використовує адаптивні фільтри сигналізації для виявлення невизначеностей та можливих атак, що забезпечує надійний захист корпоративної інформації. Показано схематичне представлення процесу (рис. 1, 2).

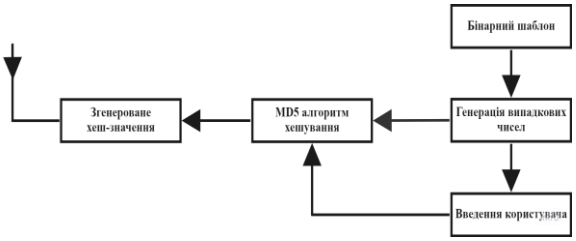

Рис. 1. Схематичне зображення блоку передачі інформації

При реалізації системи використовується важливий елемент безпеки − двійковий шаблон, який функціонує як секретний ключ, відомий також як SALT. Цей двійковий шаблон представляє собою набір двійкових даних, що інтерпретуються як унікальний секретний ключ [2, 14, 16]. Використання двійкового шаблону додає важливий елемент випадковості та унікальності до процесу генерації хеш-значення, покращуючи стійкість системи до атак.

Одним із параметрів, які враховуються в алгоритмі, є чотиризначний пін-код. Цей пін-код виступає як додатковий елемент для аутентифікації та стає ще однією складовою для формування унікального хеш-значення. При введенні користувачем чотиризначного пін-коду система обробляє його за допомогою алгоритму хешування MD5 разом із двійковим шаблоном, щоб сформувати надійне та унікальне хеш-значення. Основним етапом в процесі захисту інформації є застосування алгоритму хешування MD5, який використовується для обчислення хеш-значення з комбінації двійкового шаблону та чотиризначного пін-коду. Цей хеш виступає унікальним відображенням вхідних даних і служить як цифровий відбиток під час аутентифікації [4, 7-10, 19]. Після успішної генерації хеш-значення воно відправляється на віддалений пристрій для подальшої перевірки. Віддалений пристрій, який може бути частиною автоматизованої системи або сервером, здійснює порівняння отриманого хеш-значення зі збереженим оригінальним хешем. Якщо вони збігаються, система визнає правильність введених даних та ініціює необхідні дії, такі як активація доступу чи аутентифікація користувача. В іншому випадку система може сповістити власника або відмовити в доступі, інформуючи про можливий несанкціонований доступ.

Згенероване хеш-значення порівнюється зі значенням, яке вже зберігається в пам'яті віддаленого пристрою. У випадку виявлення співпадіння значень, пристрій дозволяє доступ, підтверджуючи ідентичність ініціатора. Така система базується на криптографічних методах захисту, надає адаптивний фільтр сигналізації, що реагує на невизначеності та можливі атаки, забезпечуючи надійне виявлення спроб несанкціонованого доступу до важливої корпоративної інформації [3, 5-7, 11, 18-19]. Криптографічні алгоритми гарантують надійність та унікальність генерованих хеш-значень, адаптивний фільтр сигналізації забезпечує реагування на будь-які спроби несанкціонованого доступу. Така система контролю доступу взаємодіє із засобами криптографічного захисту, надаючи надійний механізм виявлення можливих загроз і забезпечуючи безпеку важливої корпоративної інформації. Криптографічні методи, такі як алгоритм MD5, використовуються для генерації стійких хеш-значень, що служать цифровими підписами. Адаптивні фільтри реагують на невизначеності та аномалії в оточенні, що дозволяє системі адаптуватися до нових умов та ефективно виявляти можливі атаки. Ця комбінація забезпечує надійний та адаптивний захист важливої корпоративної інформації, забезпечуючи конфіденційність, цілісність та автентифікацію даних [2, 8-13, 16-17].

Рис. 2. Схематичне зображення блоку приймання інформації

Методологія складається з двох модулів: модуль передавача та модуль приймача. Ці модулі відіграють важливу роль у систематизації ознак несанкціонованого доступу до корпоративної інформації, базуючись на використанні криптографічних методів захисту. Перший модуль відповідає за обробку вхідних даних, включаючи формування секретного ключа (SALT) через двійковий шаблон, приймання чотиризначного пін-коду та застосування алгоритму хешування MD5 для генерації хеш-значення. Отримане хеш-значення відправляється на віддалений пристрій для порівняння. Другий модуль отримує передане хеш-значення та виконує процес порівняння зі збереженим значенням в системі. Це ключовий етап, де

здійснюється ефективна перевірка цілісності і автентичності інформації. Залежно від результату порівняння, модуль приймача вирішує, чи дозволити доступ до системи, підтверджуючи ідентичність ініціатора, чи відмовити у доступі в разі виявлення неспівпадіння значень [8, 11, 15-19]. Цей процес є ключовим етапом в системі захисту, оскільки дозволяє ефективно перевірити цілісність і автентичність інформації під час передачі та прийому даних. Систематизація ознак несанкціонованого доступу до корпоративної інформації в даному випадку базується на залученні криптографічних методів захисту, які забезпечують високий рівень безпеки під час обробки та передачі конфіденційних даних. Отже, взаємодія обох модулів в системі створює надійний механізм, спрямований на запобігання несанкціонованому доступу та забезпечення цілісності корпоративної інформації [5, 8, 10-13, 15-18].

На етапі процесу формування ключа отримується двійковий шаблон, який використовується для генерації ключа. Цей шаблон зберігається в відведеній для цього області пам'яті. Сам шаблон представляє собою двійкові дані, що відображають значення кожної точки. Далі наведемо детальний опис алгоритму генерації ключа за допомогою випадкових чисел. Цей алгоритм ґрунтується на двійкових шаблонах, де ключ має довжину 128 біт. Після отримання двійкових шаблонів, які зберігаються в пам'яті, значення може бути використане як секретний ключ або SALT для процесу хешування. Секретний ключ формується на основі обох токенів і двійкового шаблону. Токен використовується для отримання випадкових значень з двійкових шаблонів. Двійковий ключ "k" спочатку генерується як послідовність випадкових бітів, після чого проводиться логічна операція з введеними користувачем даними [1, 3-7, 9-16, 17-19]. Отриманий результат перетворюється у шістнадцяткове значення і подається на вхід алгоритму хешування MD5, щоб отримати хеш-значення. Кожне нове введення користувача призводить до генерації іншого унікального хеш-значення для тих самих чи інших вхідних даних.

Таким чином, важко визначити, якому входу відповідає конкретний хеш. Наприклад, якщо двійковий шаблон складається з матриць і позначається як T, то цей підхід забезпечує додатковий рівень безпеки та систематизації ознак несанкціонованого доступу:

$$T = \begin{bmatrix} x1_1 & x1_2 & x1_3 & \cdots & x1_n \\ x2_1 & x2_2 & x2_3 & \cdots & x2_n \\ x3_1 & x2_2 & x3_3 & \cdots & x3_n \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ xm_1 & xm_2 & xm_3 & \cdots & xm_n \end{bmatrix}, \quad (1)$$

де m – кількість рядків у шаблоні, n – кількість стовпців у шаблоні.

Нехай "a" – випадково вибраний рядок, а X_n – випадково згенерований стовпець з рівняння:

$$X_n + 1 = (aX_n + b)\ mod\ m, \quad (2)$$

де a, b – цілі числа, а $m = m + n + 1$.

За допомогою математичного рівняння, випадковим чином вибираються рядок та стовпець шаблонної матриці. Далі, обраний рядок матриці поступово збільшується до тих пір, поки не буде отримано чотири значення. Таким чином, ми формуємо матрицю розміром [1x4], яка виступатиме однією з вхідних даних для створення приватного ключа. Цю операцію повторюють тричі, отримуючи три інші матриці розміром [1x4]. У результаті отримуємо чотири матриці [1x4], які об'єднуються для утворення однієї великої матриці [4x4]. Ця велика матриця є випадково згенерованою вхідною матрицею для створення секретного ключа і позначається як $R(T)$:

$$R(T) = \begin{bmatrix} x2_1 & x1_3 & x5_4 & x2_2 \\ x3_1 & x2_3 & x1_4 & x3_2 \\ x4_1 & x3_3 & x2_4 & x4_2 \\ x5_1 & x4_3 & x3_4 & x5_2 \end{bmatrix}, \quad (3)$$

де $a[0]$ – перший стовпець $R(T)$; $a[1]$ – другий стовпець $R(T)$; $a[2]$ – третій стовпець $R(T)$; $a[3]$– четвертий стовпець $R(T)$.

Розглядаючи значення в кожному стовпчику як двійкові значення, перетворимо потім їх у десяткові:

$$a[0] = \begin{bmatrix} (x_2 1 \cdot 1000) + (x_3 1 \cdot 100) + \\ (x_4 1 \cdot 10) + (x_5 1 \cdot 1) \end{bmatrix}. \quad (4)$$

Перетворимо $a[0]$ у шістнадцяткове значення, а потім зробимо те саме для $a[1]$, $a[2]$, $a[3]$:

$$D[R(T)] = a[3] \cdot 16^3 + a[2] \cdot 16^2 + a[1] \cdot 16^1 + a[0] \cdot 16^0, \quad (5)$$

$$H(K) = I \oplus D[R(T)], \quad (6)$$

де $H(K)$ – хеш-ключ; I – вихідні дані користувача; $R(T)$ – випадково згенерований секретний ключ.

$$H(K1) = Hex\ \{H(K)\}, \quad (7)$$

$H(K1)$ – шістнадцяткове значення $H(K)$.

Потім алгоритм хешування обчислює хеш-значення на основі хеш-ключа:

$$Hash \Longrightarrow MD5hash\ \{H(K1)\}. \quad (8)$$

Хеш-функція, що використовується для забезпечення надійності збереженої інформації, є важливим елементом систематизації заходів захисту корпоративної інформації від несанкціонованого доступу. Давайте розглянемо цей аспект більш детально [2-7, 10-13, 16-18]. Хеш-функція, іноді відома як «дайджест повідомлення», генерує фіксований розмір дайджесту для будь-яких вхідних даних, а також дозволяє перевірити цілісність та автентичність інформації. Отримана математична формула $MD5 = f(x)$ визначає процес отримання хеш-значення MD5 для конкретного вхідного повідомлення. Хоча функція хешування є односторонньою – легко отримати хеш з вхідного повідомлення, обернений процес важко виконується. Це означає, що на практиці неможливо відновити оригінальне повідомлення, використовуючи

тільки його хеш MD5. Важливою властивістю хеш-функції є унікальність дайджестів для різних вхідних даних, оскільки забезпечує високий рівень безпеки і запобігає несанкціонованим особам визначити, якщо два повідомлення мають однаковий дайджест [1-6, 11, 13, 19].

Застосування криптографічних методів захисту на базі хеш-функцій стає ключовим елементом стратегії забезпечення конфіденційності і цілісності корпоративної інформації. Вони дозволяють ефективно систематизувати й категоризувати ознаки потенційних атак та неупереджених доступів до важливих даних. При цьому $f(x1) \neq f(x2)$.

Хеш-функція повинна задовольняти всім вимогам криптографічної стійкості. Оскільки, хеш-функція − це одностороння функція $h = H(M)$, яка перетворює бітову послідовність M довільної довжини в послідовність h фіксованої довжини, то обчислюється ітеративним чином. У загальному випадку, формулу хеш-функції (раундового перетворення хеш-функції) можна представити в такому вигляді:

$$H_i = F(H_{i-1}, M_i), i = 1,2, \dots, n, \quad (9)$$

де F – блокова функція, що стискає, M_i – значення i-го блоку даних хешованого повідомлення $M = \{M_1, M_2, \dots, M_n\}$, H_{i-1} – значення хеш-функції, визначене на попередньому раунді, H_0 – визначене в специфікації початкове значення. Підсумковим значенням хеш-функції від повідомлення M є значення H_n.

Стійкі хеш-функції повинні відповідати таким вимогам: в разі відомого вихідного значення хеш-функції слід ускладнити обчислення вхідного значення хеш-функції, що визначається як властивість важко зворотності хеш-функції; а також забезпечувати неможливе знаходження двох повідомлень $M^{/}$ і $M^{//} \neq M^{/}$, для яких ймовірності виконання умови $H(M^{/}) = H(M^{//})$ є істотними, що визначається як властивість колізійної стійкості хеш-функції.

Підхід до побудови хеш-функцій із потаємним ходом передбачає можливість обходу вимоги колізійної стійкості для володаря ключа до потаємного ходу, зберігаючи при цьому властивість важко зворотності. Ключ до потаємного ходу складається з закритих параметрів хеш-функції, які не розголошуються публічно. Ці параметри не використовуються у відкритому вигляді, що унеможливлює базове обчислення хеш-функції без знання цих параметрів.

Процес формування колізії хеш-функції для конкретного повідомлення включає вибір закритих параметрів, відомих лише власнику ключа. На їхній основі створюються відкриті параметри, що входять у специфікацію хеш-функції. Власник ключа модифікує вихідне повідомлення, а потім, використовуючи закриті параметри, генерує спеціальний коригувальний блок даних, який вставляється в модифіковане повідомлення [5, 10-13, 15, 17-19]. Таким чином, модифіковане повідомлення із коригувальним блоком матиме те саме значення хеш-функції, що і вихідне повідомлення.

Нехай є документ M, розбитий на блоки $\{M_1, M_2, \dots, M_n\}$. Результати обчислення значення хеш-функцій після проходження кожного блоку позначимо як $\{H_1, H_2, \dots, H_n\}$. Значення хеш-функції для i-го блоку обчислюється за формулою:

$$H_i = h(M_i, H_{i-1}), \quad (10)$$

де $1 \leq i \leq n$, h – раундова хеш-функція.

Необхідно сформувати змінений документ $M^{/}$, розбитий на блоки $\{M_1^{/}, M_2^{/}, \dots, M_n^{/}\}$ і зі значеннями хеш-функції після проходження кожного блоку $\{H_1^{/}, H_2^{/}, \dots, H_n^{/}\}$, так, щоб вихідні значення хеш-функцій були рівні ($H_n = H_n^{/}$). Наведена схема обчислення значення хеш-функції від вихідного і модифікованого документів (рис. 3).

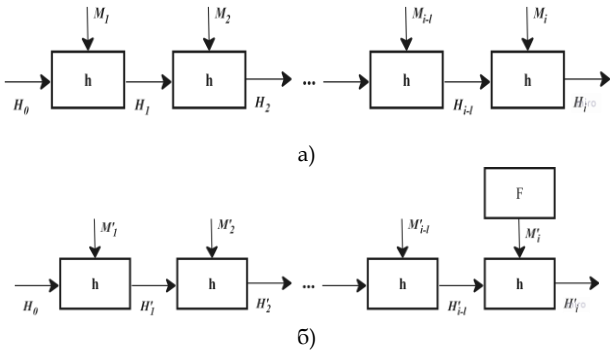

Рис. 3. Обчислення значення хеш-функції від а) вихідного та б) модифікованого документів (h – раундова хеш-функція; F – функція формування коригувального блоку)

Початкове значення H_0 є специфікованим значенням і не змінюється. Вставка коригувального блоку $M_i^{/}$ забезпечує рівність $H_i = H_i^{/}$. Коригувальний блок $M_i^{/}$ може бути вставлений у будь-яке місце модифікованого повідомлення, що модифікується, однак для того, щоб підсумкові значення хеш-функцій дорівнювали ($H_n = H_n^{/}$), необхідно, щоб усі наступні блоки вихідного і модифікованого повідомлень були однакові ($\{M_{i+1}, \dots, M_{n-1}, M_n\} = M_{i+1}^{/}, \dots, M_{n-1}^{/}, M_n^{/}\}$). У зв'язку з цим, зручно використовувати як коригувальний блок останній блок. Той, хто не володіє ключем до потайного ходу, може обчислити значення хеш-функції H_n і $H_n^{/}$, але не може сформувати коригувальний блок.

Стійкість хеш-функції та потайного ходу може бути заснована на математичних задачах, таких як задача дискретного логарифмування і задача факторизації чисел спеціального виду. Використовуючи задачу дискретного логарифмування, раундове обчислення хеш-функції з потайним ходом можна представити у вигляді формули:

$$H_i = \alpha^{H_{i-1}} \beta^{M_i} mod\ p, \quad (11)$$

де p – велике просте число, $M_i < p - 1$, α – перший корінь за модулем p. Розкладання $p - 1$ повинно містити як мінімум один великий простий множник, тоді β обчислюється за формулою:

$$\beta = \alpha^x \, mod \, p, \tag{12}$$

де x – ключ до потайного ходу хеш-функції. Ключ x відіграє роль закритого параметра хеш-функції. Після вибору x, обчислюється значення p, яке відіграє роль відкритого параметра, і вписується в специфікацію хеш-функції. Якщо підставити розкладання β у раундову формулу обчислення хеш-функції:

$$H_i = \alpha^{H_{i-1}}\beta^{M_i} mod \; p = \alpha^{H_{i-1}}(\alpha^x \, mod \, p)^{M_i} = \alpha^{H_{i-1}+xM_i} mod \; p. \tag{13}$$

З даного розкладання видно, що при знанні x можна створити два або більше повідомлень, для яких би обчислювалося однакове значення хеш-функції H_i. Стійкість знаходження ключа x ґрунтується на складності завдання дискретного логарифмування. Знання ключа x дає змогу обчислити колізію для заданого повідомлення або документа, не розв'язуючи задачу дискретного логарифмування.

При знанні ключа до потаємного ходу колізія знаходиться таким чином. Для наявного документа M, представленого у вигляді блоків $\{M_1, M_2, \dots, M_{i-1}, M_i\}$, необхідно сформувати модифікований документ M', що складається з блоків $\left\{M_1', M_2', \dots, M_{i-1}', M_i'\right\}$, так, щоб їм відповідало однакове вихідне значення хеш-функції. Блоки документів відповідають блокам, що подаються на вхід раундової функції хешування. Результати хешування блоків позначимо як $\{H_1, H_2, \dots, H_{i-1}, H_i\}$, для вихідного документа і $\left\{H_1', H_2', \dots, H_{i-1}', H_i'\right\}$ для зміненого документа. Блоки $\{M_1, M_2, \dots, M_{i-1}\}$ модифікуються довільним чином. Блок M' відіграє роль коригувального блоку, тобто блоку, що забезпечує рівність $H_i = H_i'$. Коригувальний блок знаходиться з рівності:

$$\alpha^{H_{i-1}'+xM_i'} \, mod \; p = \alpha^{H_{i-1}+xM_i} mod \; p. \tag{14}$$

Виходячи з того, що α – перший корінь за модулем p, маємо:

$$H_{i-1}' + xM_i' = H_{i-1} + xM_i \; mod \; (p-1). \tag{15}$$

Формула коригувального блоку даних M_i' має такий вигляд:

$$M_i' = (H_{i-1} - H_{i-1}') \cdot x^{-1} + M_i \; mod \; (p-1). \tag{16}$$

Однак, якщо мати в наявності два документи, визначені з використанням даної схеми, можна обчислити ключ x. Таким чином, подана схема потребує посилення. Систематизація ознак несанкціонованого доступу до корпоративної інформації є надзвичайно важливим аспектом сучасної кібербезпеки. Застосування криптографічних методів захисту відіграє ключову роль у створенні надійних механізмів оборони. Одним із ефективних інструментів є використання хеш-функцій, таких як MD5, SHA-256, SHA-3 та інших, для забезпечення цілісності та конфіденційності даних.

Один із підходів до систематизації ознак несанкціонованого доступу базується на використанні багаторівневої аутентифікації. Цей метод передбачає використання не лише паролів, але й додаткових аутентифікаційних етапів, таких як біометричні дані, картки доступу, або одноразові коди. Такий підхід дозволяє створити надійний бар'єр для потенційних зловмисників [2, 3-5, 9, 11-16].

Ще однією важливою складовою є використання «солі» при хешуванні паролів. «Сіль» представляє собою унікальні випадкові дані, які додаються до пароля перед його хешуванням. Цей підхід істотно ускладнює атаки методом перебору грубою силою, оскільки для кожного користувача генерується унікальний хеш, навіть у випадку, коли вони використовують однакові паролі. Коли користувач вводить свій пароль, система додає унікальну «сіль» до нього. Це стає частиною початкових даних для алгоритму хешування. Такий підхід робить неможливим використання заздалегідь підготовлених таблиць рейнджів (rainbow tables) для розкриття пароля, оскільки навіть однакові паролі при різних "солях" будуть мати різні хеш-значення. Використання «солі» важливе для забезпечення додаткового рівня безпеки, запобігаючи використання загальнопоширених атак на паролі та забезпечуючи індивідуалізацію хеш-значень для кожного користувача [16-19]

Зокрема, важливо зазначити, що сучасні криптографічні методи захисту активно розвиваються для протистояння новим викликам кібербезпеки. Застосування квантової криптографії, використання блокчейн-технологій в системах безпеки, та розвиток алгоритмів, стійких до квантових обчислень, відкривають нові перспективи для захисту корпоративної інформації. Такі інновації роблять системи захисту більш надійними та відповідними вимогам сучасного цифрового середовища [5-7, 8, 11-13, 17-19].

Отримавши хеш-значення від передавача, вбудований пристрій усередині системи проводить складний процес порівняння між цим хеш-значенням та збереженим еталонним значенням у базі даних. У разі успішного зіставлення обох значень, система дозволяє доступ до корпоративної інформації.

На відміну від стандартного застосування криптографічних методів, в даній системі використовуються не тільки алгоритми хешування MD5 або SHA-256, але й передові технології, такі як квантова криптографія, для забезпечення ще вищого рівня захисту. Важливим аспектом цього підходу є систематизація різноманітних ознак несанкціонованого доступу. Тут не лише виявляється сам факт порушення, але і аналізуються всі можливі аномалії в хеш-значеннях, що можуть свідчити про спроби несанкціонованого доступу. Це зроблено для того, щоб система була не лише реактивною, але і прогнозованою, відповідаючи на потенційні загрози та уникати їхнього ушкодження [9-13, 17-19].

Такий підхід робить систему адаптивною та здатною ефективно виявляти та захищати корпоративну

інформацію від небажаних втручань, що вносить вагомий внесок у загальну безпеку корпоративного середовища.

Розглянута стратегія систематизації ознак несанкціонованого доступу до корпоративної інформації, заснована на використанні криптографічних методів захисту, спрямована на вдосконалення та ефективний захист від потенційних вторгнень. Перший етап цієї стратегії включає в себе впровадження стійких криптографічних алгоритмів, зокрема використання алгоритму MD5 для генерації хеш-значення від випадкового ключа та вхідних даних. Цей підхід створює надійну основу для подальшого забезпечення безпеки та збереження конфіденційності корпоративної інформації [4-9, 11, 16, 17-19].

Обрана архітектура системи використовує платформу Arduino UNO та модуль Zigbee для оптимізації операції передачі даних між пристроями. Arduino UNO виступає як основна платформа, забезпечуючи обробку та передачу інформації, тоді як модуль Zigbee використовується для забезпечення надійного бездротового зв'язку між пристроями. Принцип роботи системи полягає в тому, що на етапі формування ключа використовується двійковий шаблон, який є основою для генерації ключа. У системі використовується метод хешування MD5 для створення хеш-значення на основі введених даних та використаного ключа. Після отримання хеш-значення воно передається віддаленому пристрою за допомогою модуля Zigbee. На стороні віддаленого пристрою використовується другий модуль, який відповідає за обробку отриманого хеш-значення. Цей модуль виконує необхідні операції для порівняння отриманого хеш-значення з тим, що зберігається в системі. Цей процес є ключовим етапом в системі захисту, оскільки дозволяє ефективно перевірити цілісність та автентичність інформації під час передачі та прийому даних [4, 10, 12, 14-17]. Аналіз генерації хеш-значення MD5 виявив важливість використання випадково згенерованого ключа. Процес введення даних користувачем через матричну клавіатуру 4x4 ініціює формування секретного ключа, який в подальшому використовується для створення хеш-значення. Здобуте хеш-значення передається на іншу обчислювальну платформу через модуль зв'язку для додаткової обробки та перевірки доступу. Ці інноваційні методи сприяють впровадженню ефективної та безпечної системи передачі та обробки даних між електронними пристроями.

Застосування принципів безпеки та криптографічних методів в цьому контексті максимально ефективно, оскільки вони гарантують високий рівень захисту інформації від несанкціонованого доступу. При цьому виключаються можливість втручання та порушення конфіденційності корпоративних ресурсів, забезпечуючи тільки авторизований доступ [7-10].

В рамках дослідження, спрямованого на систематизацію ознак несанкціонованого доступу до корпоративної інформації з використанням криптографічних методів захисту, розглядаємо процес введення пін-коду та його вплив на безпеку даних. При правильному введенні користувачем пін-коду система генерує хеш-значення, яке в подальшому порівнюється із збереженим хеш-значенням [3, 11-19]. У випадку відповідності обидвох значень, передавач ініціює відповідні заходи забезпечення доступу. З іншого боку, неправильний пін-код призводить до створення хешу, який не збігається із збереженим значенням. У цьому випадку система автоматично повідомляє власника про виявлену проблему.

Отримані результати аналізу, де вказані коефіцієнти кореляції (рис. 4), дозволяють оцінити ступінь взаємозв'язку між вхідними даними.

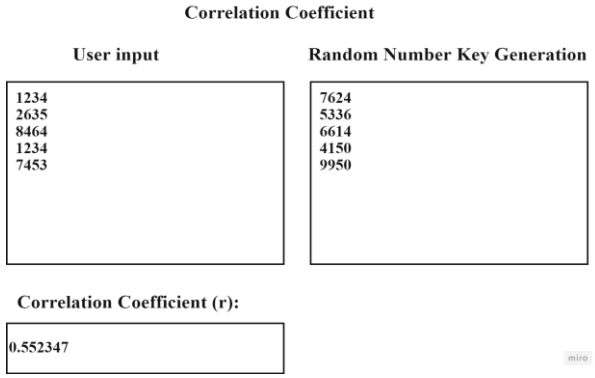

Рис. 4. Коефіцієнти кореляції

Значення коефіцієнта кореляції, що дорівнює 0,552347, свідчить про наявність певного рівня залежності між визначеними параметрами.

З аналізу (табл. 1) можна визначити, що генерація хеш-значення для вхідних даних включає в себе етап випадкової генерації чисел, що сприяє підвищенню рівня безпеки та непередбачуваності цього процесу.

Таблиця 1

Представлення згенерованого хеш-значення

Input	Random Key Generation	Generated Hash
1234	7624	ec5a9922acec4dad14377237d38fe193
2635	5336	276c2f2bff48d7930c717a6a01457c00
8464	6614	a414e9f523a5ac020356a8bb467c3397
1234	4150	f0599bef811233125c682ac5b1649150
7453	9950	c57d70034892e3efe871c12f022486ca

Висновки. Швидкий розвиток інформаційних технологій, що супроводжується зростанням обсягів обробленої, збереженої та переданої інформації в комп'ютерних і комунікаційних системах, створює сприятливі умови для незаконних дій у сфері електронної інформації. Для вирішення завдань інформаційної безпеки набуває ключового значення використання програмно-технічних засобів керування правами доступу до ресурсів інформаційно-обчислювальних систем. Ці засоби забезпечують розмежування повноважень користувачів, які беруть участь у технологічному процесі автоматизованої обробки інформації. Важливим аспектом ефективного управління

доступом є широке використання криптографічних перетворень, які гарантують автентифікацію та цілісність інформації, а також захист від несанкціонованого доступу до корпоративної інформації. Тому важливо вдосконалити засоби шифрування як базовий механізм захисту інформації, щоб підвищити її рівень захищеності на всіх етапах обробки.

Застосування механізму шифрування як важливої складової системи захисту стало визначеним технологічним аспектом. Актуальність даної теми обумовлена широким впровадженням комп'ютерних технологій у системи управління та обробки корпоративної інформації, де вирішення проблем інформаційної безпеки вимагає високого рівня захисту, зокрема за допомогою програмних механізмів, які включають в себе реалізації криптографічних алгоритмів.

У контексті актуальних викликів, пов'язаних із забезпеченням безпеки корпоративної інформації, розглянуто систематизацію ознак несанкціонованого доступу до даних, що базується на застосуванні криптографічних методів захисту. Проведено аналіз цієї проблеми, фокусуючись на ключових аспектах, що визначають стійкість та ефективність застосованих методів. У рамках розгляду проблематики несанкціонованого доступу до корпоративної інформації, визначено необхідність систематизації ознак, що свідчать про потенційні загрози та порушення конфіденційності корпоративних даних. Цей підхід передбачає структурування та класифікацію можливих векторів атак, що дозволяє розробити ефективні криптографічні заходи захисту.

На перший погляд, важливим етапом є впровадження криптографічних алгоритмів, спрямованих на генерацію стійких хеш-функцій. Використання конкретних алгоритмів, таких як MD5, забезпечує створення хеш-значень на основі випадкових ключів та вхідних даних. Наприклад, використання алгоритму MD5 включає створення хеш-значень з використанням випадкових ключів і конфіденційних вхідних даних, що надає основу для наступного рівня захисту в системі. Такий підхід дозволяє підвищити безпеку та стійкість системи до потенційних атак на основі криптографічних методів захисту. Не менш важливим елементом є реалізація цих методів через використання технічних засобів, таких як платформа Arduino UNO та модуль Zigbee. Проведений експериментальний аналіз генерації хеш-значень MD5 демонструє високу ступінь ефективності використання випадкових ключів у вказаному контексті.

Окрім того, важливим аспектом є процес аутентифікації користувача, який базується на введенні пін-коду через матричну клавіатуру. Секретний ключ, згенерований внаслідок цього процесу, використовується для подальшої генерації хеш-значень, що визначає правомірність доступу.

Підсумовуючи, запропонована стратегія систематизації ознак несанкціонованого доступу на базі криптографічних методів захисту відкриває перспективи удосконалення та розширення систем безпеки корпоративної інформації. Додатковий розвиток цього напрямку може полягати у вдосконаленні алгоритмів, розширенні застосувань технічних рішень та вдосконаленні політики безпеки для забезпечення найвищого рівня захисту корпоративної інформації.

Список літератури

[1]. Saibal K. Pal, Diwakar Bhardwaj, Rajat Kumar & Varun Bhatia. A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations. IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[2]. R. Steinwandt, M. Grassl, W. Geiselmann, Beth, T., Weaknesses in the SL2(F2n) hashing scheme. In CRYPTO 2000. Lecture Notes Computer Science, vol. 1880 (Springer, Berlin, 2000), pp. 287-299.

[3]. K.S. Abdukhalikov, C. Kim, On the security of the hashing scheme based on SL2. In Fast Software Encryption 1998. Lecture Notes Computer Science, vol. 1372 (Springer, Berlin, 1998), pp. 93-102.

[4]. Meng YK, Wok L. Adaptive non-critical alarm reduction using hash-based contextual signatures in intrusion detection. Computer Communications. 2014 Feb; 38: 50-9.

[5]. Wang C, Zhang X, Zheng Z. Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme. Plos One. 2016; 11(2): e0149173.

[6]. Maitra T, Obaidat MS, Islam SH, Giri D, Amin R. Security analysis and design of an efficient ECC-based two-factor password authentication scheme. Secur Commun Netw. 2016; 9(17): 4166-4181.

[7]. Murillo-Escobar M, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez R. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert Systems with Applications. 2015 Nov; 42(21): 8198-211.

[8]. Mihailescu M. New enrollment scheme for biometric template using hash chaos-based cryptography. Procedia Engineering. 2014 Mar; 69:1459-68.

[9]. Yu J, Hao R, Zhao H, Shu M, Fan J. IRIBE: Intrusion-Resilient Identity-Based Encryption. Information Sciences. 2016 Feb; 329:90-104.

[10]. Guo H, Wang P, Zhang X, Huang Y, Ma F. A robust anonymous biometric-based authenticated key agreement scheme for multi-server environments. Plos One. 2017; 12(11): e0187403. https: // doi.org / 10.1371/ journal. pone. 0187403 PMID: 29121050.

[11]. Yang L, Zheng Z. Cryptanalysis and improvement of a biometrics-based authentication and key agreement scheme for multi-server environments. Plos One. 2018; 13(3): e0194093. https: // doi.org/10.1371/ journal-pone.0194093 PMID: 29534085.

[12]. Jo Hyang-Rim, Pak Kyong-Sok, Kim Chung-Hyok, Zhang Il-Jin: Cryptanalysis and improved mutual authentication key agreement protocol using pseudo-identity. PLoS ONE , Volume 17 (7), Jul 28, 2022.

[13]. Ghosh R, Verma S, Kumar R, Kumar S, Ram S. Design of hash algorithm using Latin square. Procedia Computer Science, Jan 1, 2015.

[14]. Zhao T, Ran Q, Yuan L, Chi Y, Ma J. Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography. PLoS ONE , Volume 17 (9), Sep 16, 2022.

[15]. Politou Eugenia, Alepis Efthimios, Patsakis Constantinos. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity , Volume 4 (1), Jan 1, 2018.

[16]. Azzaz Mohamed Salah, Tanougast Camel, Maali Abdelmadjid, Benssalah Mustapha. An efficient and lightweight multi-scroll chaos-based hardware solution for protecting fingerprint biometric templates. International Journal of Communication Systems , Volume 33 (10), Jul 10, 2020.

[17]. Vijayarajan R, Gnanasivam P, Avudaiammal R. Bio-Key Based AES for Personalized Image Cryptography. The Computer Journal , Volume 62 (11), Nov 11, 2019.

[18]. Kocher P, Jaffe J, Jun B, Rohatgi P. Introduction to differential power analysis. Journal of Cryptographic Engineering. 2011; 1(1): 5–27.

[19]. Tzeng SF, Horng SJ, Li T, Wang X, Huang PH, Khan MK. Enhancing Security and Privacy for Identitybased Batch Verification Scheme in VANET. IEEE Transactions on Vehicular Technology. 2017; 66 (4):3235–3248.

УДК 681.3.06

Kryvoruchko O., Kostiuk Y., Desiatko A. Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods

Abstract. *Recently, an increase in incidents of unauthorized access to corporate information has been detected. The article considers an approach aimed at solving the issue of developing a method whose main purpose is to propose a scheme for protecting corporate information from any unauthorized access using a cryptographic algorithm. The reliability of the algorithm is achieved by combining a cryptographic algorithm with a secret key. The implementation of a binary template as a secret key, which is integrated into the process of generating a hash value using the MD5 hashing algorithm, is characterized by a relatively high degree of stability and reliability. The subsequent comparison of the obtained hash value with the stored one is carried out in order to effectively manage access to corporate information. The use of a hidden key in the hashing algorithm means that the data is used as an additional input to a one-way function that hashes the password. Thus, the method of the chosen cryptographic scheme demonstrates effectiveness in ensuring the confidentiality, integrity and availability of corporate information.*

Keywords: *unauthorized access, cryptographic methods of protection, hashing algorithm, hash value, hidden key, stability.*

Криворучко Олена Володимирівна, д.т.н., професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету, Україна.

Olena Kryvoruchko, Doctor of Technical Sciences, Professor, Head of the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics.

Костюк Юлія Володимирівна, PhD, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.

Yuliia Kostiuk, PhD in Engineering, Senior Lecturer at the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics.

Десятко Альона Миколаївна, к.т.н., доцент кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.

Alyona Desyatko, PhD in Engineering, Associate Professor at the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics.

Отримано *4 березня 2024 року,* затверджено редколегією *1 квітня 2024 року*