МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Гулька Олександр Олександрович

Програмний засіб захисту інформації на основі хеш-функції / The software of information security based on hash-function "

напрям підготовки: 6.050102 - Комп’ютерна інженерія
фахове спрямування - Комп’ютерні системи та мережі
Бакалаврська робота

Виконав студент групи КСМ 41/1
О.О. Гулька

Науковий керівник: к.т.н., доцент
Дубчак Л.О.

Тернопіль - 2018

РЕЗЮМЕ

Дипломний проект містить 95 сторінок пояснюючої записки, 3 рисунки, 7 таблиць, 2 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою даного дипломного проекту є розробка програмного комплексу, що дозволяє обчислити значення хеш-функції модифікованого алгоритму MD5 для перевірки цілісності даних в операційній системі Windows XP.

Розроблений програмний комплекс використовує методи інтерфейсу CryptoAPI, що дозволяє побудувати багаторівневу систему захисту, що залежить від рівнів загроз.

Розроблена система апробована на практиці і може бути використана для встановлення цілісності і автентичності інформації.

Ключові слова: ХЕШУВАННЯ, КОМП’ЮТЕРНА СИСТЕМА, MD5, ПРОГРАМНИЙ ЗАСІБ, СИСТЕМА ЗАХИСТУ.

RESUME

Diploma project contains 95 pages of explaining message, 3figures, 7 tables, 2 additions. Volume of graphic material 2 leaves of format A3.

The purpose of this work is development of programmatic complex, which allows calculating the value of one way modification algorithm of hash function MD5 for verification of integrity the data in operation system Windows XP.

Developed a programmatic complex uses the methods of interface of CRYPTOAPI, which allows to build the multilevel security system, which depends on the levels of threats.

The system is developed approved in practice and can be used for establishment of integrity and authenticity of information.

Key words: HASHING, COMPUTER SYSTEM, MD5, SOFTWARE, SECURITY SYSTEM.

ЗМІСТ

Вступ 10

1 Аналіз інформаційної безпеки в комп’ютерних системах 12

1.1 Сучасний стан захисту інформації в комп’ютерних системах 12

1.2 Структурний підхід до проведення атак в операційній системі сімейства Windows 17

1.3 Формування вимог та постановка задачі 24

2 Алгоритмічне забезпечення модифікованої хеш-функції MD5 28

2.1 Структура модифікованої хеш-функції MD5 28

2.2 Особливості застосування хеш-функції в комп’ютерних системах 34

2.3 Оцінка стійкості хеш-функції 37

3 Розробка програмного комплексу 45

3.1 Вибір мови програмування 45

3.2 Опис основних модулів програмного комплексу 47

3.3 Результати роботи програмного комплексу 56

4 Охорона праці 60

4.1 Аналіз санітарно-гігієнічних умов праці 60

4.2 Пожежна безпека 72

Висновки 74

Список використаних джерел 76

Додаток А Фрагмент програмного коду 82

Додаток Б Довідка про використання 97

ВСТУП

Важливою задачею захисту інформації залишається перевірка її цілісності. Контроль цілісності здійснюється шляхом розрахунку деякої контрольної суми даних. Проблема простих алгоритмів обчислення контрольної суми полягає в тому, що досить легко підібрати кілька масивів даних, що мають однакову контрольну суму. Криптоалгоритми широко застосовуються не лише для задач шифрування даних, але й для автентифікації та перевірки цілісності. На сьогодні існують добре відомі і апробовані криптоалгоритми (як симетричні, так і несиметричні), стійкість яких доведена математично або базується на необхідності рішення математично складної задачі (факторизації, дискретного логарифму і т.д.). Криптографічно стійкими вважаються контрольні суми, які обчислюються за допомогою знаходження хеш-функції, яка приєднується до вихідного тексту.

Якщо потрібно перевірити ідентичність файлу, необхідно послати значення хеш-функції. Якщо її значення збігаються, то файли вважаються ідентичними. Одностороння функція визначена на множині натуральних чисел і не потребує великих ресурсів для обчислення власного значення. Проте, обчислити зворотнє значення функції є надзвичайно складною задачею.

В односторонньої хеш-функції може бути безліч імен: функція стиснення, функція скорочення (contraction function), короткий виклад, криптографічна контрольна сума, код цілісності повідомлення (message integrity check (MIC)) і код виявлення маніпуляції (manipulation detectioncode (MDC)). Як би вона не називалася, ця функція посідає важливе місце в сучасній криптографії. Однонапрямлена хеш-функція — це одна із частин багатьох протоколів.

Актуальність даної роботи полягає в тому, що розроблений програмний комплекс дозволить застосувати модифікований алгоритм MD5 для обчислення хеш-функції, що дозволяє встановити автентичність інформації.

Мета роботи полягає у розробці програмного комплексу для операційної системи Windows XP на основі модифікованого алгоритму хешування MD5, що дозволить здійснити перевірку достовірності інформації.

1 АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Сучасний стан захисту інформації в комп'ютерних системах

Надійний захист інформації, який забезпечував би попередження, перекручення або знищення інформації, а також унеможливлював би її зловмисне отримання, використання або несанкціоновану модифікацію є однією із важливих задач. Особливої гостроти набуває ця проблема у зв'язку із масовою комп'ютеризацією інформаційних процесів і, насамперед, у зв'язку з об'єднанням комп'ютерів в інформаційно-обчислювальні мережі, що забезпечує масовий доступ будь-яких користувачів до їх ресурсів.

Впровадження популярних дешевих комп'ютерних систем масового попиту і застосування робить їх надзвичайно вразливими щодо деструктивних впливів. Безліч прикладів, що підтверджують поширеність цього явища, можна знайти на сторінках численних видань, а ще більше в Internet. Причому понад 80% комп'ютерних злочинів відбувається за допомогою Internet. Оцінки втрат коливаються від десятків мільйонів до мільярдів. Точні оцінки неможливо отримати в принципі з багатьох причин.

Протягом останніх років постійно винаходять нові й нові види та форми обробки інформації і паралельно винаходять все нові види і форми її захисту. Однак цілком її ніяк не вдається захистити і, напевно, не вдасться взагалі. Інакше кажучи, можна говорити про деяке кризове становище в забезпеченні безпеки в інформаційних технологіях [1].

Спостерігається збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою засобів обчислювальної техніки. При цьому мова йде не тільки про різке і буквальне збільшення самих обсягів, а про розширення методів, способів і можливостей її зосередження і збереження. Наприклад, проникнувши в базу даних, можна отримати інформацію практично

про все на світі. Особливо розширилися можливості подібного роду з виникненням глобальної мережі Internet.

Комп'ютерна техніка за останні роки отримали гігантську потужніть, але стали набагато простішими в експлуатації. Це означає, що все більша кількість користувачів одержує доступ до комп'ютера, а середня кваліфікація їх знижується. Користувачі самі здійснюють їх адміністрування, але більшість з них не в змозі постійно підтримувати безпеку своїх систем на високому рівні, оскільки це вимагає відповідних знань, навичок, часу і коштів. Поширення мережевих технологій об'єднало їх в мережі, тепер безпека мережі починає залежати від безпеки її компонентів і зловмиснику досить порушити роботу однієї з них, щоб скомпрометувати всю мережу.

Телекомунікаційні технології об'єднали локальні мережі в глобальні. І саме розвиток Internet, окрім всіх плюсів користування, забезпечує широкі можливості для здійснення порушень безпеки систем обробки інформації всього світу. Якщо комп'ютер підключений до Internet, то для зловмисника немає ніякого значення, де він знаходиться — у сусідній кімнаті чи на іншому кінці світу.

Розвиток локальних мереж і Internet диктує необхідність здійснення ефективного захисту при віддаленому доступі до інформації, а також взаємодії користувачів через загальнодоступні мережі.

Варто зазначити, що захисту підлягає не будь-яка інформація, а тільки цінна. Цінною ж стає та інформація, володіння якою дасть змогу її дійсному чи потенційному власнику одержати який-небудь виграш: моральний, матеріальний, політичний і ін. Оскільки, в суспільстві завжди існують люди, які бажають мати якісь переваги над іншими, то в них може виникнути бажання незаконним шляхом одержати цінну інформацію, а в її власника виникає необхідність її захищати. Цінність інформації є критерієм при прийнятті будь-якого рішення про її захист. Хоча було багато спроб формалізувати процес оцінки інформації з використанням методів теорії інформації та аналізу рішень,

цей процес залишається дуже суб'єктивним.

Для оцінки інформації потрібен її розподіл на категорії не тільки відповідно до її цінності, а й за важливістю. За рівнем важливості можна розділити: життєво важлива незамінна інформація, наявність якої необхідна для функціонування системи; важлива інформація, яку можна замінити чи відновити, але цей процес важкий і пов'язаний з великими витратами; корисна інформація, яку важко відновити, однак система може досить ефективно функціонувати і без неї; несуттєва інформація, без якої система продовжує існувати.

Для власника джерела інформації та зловмисника (організація чи особа, що прагне незаконно одержати інформацію) значущість однієї і тієї ж інформації може бути різна. Практика показала, що захищати потрібно не тільки секретну інформацію, оскільки і несекретна, піддана несанкціонованим ознайомленням чи модифікації, може привести до витоку чи втрати пов'язаної з нею секретної інформації, а також невиконання функцій обробки секретної інформації.

Перехід до інформаційного суспільства у велетенській сфері інформаційної діяльності людей виокремив інформаційний сектор економіки, основну частину якого становить суто інформаційна індустрія, а в ній найперспективніша структура — Internet-економіка. Глобальна комп'ютерна мережа Internet вважається „четвертим каналом", що зв'язує людей між собою [1]. В інформаційному світі існує дві відомі технологічні тенденції: потужність комп'ютерів зростає вдвічі кожен рік і корисність мережі для суспільства пропорційна квадрату числа користувачів. Надзвичайно високі темпи зростання глобальної комп'ютерної мережі Internet зумовлені тим, що вона базується на обох цих закономірностях. Сьогодні світ бурхливо переживає ще один бум – зміщення акцентів з комунікаційної та інформаційно-пошукової функцій Internet на реалізацію за її допомогою сучасного бізнесу. Електронна пошта, програми електронних пейджерів, чати та інші способи спілкування у мережі забезпечують обмін між діловими партнерами пересічною і навіть стратегічною комерційною інформацією за лічені хвилини. Завдяки цьому долаються географічні та

національні кордони географічного простору. Весь світ стає клієнтом фірми, що визначає стратегію маркетингу, оскільки ареною конкуренції стає весь світовий економічний простір. Це до небачених меж розширює можливості підприємства, хоч і підвищує його ризики.

Мережа стала неперевершеним засобом для проведення маркетингу і здійснення прямих онлайнових продажів, підвищення рівня обслуговування клієнтів, найпотужнішим інструментом управління фірмою і джерелом інформації для наукових і практичних розробок. Складне управлінське завдання з налагодження спільної роботи багатьох структурних підрозділів установи під час обробки інформації вирішується шляхом створення і реалізації Intranet локальної комп'ютерної мережі підприємства, яка працює на основі Internet-технологій. Протягом найближчого десятиріччя глобальна тенденція використання можливостей Internet для бізнесу вплине на десятки секторів світової економіки. Перетворення основних бізнес-процесів з допомогою Internet-технологій становить сутність електронного бізнесу та електронної комерції. І тут особливо важливими є засоби захисту передавання електронних повідомлень, надійний та ефективний зв'язок. Безпека продавців і покупців у мережі має підтримуватися не тільки законодавчими заходами, а й програмно-технічними засобами. Виробники апаратних пристроїв і розробники програмних продуктів, усвідомлюючи важливість ринку електронної комерції як найперспективнішого в сучасній інформаційній економіці, повинні приділяти велику увагу розробці надійних правил і засобів захищеної передачі інформації мережею.

Однією з найпоширеніших крадіжок є ідентифікаційна інформація: злодії збирають персональну інформацію — імена, адреси та інші важливі дані, а після цього замовляють картки під цими іменами. Хакери і кракери „зламують" сайти, які зберігають цю інформацію, а в деяких випадках злочинці вдають із себе легітимних онлайнових торговців і збирають інформацію в покупців, які нічого не підозрюють. Дійсні номери карток також можуть бути автоматично

згенеровані [2]. Отже, головними вимогами до здійснення комерційних операцій в Internet є конфіденційність, цілісність, автентифікація, гарантії і збереження таємниці. Крім відповідальності осіб і установ та дотримання законів, що захищають споживача від можливого шахрайства, наведені вимоги можна забезпечити технічними і програмними засобами захисту інформації.

Таким чином, інформація — це одна з найцінніших речей в сучасному житті, і поява глобальних комп'ютерних мереж зробила простим отримання доступу до інформації як для окремих людей, так і для великих організацій. Але легкість і швидкість доступу до даних за допомогою комп'ютерних мереж, таких як Internet, також зробили значними наступні загрози безпеки даних за відсутності заходів їх захисту: неавторизований доступ до інформації; неавторизована зміна інформації; неавторизований доступ до мереж та інших сервісів; інші мережеві атаки, такі як повтор перехоплених раніше транзакцій і атаки типу "відмова в обслуговуванні" [2].

Коли кінцевий користувач посилає електронне повідомлення по мережі, він широко відкриває двері перед потенційним агресором. Як стверджують знавці комп'ютерної безпеки, люди навіть не уявляють собі, наскільки легко досвідчений хакер може скористатися недосконалістю комунікаційних протоколів і ознайомитися із змістом електронних Internet-листів, послати фальшиве повідомлення і навіть отримати доступ до інших підключених до мережі систем. Все, що для цього треба знати — це ім'я домена або одна IP-адреса; якщо дана інформація стає відома зловмиснику, то перед ним відкривається шлях до здійснення різноманітних негативних дій.

Саме з цих причин на сьогодні велика частина уваги приділяється пошуку і аналізу засобів і методів підвищення захисту інформації в глобальній комп'ютерній мережі. Всі рішення грунтуються на попередньому шифруванні даних при передачі по каналах зв'язку. Такий підхід істотно зменшує вірогідність злому. Існує багато технологій, які використовують різні алгоритми і стандарти шифрування. Але слід врахувати, що при роботі в мережі на

криптографічну підсистему накладається ряд обмежень. Оскільки час шифрування обмежений, в ній повинен використовуватися дуже простий, легко реалізований і в той же час криптостійкий алгоритм шифрування. Для підвищення виробництва в цілому, виробники таких систем пішли по шляху реалізації деяких блоків на апаратному рівні. Тобто було створено спеціальне обладнання, що виконує ряд функцій, пов'язаних з обробкою і шифруванням даних.

1.2 Структурний підхід до проведення атак в операційній системі сімейства Windows

Під час дослідження ядра операційної системи Windows NT провідний спеціаліст з інформаційних систем Нім Вочман виявив, що при звичайній зміні одного біта програмного коду змінюються всі налаштування безпеки для всієї мережі комп'ютерів під керуванням Windows.

Варто звернути увагу і на вектор вторгнення. Це є структурний підхід, що дозволяє виявити недолік в програмі, здійснює переміщення коду з одного місця зберігання в інше; характеризує структуру даних або середовище, яке містить і передає код з одної області зберігання в іншу. Що стосується переповнення буфера, то вектори вторгнення — це добре підготовлені вхідні повідомлення, які заставляють програму порушника переходити в стан переповнення буфера. Тобто це фрагмент атаки, під час якої відбувається проникнення і запуск коду в програмі.

Розрізняють вектор вторгнення і корисне навантаження (payload) [3]. Корисне навантаження — це програмний код, який реалізує наміри атакуючого. Поєднання вектора вторгнення і корисного навантаження використовується для проведення повної (цілісної) атаки, а сам вектор вторгнення використовується

для отримання контролю над вказівниками команд. Після отримання контролю над вказівником команди зловмисник може встановити його на будь-який буфер, що контролюється, або іншу область пам’яті, в якій зберігається корисне навантаження. Таким чином, коли атакуючий може контролювати вказівник команд, тоді в нього з’являється можливість передати керування (змінити хід виконання програми) програмою коду корисного навантаження. Зловмисник заставляє вказівник команд вказувати на небезпечний код, що призводить до його виконання.

Вектори вторгнення завжди пов’язані з конкретною помилкою або недоліком в програмному забезпеченні, що підлягає атаці. Для кожної версії програмного забезпечення існують унікальні вектори вторгнення. При розробці засобів атаки зловмисник повинен спроектувати і створити конкретні вектори вторгнення для конкретної задачі.

При створенні вектора вторгнення повинні враховуватись деякі фактори: розмір буфера, впорядкування даних в пам’яті і обмеження набору символів. За звичай, вектори вторгнення відповідають правилам визначеного протоколу. Наприклад, переповнення буфера в маршрутизаторі може бути організовано за допомогою вектора вторгнення для обробки пакетів протокола BGP (Border Gateway Protocol). Цей вектор вторгнення реалізовано як спеціально підготовлений BGP – пакет. Оскільки підтримка протоколу BGP є необхідною для нормальної роботи в Internet, то атака такого типу здатна знищити системи, які обслуговують мільйони користувачів. Більш яскравим прикладом є протокол OSPF (Open Shotest Path First). В маршрутизаторах Cisco реалізація цього протокола може бути використана для видалення інформації про цілу локальну мережу масштабного мережевого вузла.

Для атак на переповнення буфера характерна наявність чіткої межі між вектором вторгнення і корисного навантаження. Ця межа називається адресою повернення (return address). Адресу повернення можна схематично визначити в той момент, коли корисне навантаження або отримує керування над центральним

процесором, або не спрацьовує [3].

Варто зазначити, що однією із важливих задач вектора вторгнення є вибір області пам’яті, в якій повинно зберігатися корисне навантаження. Його можна зберігати безпосередньо у буфері або в окремій області пам’яті. Зловмисник повинен знати адресу комірки пам’яті (в якій зберігається корисне навантаження), і цю адресу має враховувати вектор вторгнення (рисунок 1.1). Обмеження для набору символів призводять до обмежень в значеннях, які доступні для того, щоб вказати адреси пам’яті. Наприклад, при обмеженні на введення чисел більше ніж 0xB0000001, вибраний вказівник повинен знаходитися в пам’яті вище цієї адреси [4]. Такі обмеження відповідають проблемам, які виникають при перетворенні аналізаторами байтів, які використовуються для символів коду атаки, на інші значення, або при роботі фільтрів, які блокують недопустимі символи у потоці даних. На практиці в багатьох атаках використовуються літерно-цифрові символи.

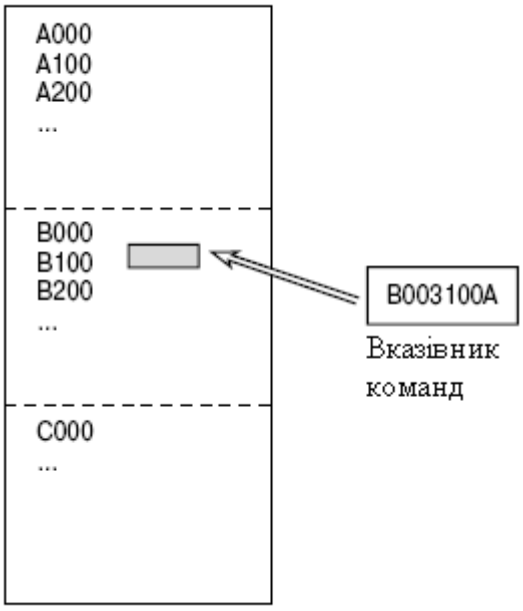

Рисунок 1.1 — Вказівник на корисне навантаження в пам’яті

Атаки на переповнення буфера застосовуються і до вбудованих систем

(мережеве обладнання, принтери, мобільні телефони та ін. невеликі пристрої). Програмний код, який здійснює керування цими вбудованими системами вразливий до вище згаданих атак. Цікаво, що серверне програмне забезпечення стає більш стійким до атак на переповнення буфера, а основний акцент зміщається на програмне забезпечення вбудованих систем.

Вбудовані системи запускаються на різних апаратних платформах. У більшості таких систем для зберігання даних використовується технологія NVRAM. Вбудовані системи широко застосовуються у воєнній апаратурі, наприклад, стандартній воєнній радарній системі AN/SPS-73 [4]. Ця радарна система працює під керуванням захищеної системи VxWorks. Як і в більшості комерційних системах із закритим кодом, в операційній системі VxWorks і програмному забезпеченні для неї є багато помилок, що дозволяють проводити атаки на переповнення буфера. Більшість вразливих місць можуть бути без аутентифікації, наприклад, через RPC-пакети [4]. Таким чином, апаратне забезпечення із вбудованими системами є ціллю для проведення атак.

Проте існує думка, що вбудовані системи не вразливі до віддалених атак, оскільки через відсутність в пристрої інтерактивного командного інтерпретатора доступ або використання “коду командного інтерпретатора” є неможливим. Помилковим є твердження, що зловмисник зможе лише вивести із ладу пристрій керування. Насправді внесений код здатний виконати будь-який набір команд, в тому числі і програму командного інтерпретатора, яка підтримує функції рівня операційної системи. Немає значення, що код не постачається разом із пристроєм. Цей код додається під час атаки. Тобто при атаках на переповнення буфера не потрібно наявності повнофункціонального інтерактивного інтерпретатора TCP/IP. Натомість, при атаці може повністю стиратися конфігураційний файл або замінюватися пароль [5].

Багато складних програм можуть бути встановлені в ході віддалених атак на вбудовану систему. Код командного інтерпретатора є лише одним із варіантів. Не відіграє важливої ролі те, який процесор використовується або яка схема

адресації, оскільки зловмиснику потрібно створити лише діючий код для апаратних засобів, що підлягають атаці. Апаратні засоби із вбудованим програмним забезпеченням є достатньо документовані і загальнодоступні.

Група дослідників з проблем захисту Phenoelit створила програму з кодом командного інтерпретатора для проведення віддаленої атаки на маршрутизатор Cisco 1600 на основі процесора Motorola 68360 QUICC (програма демонструвалася на конференції Blackhat в 2002 році) [5]. Для цієї атаки вектор вторгнення використовує переповнення буфера в операційній системі IOS від Cisco і декілька нових методів використання структур керування “купами” в IOS. Змінюючи структури “купи”, можна впровадити і виконати зловмисний код. В опублікованому варіанті атаки код командного інтерпретатора — це створений код у вигляді машинних команд Motorola, який відкриває потайний хід до маршрутизатора. Цим кодом можна скористатися при наявності будь-якого переповнення буфера в пристроях Cisco.

Ціллю атак на переповнення буфера стають і СУБД (системи управління базами даних). В будь-якій системі керування базами даних існує декілька точок для проведення атак. Програма для роботи з базою даних складається із певного числа взаємодіючих компонентів. В їх число входять сценарії (об’єднують різні модулі між собою), програми для роботи через інтерфейс командної стрічки, процедури і клієнтські програми, що безпосередньо пов’язані з базою даних. Кожен із цих компонентів є потенційним об’єктом для проведення атаки на переповнення буфера. В якості прикладу можна навести вразливу платформу SQL, в якій є нестійка функція OpenDataSource().

Атака на функцію OpenDataSource() була виконана за допомогою протокола трансакції SQL (T- SQL), для якого встановлюється прив’язка до TCP – порту 1433 [6]. Тобто цей протокол дозволяє багатократно передавати аналізатору оператори SQL.

Процедури, що зберігаються, використовуються для передачі даних сценаріям або бібліотекам DLL. Якщо в сценарії або бібліотеці DLL є помилки

стрічки форматування, або якщо в сценарії використовуються вразливі виклики функцій бібліотеки (наприклад, strcpy() або system()), то з'являється можливість їх використати в своїх цілях для системи управління базою даних. Майже кожна процедура передає частину запиту. В даному випадку зловмисник може використати частину запиту, що передається, для переповнення буфера. Наявним прикладом є помилка в Microsoft SQL Server [6]. Зловмисник міг викликати переповнення буфера в коді, який обробляє розширені процедури, що зберігаються.

Деколи сценарії або процедури, що зберігаються, викликають програму з інтерфейсом командної стрічки і подають її на введення даних із запиту. У багатьох випадках це призводить до переповнення буфера або вразливості з можливістю передачі команд. Окрім того, якщо в сценарії не використовується бібліотека API для роботи з базою даних, то звичайні оператори SQL можна передавати для обробки програмі з інтерфейсом командної стрічки. Це ще одна можливість для проведення атаки на переповнення буфера.

Програмні атаки на системи, що написані мовою Java, використовують особливості мови і при перевірці цифрового підпису аплетів [6]. Переповнення буфера частіше виникає в програмах підтримки, які є зовнішніми по відношенню до JVM. Сама JVM пишеться на C для конкретної платформи, тобто без ретельної уваги до деталей реалізації, тому віртуальна машина JVM може виявитися нестійкою до атак на переповнення буфера. Проте стандартна реалізація JVM від компанії Sun Microsystems добре перевірена, і статистичні перевірки, які виконуються для викликів вразливих функцій, не дають позитивних результатів.

Окрім JVM, багаточисельні проблеми переповнення буфера характерні для систем, в яких використовується Java. В якості прикладу розглянемо систему керування реляційними базами даних Progress, в якій вбудована програма jvmStart, що призначена для запуску віртуальної Java - машини. В jvmStart є помилка перевірки на правильність вхідних даних, що представляються в

командній стрічці (помилка стрічки форматування). Дані вводяться в стрічку через функцію printf () як аргумент стрічки. Звідси можна зробити висновок, що розробники програмного забезпечення повинні розглядати систему цілому, а не лише створювати окремі компоненти.

Багато атак базуються на використанні змінних середовища, які є вразливим місцем, де переповнення буфера може застосуватися для передачі в програму зловмисного коду. При цьому програма може приймати неперевірені вхідні дані.

Одним із методів пошуку можливостей переповнення буфера є подання на вхід програми довгих аргументів, що дозволяє досліджувати результати виконання.

Цей підхід використовується засобами безпеки програмного забезпечення. Тому, можна створювати довгі запити для Web або FTP-сервера.

1.3 Формування вимог та постановка задачі

У сучасному програмному забезпеченні (ПЗ) криптоалгоритми широко застосовуються не лише для задач шифрування даних, але й для автентифікації та перевірки цілісності. На сьогодні існують добре відомі і апробовані криптоалгоритми (як симетричні, так і несиметричні), стійкість яких доведена математично, або базується на необхідності рішення математично складної задачі (факторизації, дискретного логарифму і т.д.). Таким чином, атака проводиться шляхом повного перебору або за допомогою рішення математично складної задачі.

Постійно з'являється інформація про помилки або «дірки» в тій чи іншій програмі (в т.ч. які використовують криптоалгоритми). Тому знання про атаки і «дірки» в криптосистемах, а також розуміння причин їхнього виникнення є

однією із необхідних умов розробки захищених систем. Перспективним напрямом досліджень в даній області є аналіз успішно проведених атак або виявлених недоліків в криптосистемах з метою їх узагальнення, класифікації і виявлення причин і закономірностей їх появи і існування.

Група нестійких криптоалгоритмів є найбільш поширеною причиною через чинники, які розглянемо нижче.

Мала швидкість стійких криптоалгоритмів — це основний чинник, що ускладнює застосування хороших алгоритмів, наприклад, в системах «тотального» шифрування або поточного шифрування. Зокрема, програма Norton DiskReet, що містить в собі реалізацію алгоритму DES, при зміні користувачем ключа може не перешифрувати весь диск, оскільки це займе багато час. Аналогічно, програма компресії Stacker фірми Stac Electronics має опцію закриття паролем компресуючих даних. Проте вона не має фізичної можливості шифрувати цим паролем свій файл розміром в декілька сот мегабайт, тому вона обмежується дуже слабким алгоритмом і зберігає хеш-функцію, що залежить від пароля і захищених даних. Досліджено величину криптостійкості цієї функції, яка дорівнює 2^8, тобто пароль може бути розкритий тривіально.

Експортні обмеження — це причина, що пов'язана з експортом криптоалгоритмів або з необхідністю здобувати патент чи права на них. Зокрема, в США заборонений експорт криптоалгоритмів з довжиною ключа більше 40 біт. Очевидно, що така криптостійкість не може вважатися надійною при сучасних обчислювальних потужностях і навіть на персональному комп'ютері, якщо припустити, що швидкість перебору становитиме 50 000 паролів/сек, то в середньому одержимо час перебору близько 4 місяців. Відомі приклади програм, що підлягають експортним обмеженням - це останні версії браузерів Інтернету, зокрема, Netscape Navigator фірми Netscape Communications і Internet Explorer фірми Microsoft. Вони шифрують дані зі 128-бітним ключем для користувачів всередині США і зі 40-бітним ключем для всіх інших [2].

Незнання або небажання використовувати відомі алгоритми — це ситуація,

яка особливо спостерігається в програмах типу Freeware і Shareware, наприклад, в архіваторах. Архіватор ARJ (до версії 2.60 включно) використовує (по замовчуванню) дуже слабкий алгоритм шифрування – просте гамування. Припустимо, що в даному випадку його використання допустимо, оскільки текст, що стискається, повинен бути абсолютно не надмірним і статистичні методи криптоаналізу тут не підходять. Проте після детальнішого дослідження виявилось, що в тексті, що архівується, присутня деяка невипадкова інформація, наприклад, таблиця Хаффмана і деяка інша службова інформація. Тому, коли відомо або з деякою ймовірністю можна передбачити значення цих службових змінних, то можна із тією ж ймовірністю визначити і відповідні символи пароля.

Використання слабких криптоалгоритмів часто призводить до успішного проведення атаки за відкритим текстом. У випадку з архіватором ARJ, якщо зловмиснику відомий хоч би один файл із зашифрованого архіву, то він з легкістю визначить пароль архіву і витягне звідти решту файлів. Навіть, якщо немає жодного файлу в не зашифрованому вигляді, то в будь-якому випадку просте гамування дозволяє досягти швидкості перебору в 350000 паролей/сек. на машині класу Pentium.

Не дивлячись на те, що в цьому випадку застосовуються криптостійкі або сертифіковані алгоритми, ця група причин призводить до порушень безпеки криптосистем із-за їх неправильної реалізації.

Перевірка на слабкі ключі має бути важливою вимогою до створення захищеної системи. Деякі криптоалгоритми (зокрема, DES, IDEA) при шифруванні із специфічними ключами не можуть забезпечити належний рівень криптостійкості. Такі ключі називають слабкими (weak). Для DES відомо 4 слабких і 12 напівслабких (semi-weak) ключів. Приблизна кількість слабких ключів IDEA складає близько 251.

Недостатня захищеність від руйнуючих програмних засобів (РПЗ) — це комп'ютерні віруси, програмні закладки і тому подібні програми, що здатні перехопити секретний ключ або відкриті дані, а також замінити алгоритм на не

криптостійкий. У тому випадку, якщо програміст не передбачив достатніх способів захисту від РПС, вони легко здатні порушити безпеку криптосистеми. Особливо це актуально для операційних систем, які не мають вбудованих засобів захисту або засобів розмежування доступу. Перехоплення пароля — це давно відомий спосіб викрадення пароля, коли программа-«фантом» емулює запрошення ОС, пропонуючи ввести ім'я користувача і пароль, запам'ятовує його в деякому файлі і зупиняє роботу з повідомленням "Invalid password". Для MS DOS і Windows існує безліч закладок для читання і збереження паролів, що набирають на клавіатурі (через перехоплення відповідного переривання), наприклад, при роботі утиліти Diskreet v. 6.0.

Наявність залежності в часі обробки ключів — це порівняльно новий аспект щодо недостатньо коректної реалізації криптоалгоритмів. Багато криптосистем з різною швидкістю обробляють різні вхідні дані.

Основним методом виявлення атак, що використовує більшість сучасних комерційних продуктів, є сигнатурний аналіз. Відносна простота даного методу дозволяє з успіхом використовувати його на практиці. Система виявлення атак (IDS), що застосовують сигнатурний аналіз, звичайно нічого не знають про правила політики безпеки (тому в даному випадку мова йде не про злочинну активність, а тільки про атаки). Основний принцип їхнього функціонування — порівняння у системі/мережі подій із сигнатурами відомих атак — той же принцип, що використовується й в антивірусному програмному забезпеченні.

Існує два, які не виключають один одного, підходи до виявлення мережевих атак: аналіз мережевого трафіка й аналіз контента. У першому випадку аналізуються тільки заголовки мережевих пакетів, у другому — їхній вміст.

Звичайно, найбільш повний контроль інформаційних взаємодій може бути забезпечений тільки шляхом аналізу всього вмісту мережевих пакетів, включаючи їхні заголовки й області даних.

2 АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ МОДИФІКОВАНОЇ ХЕШ-ФУНКЦІЇ MD5

2.1 Структура модифікованої хеш-функції MD5

Криптографічні методи забезпечують не лише конфіденційність, але і контроль цілісності даних, що передаються або зберігаються. Контроль цілісності в основному здійснюється шляхом розрахунку деякої "контрольної суми" даних. Математиками та інженерами, що працюють в області передачі даних і теорії кодування розроблено безліч алгоритмів, що розраховують контрольні суми даних, що передаються. Для багатьох випадків простої контрольної суми (наприклад, відомого алгоритму crc32 чи послідовного побайтно або послівного додавання вихідного тексту з відомою константою) її вистачає для роботи, особливо тоді, коли хороша швидкість обробки даних і не відомий наперед обсяг даних (типовий випадок — передача даних по каналах зв'язку) [5].

Проблема простих алгоритмів обчислення контрольної суми полягає в тому, що досить легко підібрати кілька масивів даних, що мають однакову контрольну суму. Криптографічно стійкі контрольні суми обчислюються як результат застосування до вихідного тексту хеш-функції.

Однією із гіпотез теорії складності і теорії функцій є гіпотеза про існування однобічних функцій. Під однобічною функцією розуміють функцію, яка визначена (наприклад) на безлічі натуральних чисел і не потребує для обчислення свого власного значення великих обчислювальних ресурсів. Проте, обчислення зворотної функції (тобто за відомим значенням функції відновити значення аргументу) виявляється неможливо чи теоретично (у крайньому випадку) неможливо обрахувати [6].

Загальне існування односторонніх функцій поки не доведено. Тому, всі хеш-функції, що використовуються на даний час, є лише "кандидатами" в односторонні функції, хоча і мають досить хороші властивості. Основними

властивостями криптографічно "стійкої" хеш-функції є властивість розсіювання, властивість стійкості до колізій і властивість необоротності.

Колізією хеш-функції H називається ситуація, при який існують два різних тексти T1 і T2, але H(T1) = H(T2). Значення хеш-функції завжди має фіксовану довжину, а на довжину вихідного тексту не накладається ніяких обмежень. Звідси можна зробити висновок, що колізії існують. Вимога стійкості до колізій означає, що для криптографічно "стійкої" хеш-функції для заданого тексту T1 неможливо знайти текст T2, що викликає колізію.

Властивість розсіювання вимагає, щоб мінімальні зміни тексту, що підлягає хешуванню, викликали максимальні зміни в значенні хеш-функції.

Основними алгоритмами, що застосовуються на сьогоднішній день алгоритмами, які реалізують хеш-функції є MD2, MD4, MD5, HAVAL, SHA-1 і його варіант SHA-2, російський алгоритм, що описується в стандарті ДСТ Р 34.11-94. Найбільш часто використовуються MD5, SHA-1. Довжина значення хеш-функції різна. Типовою довжиною є 16—32 байта. Проте, багато досліджень у застосуванні хеш-функції, стверджують, що прийдеться відмовитися від MD5, тому що, як було виявлено, "його стійкість до колізій знизилась і, напевно, підійшла близько до тієї оцінки, після якої про стійкість взагалі говорити не приходиться" [6].

Хеш-функції — це функції, математичні чи інші, які одержують на вхід змінну довжину і перетворюють її у фіксовану довжину, звичайно, меншої довжини (значення хеш-функції). Просту хеш-функції можна розглядати як функцію, що одержує змінну довжину і повертає байт, який є результатом операцій XOR всіх вхідних байтів.

Зміст хеш-функції представляє собою одержання характерної ознаки змінної довжини — значення, за яким аналізуються різні вхідні повідомлення при рішенні зворотньої задачі. Оскільки, хеш-функція є співвідношенням "багато до одного", неможливо з усією визначеністю сказати, що два рядки збігаються, але їх можна використовувати, одержуючи прийнятну оцінку точності.

Однонапрямлена хеш-функція — це хеш-функція, що працює тільки в одному напрямку: легко обчислити значення хеш-функції за вхідним повідомленням, але важко відновити вхідне повідомлення, значення хеш-функції якого дорівнює заданій величині. Згадувані раніше хеш-функції не є однонапрямленими: задавши конкретний байт, не представляє великих затрат створити рядок байтів, XOR яких дає задане значення.

Хеш-функція є відкритою. Безпека однонапрямленої хеш-функції полягає саме в її однонапрямленості. На виході немає видимої залежності від входу. Зміна одного біту вхідного повідомлення призводить до зміни, в середньому, половини бітів значення хеш-функції. Неможливо знайти таке вхідне повідомлення, що відповідає заданому значенню хеш-функції.

Якщо потрібно перевірити ідентичність файлу, необхідно послати значення хеш-функції. Якщо значення хеш-функції збігається, то файли вважаються ідентичними. Це особливо корисно при фінансових транзакціях, коли захищають електронну комерцію, щоб замість зняття з рахунку $100 не зняли $1000. В звичайних умовах можна використовувати однонапрямлену хеш-функцію без ключа, для того, щоб будь-хто міг перевірити значення хеш-функції. Якщо потрібно, щоб перевірку значення хеш-функції міг здійснювати тільки один одержувач, то для цього використовуються методи наведені нижче.

Код перевірки дійсності повідомлення (message authentication code (MAC)), відомий також як код перевірки дійсності даних (data authentication code (DAG)), це є однонапрямлена хеш-функцію з додаванням секретного ключа. Значення хеш-функції є функцією від вхідного повідомлення і ключа. Особливості застосування ті, що і для хеш-функцій, але тільки той, хто знає ключ, може перевірити значення хеш-функції. MAC можна створити за допомогою хеш-функції чи блокового алгоритму шифрування, існують також і спеціалізовані MAC [6].

Однонапрямлена функція $H(M)$ застосовується до повідомлення довільної довжини M і повертає значення фіксованої довжини h, $h = H(M)$, де h має

довжину *m*. Багато функцій дозволяють обчислювати значення фіксованої довжини по вхідних даних довільної довжини, але в однонапрямлених хеш-функцій є додаткові властивості, які роблять їх однонапрямленими.

Знаючи *M*, можна легко обчислити *h*. Знаючи *H*, важко визначити *M*, для якого *H*(*M*)=*h*. Знаючи *M*, важко визначити інше повідомлення, *M'*, для якого *H*(*M*)= *H*(*M'*). Довжина 64-бітових хеш-функцій є занадто малою, щоб протистояти розкриттю методом дешифрування. Більш практичні однонапрямлені хеш-функції, що видають 128-бітові хеш-значення. При цьому, щоб знайти два документи з однаковими хеш-значеннями, для розкриття методу дешифрування прийдеться хэшувати 2^{64} випадкових документів, що не характеризує її стійкою до атак. NIST у своєму стандарті безпечного хешування (Secure Hash Standard (SHS)), використовує 160-бітове хеш-значення. Це ще більше ускладнює розкриття методу дешифрування, для якого знадобиться 2^{80} хешувань.

Після деякої первісної обробки MD5 обробляє вхідний текст 512-бітовими блоками, розбитими на 16 32-бітових підблоків. На виході алгоритму буде набір з чотирьох 32-бітових блоків, що з'єднується в єдине 128-бітове хэш-значення. По-перше, повідомлення доповнюється так, щоб його довжина була на 64 біта коротшою за числа, кратні 512. Цим доповненням є 1, за якою до кінця повідомлення ставляться нулі (скільки потрібно). Потім, до результату додається 64-бітове представлення довжини повідомлення. Ці дві дії служать для того, щоб довжина повідомлення була кратна 512 бітам (що потрібно для частини алгоритму, що залишилася) і щоб гарантувати, що різні повідомлення не будуть виглядати однаково після доповнення. Ініціалізуються чотири змінних:*A* = 0x01234567, *B* = 0x89abcdef, *C* = 0xfedcba98, *D* = 0x76543210. Вони називаються змінними зчеплення.

Розглянемо основного циклу алгоритму. Цей цикл продовжується виконуватися, поки не вичерпаються 512-бітові блоки повідомлення. Чотири змінних копіюються в інші змінні: *A* в *a*, *B* в *b*, *C* в *c* і *D* в *d*.

Головний цикл складається з чотирьох дуже схожих етапів. На кожному етапі 16 разів використовуються різні операції. Кожна операція є нелінійною функцією над трьома змінними з *a*, *b*, *c* і *d*. Потім вона додає цей результат до четвертої змінної, підблоку тексту і константи. Далі результат циклічно зсувається вправо на змінне число бітів і додає результат до однієї із змінних *a*, *b*, *c* і *d*. Нарешті результат заміняє одну із змінних *a*, *b*, *c* і *d*. Існують чотири нелінійних функції, що використовуються на кожному етапі для обчислення алгоритму (для кожного етапу - інша функція).

Ці функції розроблені таким чином, щоб відповідні біти *X*, *Y* і *Z* були незалежні і незміщені, а кожен біт результату також був би незалежним і незміщеним. Функція F — це побітова умова: якщо *X*, то *Y*, інакше *Z*. Функція H —побітова операція парності.

Якщо M_j означає j-ий підблок повідомлення (від 0 до 15), а $<<<s$ означає циклічний зсув вліво на *s*-бітів, то використовуються наступні чотири операції:

FF(a,b,c,d,M_j,s,t_i) означає $a = b + ((a + \mathrm{F}(b,c,d) + M_j + t_i) <<< s)$

GG(a,b,c,d,M_j,s,t_i) означає $a = b + ((a + \mathrm{G}(b,c,d) + M_j + t_i) <<< s)$

HH(a,b,c,d,M_j,s,t_i) означає $a = b + ((a + \mathrm{H}(b,c,d) + M_j + t_i) <<< s)$

II(a,b,c,d,M_j,s,t_i) означає $a = b + ((a + \mathrm{I}(b,c,d) + M_j + t_i) <<< s)$.

Вище наведені константи t_i вибиралися наступним чином:

На *i-ому* етапі t_i є цілою частиною 2 32 *abs(sin(*i*)), де *i* виміряється в радіанах. Після всього цього *a*, *b*, *c* і *d* додаються до *A*, *B*, *C* і *D*, відповідно, і алгоритм продовжується для наступного блоку даних. Остаточним результатом служить об'єднання *A*, *B*, *C* і *D*:

Модифікація алгоритму MD5 — одностороння хеш-функція змінної довжини [7]. Повідомлення опрацьовується блоками по 1024 біт. Це вдвічі більше, ніж в MD5. Використовується вісім 32-бітні змінні зчеплення і змінна кількість етапів від трьох до п’яти, в кожному етапі є 16 дій. Функція може видавати хеш-значення довжиною 126, 160, 192, 224, 256 бітів. Розглянемо модифікацію алгоритму MD5, що використовує три етапи стиснення (256 біт).

Для цього на вхід подається 1024-бітне повідомлення $M = (m_0, m_2, \ldots, m_{31})$ і на виході отримуємо 256 бітне значення. Процес стиснення відбувається наступним чином:

1. Нехай $(aa, bb, cc, dd, ee, ff, gg, hh)$ буде 256-бітним значенням. Ініціалізуємо змінні (a, b, c, d, e, f, g, h) як $(aa, bb, cc, dd, ee, ff, gg, hh)$.

2. Формуємо наступні 96 кроків (оскільки кожний етап має по 32 кроки):

для $i = 0,1,2$
для $j = 0 \ldots 31$
$p = f_{i+1}(g, f, e, d, c, b, a)$
$r = (p >> 7) + (h >> 11) + m_{i,j} + k_{i,j}$
$h = g$
$g = f$
$f = e$
$e = d$
$d = c$
$c = b$
$b = a$
$a = r$

В кожному етапі використовується константа $k_{j,i}$. Символ “>>” означає циклічний зсув вправо. Перестановка повідомлення на кожному етапі описується в [5]. Функції f_1, f_2, f_3 визначаються наступним чином:

$$f_1(g, f, e, d, c, b, a) = cd \oplus ag \oplus bf \oplus ce \oplus e,$$
$$f_2(g, f, e, d, c, b, a) = adf \oplus bcf \oplus ef \oplus ef \oplus ac \oplus df \oplus bd \oplus bc \oplus fg \oplus g,$$
$$f_3(g, f, e, d, c, b, a) = def \oplus cf \oplus be \oplus dg \oplus ad \oplus a$$

3. Змінні a, b, c, d, e, f, g, h додаємо до вхідних значень.

4. 4. $H(M) = hh \| gg \| ff \| ee \| dd \| cc \| bb \| aa.$

Основні властивості функції f_1 описуються в [7].

2.2 Особливості застосування хеш-функції в комп’ютерних системах

Роль інформації на сьогодні настільки велика, що інформаційна індустрія стала однією із провідних галузей дослідження, а пристрої, що одержали поширення для обробки цифрових даних – комп'ютери – є одним із символів нашої цивілізації. Інформація, представлена у різних формах, подібно іншим товарам виробляється, зберігається, транспортується до споживача, продається, купується, нарешті споживається, застаріває, псується, і т.д. Протягом життєвого циклу інформаційні масиви можуть піддаватися різним небажаної для їхнього споживача впливам, проблемам боротьби з якими стає непередбаченою.

Через те, що інформація має нематеріальний характер, масиви даних не несуть на собі ніяких відбитків, за якими можна було б судити про їхнє минуле — про те, хто є автором, про час створення, про факти, відомості про тих, хто вносить зміни. Модифікація інформаційного масиву не залишає відчутних слідів на ньому і не може бути виявлена звичайними методами. “Сліди модифікації” у тій чи іншій формі можуть бути присутніми тільки на матеріальних носіях інформації – так, як спеціальна експертиза цілком здатна встановити, що сектор X на деякій дискеті був записаний пізніше всіх інших секторів з даними на цій же доріжці дискети, і цей запис вироблявся на іншому дисководі. Зазначений факт, будучи встановленим, може, наприклад, означати, що в дані, збережені на дискеті, були внесені зміни. Але після того, як ці дані будуть переписані на інший носій, їхньої копії вже не будуть містити ніяких слідів модифікації. Реальні комп'ютерні дані за час свого життя багаторазово змінюють фізичну основу представлення і постійно кочують із носія на носій. Оскільки створення й

використання інформаційних масивів практично завжди розділені в часі чи в просторі, у споживача завжди можуть виникнути обґрунтовані сумніви в тому, що отриманий ним масив даних створений потрібним джерелом і при тій точності такий, яким він дійшов до нього.

Таким чином, у системах обробки інформації, окрім забезпечення її таємності, важливим є гарантувати наступні властивості для кожного масиву даних, що обробляється:

– дійсність – він прийшов до споживача саме таким, яким був створений джерелом і не піддавався на своєму життєвому шляху несанкціонованим змінам;

– авторство – він був створений саме тим джерелом, яким є споживач.

Забезпечення системою обробки цих двох якостей масивів інформації і складає задачу їх аутентифікації, а відповідна здатність системи забезпечити надійну аутентифікацію даних називається її автентичністю.

На перший погляд може здатися, що дана задача визначається простим шифруванням. Дійсно, якщо масив даних шифрується із використанням стійкого шифру, такого, наприклад, як ДСТУ 28147–89, то для нього практично завжди буде справедливо наступне:

– у нього важко вносити зміни зрозумілим чином, особливо зі ступенем імовірності, що відрізняється від одиниці, факти модифікації зашифрованих масивів даних стають очевидними після їхнього дешифрування – ця очевидність виражається в тому, що такі дані перестають бути коректними для їхнього інтерпретатора: замість тексту російською мовою з'являється погана копія, архіватори повідомляють, що цілісність архіву порушена і т.д.;

– тільки ті користувачі системи, які володіють секретним ключем шифрування, можуть виготовити зашифроване повідомлення, таким чином, якщо до одержувача приходить повідомлення, зашифроване на його секретному ключі, він може бути впевненим у його авторстві, тому що крім нього самого тільки законний відправник міг створити це повідомлення.

Використання шифрування в системах обробки даних саме по собі

незручне, забезпечується його автентичність по наступних причинах:

1. Зміни, які були внесені в зашифровані дані, стають очевидними після дешифрування тільки у випадку великої надмірності вихідних даних. Ця надмірність має місце, наприклад, якщо масив інформації є текстом на будь-якої людської мови. Проте, у загальному випадку ця вимога може не виконуватися – якщо випадкова модифікація даних не робить їх неприпустимими для інтерпретації. Якщо говорити мовою криптології, то автентичність і таємність несуть різні властивості криптосистем. Якщо більш просто: властивості систем обробки інформації забезпечують таємність і дійсність даних, що обробляються, у загальному випадку можуть не збігатися.

2. Факт успішного дешифрування зашифрованих даних за допомогою секретного ключа може підтвердити їхнє авторство тільки для самого одержувача. Третя сторона не зможе зробити на підставі цього однозначного висновку про авторство масиву інформації, тому що його автором може бути кожний із власників секретного ключа, а їх як мінімум два – відправники й одержувач. Тому в даному випадку суперечки про авторство повідомлення не можуть бути дозволені незалежним арбітражем. Це важливо для тих систем, де між учасниками немає взаємної довіри, що дуже характерно для банківських систем, що зв'язані із керуванням над значними цінностями.

Таким чином, існування проблеми підтвердження дійсності й авторства масивів даних, окремої від задачі забезпечення їхньої таємності, не викликає сумніву.

2.3 Оцінка стійкості хеш-функції

Є багато методів, що дозволяють підвищити крипостійкість системи, серед них блок хешування паролів – метод, що дозволяє користувачам

запам'ятовувати не 128 байт, тобто 256 цифр ключа, а деяке осмислене вираження певної величини, чи послідовності символів, що називається паролем. При розробці будь-якого криптоалгоритму потрібно враховувати, що в більшості випадків кінцевим користувачем системи є людина, а не автоматична система. Тоді виникає питання про те чи це є зручно, і взагалі чи реально людині запам'ятати 128-бітний ключ (32 цифри). Проте, межа запам'ятовування лежить в межах від 8-12 подібних символів. Тому, якщо змушувати користувача оперувати самим ключем, тим самим він буде змушений записати його на якому-небудь листку і електронному носії, наприклад, у текстовому файлі. Це різко знижує захищеність системи [8].

Для вирішення цієї проблеми були розроблені методи, що перетворюють вимовний, осмислений рядок довільної довжини — пароль, у зазначений ключ заздалегідь заданої довжини. У переважній більшості випадків для цієї операції використовують хеш-функцію (від англ. hashing – дрібна нарізка і перемішування). Хеш-функцією називається таке математичне чи алгоритмічне перетворення заданого блоку даних, що має наступні властивості:

1) хеш-функція має нескінченну область визначення,
2) хеш-функція має кінцеву область значень,
3) вона необоротна,
4) зміна вхідного потоку інформації на один біт змінює близько половини всіх бітів вихідного потоку, тобто результату хеш-функції.

Ці властивості дозволяють подавати на вхід хеш-функції паролі, тобто текстові рядки довільної довжини на будь-якій мові і, обмеживши область значень функції діапазоном $0..2^N-1$, де N – довжина ключа в бітах, що дозволяє одержувати на виході достатньо рівномірно розподілені по області значення блоків інформації – ключі.

Вище зазначені вимоги до хеш-функції виконують блокові шифри. Це вказує на один із можливих шляхів реалізації стійких хеш-функцій – проведення блокових криптоперетворень над рядком-пароля. Цей метод і використовується

в різних варіаціях практично у всіх сучасних криптосистемах. Матеріал “рядка-пароля” багаторазово послідовно використовується як ключ для шифрування деякого заздалегідь відомого блоку даних – на виході отримуємо зашифрований блок інформації, який однозначно залежний тільки від пароля і, при цьому має досить позитивні статистичні характеристики. Такий блок і використовується як ключ для подальших криптоперетворень.

Характер застосування блокового шифру для хешування визначається відношенням розміру блоку, що використовується для даного криптоалгоритму і розрядністю необхідного хеш-результату.

Якщо зазначені вище величини збігаються, то використовується схема блокового шифрування. Первісне значення хеш-результата H_0 встановлюється рівним 0, весь рядок-пароль розбивається на побайтові блоки, які рівні по довжині ключу, що використовується для хешування блокового шифру, потім здійснюються перетворення за рекурентною формулою:

$$H_j=H_{j-1} \text{ XOR } EnCrypt(H_{j-1},PSW_j), \qquad (2.1)$$

де $EnCrypt(X,Key)$ — блочний шифр, що використовується.

Останнє значення H_k використовується як шуканий результат.

На рисунку 2.1 зображено розробку хешування, де f – функція хешування, X_i – текст, IV –ініціалізуючий вектор (ключ), D – шифротекст.

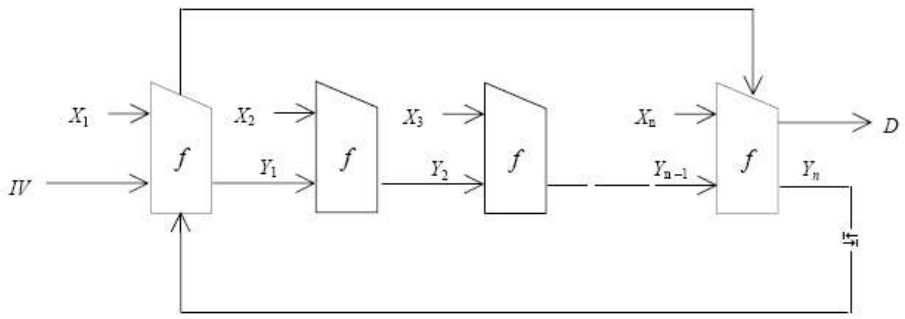

Рисунок 2.1 — Хешування повідомлення з використанням ключа IV

У тому випадку, коли довжина ключа, приблизно в два рази перевищує довжину блоку, а подібна залежність досить часто зустрічається в блокових шифрах, використовується схема, що нагадує мережу Файстеля [6]. Характерним недоліком хеш-функції, що базується на мережі Файстеля, є велика потреба у збільшенні розміру ключа.

Для проведення тільки одного перетворення, наприклад, блоковим шифром із ключем довжиною 128 біт використовується 16 - байтний рядок-пароля, а сама довжина пароля рідко перевищує 32 символів. Отже, при обчисленні хеш-функції, над паролем будуть здійснюватися максимум 2 "повноцінних" криптоперетворення.

Цю проблему можна вирішити двома шляхами:

1) попередньо "розмножити" рядок-пароль, наприклад, записавши його багаторазово послідовно до тих пір, поки не буде досягнено необхідної довжини, наприклад, у 256 символів;

2) модифікувати схему використання криптоалгоритму так, щоб матеріал рядок-пароля "повільніше" витрачався при обчисленні ключа.

Оскільки, традиційне шифрування забезпечує аутентифікацію і таке шифрування можна здійснити за допомогою вже доступних засобів, що знаходяться у широкому використанні. Є ряд програм, в яких одне і те ж повідомлення може передаватися кільком адресатам. Прикладом може бути повідомлення користувача про те, шо мережа в даний момент є недоступною, або сигнал тривоги, що надходить із центрального військового штабу. Дешевше і надійніше мати одного адресата, що відповідає за перевірку автентичності. При такому підході повідомлення передається у відкритому вигляді разом із відповідним кодом автентичності. Система, що відповідає за перевірку автентичності повинна мати секретний ключ і виконувати таку перевірку. Якщо буде знайдено порушення, інші системи-адресати попереджаються про небезпеку сигналом загальної небезпеки.

Дослідники Девіс і Майєр цю проблему розглянули по іншому. Вони

запропонували алгоритм також на основі блокового шифру, але матеріал в якості рядка-пароля, що використовується є невеликим [9]. У ньому проглядаються елементи, які характерні і для вище описаних (ДП.КСМ.07103/14.00.00.000 С1), але крипостійкість цього алгоритму підтверджена численними реалізаціями в різних криптосистемах. Алгоритм одержав назву "Tandem DM":

G_0=0; H_0=0 ;
FOR J = 1 TO N DO
BEGIN
$TMP=EnCrypt(H,[G,PSW_j])$; $H'=H$ XOR TMP;
$TMP=EnCrypt(G,[PSW_j,TMP])$; $G'=G$ XOR TMP;
END;
$Key=[G_k,H_k]$

Захист цілісності повідомлень, побітове шифрування потоку даних — це системи шифрування, які найбільш вразливі до атак на зміну вихідного тексту. Якщо вихідний текст частково відомий зловмиснику, то модифікація бітів тексту реалізується дуже просто, шляхом інвертування бітів шифрованого тексту в тих місцях, де потрібна інверсія бітів вихідного. Така модифікація цілком реальна над фінансовим повідомленням, що включає, наприклад, номінали, число і номер купюр.

Якщо повідомлення містить тільки кілька контрольних знаків, вони можуть бути також змінені, оскільки всі біти, що беруть участь в обчисленні цих знаків, відомі. Це виявляється можливим незалежно від виду функції перевірки надмірності (лінійна чи нелінійна). Звичайно, зловмиснику необхідно знати цю функцію, і він може її знати, оскільки функція перевірки не є секретною. Це означає, що зашифровані контрольні знаки, що використовуються в звичайних протоколах передачі по лініях зв'язку, — символ контролю блоку BCC (Block Check Character) і контроль за допомогою циклічного надлишкового коду CRC

(Cyclic Redundancy Check), не можуть допомогти одержувачу виявити маніпуляції з повідомленням, оскільки зловмисник може легко обчислити їхнє значення. Варто зазначити, що підтвердження дійсності повідомлення в таких системах вимагає спеціального механізму з секретними елементами, наприклад, кодом дійсності MAC (Message Authentication Code). Побітове шифрування потоку зі зворотнім зв'язком шифрування. Для багатьох реалізацій таких систем характерне явище безупинного поширення помилки, яке означає, що зловмисник не в змозі контролювати вихідний текст, що буде відновлюватися після навмисної зміни хоча б одного біта. Виключення складає ситуація, коли змінюваним є останній біт повідомлення.

Усі види контролю на надмірність будуть працювати як засіб виявлення помилкових повідомлень. В інших випадках можливо обмежене поширення помилки, наприклад, у межах 64 біт у випадку DES-алгоритму. Поки виконується контроль по надмірності, що може виявити зміни принаймні в кожному 64-му біті, наприклад, з використанням символу контролю блоку BCC, то цього є достатньо, оскільки зловмиснику нічого не залишається, окрім варіанту випадкового вгадування.

Існують реалізації, коли поширення помилки не виходить за межі одного біта. Не знаючи, як біт зворотнього зв'язку впливає на дешифрування наступного біта, зловмисник вважає, що події "біт змінений" і "біт не змінений" мають однакову імовірність (50%) [10]. Якщо наприкінці повідомлення використовується символ контролю блоку BCC, то зловмисник може модифікувати його. Вплив зворотнього зв'язку і модифікації символу контролю блоку BCC на наступний блок однаковий і складає як і раніше 50%. Кожна зміна біта в одному чи декількох символах BCC зменшує ефективність успішного контролю на 50%. Контроль за допомогою циклічного надлишкового коду CRC або іншого нелінійного методу, при умові, що зміна одного біта впливає на кілька контрольних символів, створює для зловмисника несприятливу ситуацію.

У цьому випадку найкращою стратегією для зловмисника було б виявити ті

зміни, що зачіпають лише обмежене число бітів надлишкового коду CRC. DES-алгоритм у режимі 8-бітового шифрування зі зворотним зв'язком має ті ж властивості, що й у режимі побітового шифрування. Можливо, 64-бітове шифрування з ОС має істотно інші властивості. Оскільки в цьому випадку побітове шифрування поширюється на кожен 64-бітовий блок, можливі маніпуляції на рівні блоку чи вставки або видалення блоку можуть бути виявлені. При відомому вихідному тексті можна виконати зміну останнього блоку, що містить значення контрольних функцій (символу контролю блоку BCC чи циклічного надлишкового коду CRC), щоб змінити значення контрольної функції. Додавання блоків за модулем 2 або додавання символу контролю блоку BCC не змінюють значення контрольної функції, якщо зловмисник тільки переставляє блоки повідомлення місцями.

У випадку побітового шифрування зі зворотнім зв'язком за вихідним текстом поширення внесених помилок залежить від того, як біти повідомлення впливають на роботу генератора випадкових чисел. Якщо цьому впливу піддається тільки наступний біт, то імовірність правильного дешифрування зменшується на 50% посилання кожного неправильного дешифрованого біта. Таким чином, дешифрування буде правильним тільки за умови, коли не вводяться помилки. Це означає, що зловмисник не в змозі контролювати повною мірою всі зміни, які він вводить, і це, звичайно, справедливо стосовно модифікації контрольних символів. Навіть при використанні найпростішої контрольної функції — символу контролю блоку BCC - він буде мати 50% -ний шанс на успіх. Використання більш складних функцій контролю істотно знижує ефективність вторгнення.

Проте, існує можливість, що такі системи мають більш широку область поширення помилки (і навіть необмежену). Якщо існують функції перевірки для вихідного тексту, то введення в нього нерозпізнаних змін неможливо. Нелінійні властивості процедур поблочного шифрування не дозволяють зловмиснику модифікувати блок вихідного тексту (чи байт-символ), навіть якщо йому відомо

саме вихідне повідомлення. Оскільки, зміни вихідного тексту в результаті поблочного шифрування прочитати неможливо, то зловмисник не знає, як зміняться контрольні цифри, але навіть якщо він знає, то не може здійснити бажаних змін. В результаті такі системи забезпечують високий степінь захисту від модифікацій.

У випадку поблочного шифрування потоку зі зворотнім зв'язком (ЗЗ) область поширення помилки буде складати наступний блок, а в багатьох системах і значно більше. Степінь захисту від можливих модифікацій буде вища, ніж у попередньому випадку. Область поширення помилки обмежена розмірами блоку шифрованого тексту, проте передбачати ефекти змін всередині блоку неможливо. Проте незалежність блоків дозволяє проводити маніпуляції на рівні блоку.

Будь-який криптографічний алгоритм може бути реалізований у вигляді відповідної програми. Програмними засобами захисту інформації називаються спеціально розроблені програми, що реалізують функції безпеки обчислювальної системи, здійснюють функцію обмеження доступу користувачів по паролях, ключах, багаторівневому доступу і т.д. Як правило, ці програмні засоби забезпечують досить високий степінь захисту системи і мають помірні ціни. При підключенні такої системи в глобальну мережу імовірність злому захисту збільшується.

Отже, цей спосіб захисту був прийнятий для локальних замкнутих мереж операційних систем сімейства Windows, що не мають зовнішнього виходу. Переваги такої реалізації очевидні: програмні засоби шифрування легко копіюються, вони прості у використанні, їх неважко модифікувати відповідно до конкретних потреб. Швидкодія в них достатня для забезпечення потреб локальної мережі.

3 РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ

3.1 Вибір мови програмування

Для розробки програмного комплексу було обрано мову програмування Borland C++, яка відрізняється якістю генерації програмного коду, що забезпечує швидке виконання створених з її допомогою програм, хорошу переносимість їх та, при всіх вищезгаданих перевагах, невеликі розміри. Також Borland C++ дозволяє створювати програми з використанням об’єктно-орієнтованого програмування, яке є одним з найновітніших досягнень у розвитку мов програмування високого рівня.

Об’єктно-орієнтоване програмування (ООП) — це програмування, що сфокусоване на даних, при чому дані і поведінка тісно пов’язані між собою. Разом дані і поведінка являють собою клас, а об’єкти є екземплярами класу. Наприклад, многочлен має область значень, і вона може змінюватися такими операціями, як додавання і множення многочленів.

ООП розглядає обчислення, як моделювання поведінки. Те, що моделюється, є об’єктами, що представлені обчислювальною абстракцією. В ООП об’єкти відповідають за свою поведінку. Наприклад, многочлени, комплексні числа, цілі числа, числа з плаваючою комою — все це об’єкти, що “розуміють” операцію додавання. Кожен з цих типів включає в себе код для виконання операції додавання.

До поняття ООП має відношення ціла група концепцій, яка включає наступні:

- моделювання дій з реального світу;
- наявність типів даних, які описує користувач;
- приховування деталей реалізації;
- можливість багатократного використання коду завдяки наслідуванню;
- інтерпретація викликів функцій на етапі виконання.

Деякі з цих понять досить розмиті, деякі — абстрактні, інші мають загальний характер.

Об’єктно-орієнтована парадигма пропонує новий підхід до розробки програмного забезпечення, яке призначене для розв’язку задач різних класів. Фундаментальна концепція об’єктно-орієнтованої парадигми полягає в передачі повідомлень об’єктам. Для цього необхідно, щоб об’єкти описувалися разом з повідомленнями, на які вони будуть реагувати, на відміну від процедурного програмування, де спочатку визначається структура даних, котрі будуть передаватися в процедури як параметри.

Існує п’ять компонентів об’єктно-орієнтованої парадигми: об’єкт, повідомлення, клас, наслідування і метод. Ці компоненти дуже сильно залежать одне від одного, причому кожен з них визначається в термінах інших. Для того, щоб зрозуміти один компонент, необхідно зрозуміти їх всі. Об’єктно-орієнтована мова програмування повинна володіти властивостями абстракції, інкапсуляції, наслідування і поліморфізму. Окрім того, об’єктно-орієнтованій мові бажано мати можливості розширення, повторного використання програмних компонент, а також параметризації [9].

Об’єктно-орієнтоване програмування дозволяє вирішувати проблеми будь-якого рівня складності. Це забезпечується шляхом розбиття однієї складної задачі на велику кількість простих, які тісно пов’язані між собою. Якщо програміст буде впевнений у правильності вирішення всіх простих задач (а цю правильність для простої задачі легше перевірити, ніж для складної), а також у коректності зв’язків між простими об’єктами, він може бути впевненим у коректності розв’язку глобальної (основної) задачі.

Компілятор Borland C++ надає потужну базу для розробки об’єктно-орієнтованих програм. Надзвичайно потужний синтаксис та оптимальний код, створюваний компілятором роблять його використання ефективним для вирішення більшості задач, що постають перед програмістами сьогодні.

Надійність і швидкість обробки інформації програмою багато в чому

залежать від якості проектування методів доступу до даних системи і зв'язків між окремими інформаційними одиницями.

C++ — це тісний союз програмування на низькому і високому рівні. C був розроблений як системна мова, близька до машинної. C++ доповнена об'єктно-орієнтованими властивостями, які дозволяють програмісту створювати чи імпортувати бібліотеки, які притаманні для конкретної задачі. Користувач може написати код на проблемному рівні, в той же час підтримуючи контакт з машинним рівнем реалізації деталей.

Вибрана мова програмування спрощує розв'язання задачі, дозволяючи зосередитися на даних, проте в будь-який момент можна повернутися до машинного коду. Це дуже важливий аспект, враховуючи складність поставлених задач.

3.2 Опис основних модулів програмного комплексу

Для реалізації модифікованої хеш-функції MD5 були підключені методи інтерфейсу CryptoAPI. Криптографічний інтерфейс прикладного програмування (CryptoAPI) — це набір функцій, які можна викликати з програм на мові C. Він дозволяє використовувати криптографічні функції для побудови власної програми. CryptoAPI передбачає три набори функцій:

—сертифікаційні функції;

—спрощені криптографічні функції;

—базові криптографічні функції.

Сертифікаційні функції — це засоби вилучення, збереження і перевірки сертифікатів цифрових підписів, які можуть супроводжувати ряд документів і сертифікати, що зберігаються на комп'ютері [10].

Спрощені криптографічні функції включають в себе функції високого

рівня для створення ключів, шифрування та дешифрування інформації.

Базові криптографічні функції розташовані на нижчому рівні, їх бажано уникати, оскільки їхній виклик може призвести до конфліктів, що пов'язані з видаленням із системи деяких компонентів.

Програмний пакет CryptoAPI складається з двох рівнів:

1) рівень зв'язку з програмами, що призначений для виклику функції API;

2) рівень доповнень (розташовується після першого рівня) є відкритим і призначений для поновлення і включення нових функцій у вигляді вбудованих компонентів (plug in), в тому числі і тих, що розробляються програмістами.

Структура CryptoAPI зображена на ДП.КСМ.07103/14.00.00.001.С1.

CryptoAPI забезпечує передачу повідомлень між програмами і провайдерами служби шифрування. Вбудований компонент такого типу, що реалізує алгоритму шифрування називається провайдером служби шифрування — Cryptographic Service Provider (CSP) або криптографічним сервером. В зображеній структурі (див. рисунок 3.1) використовуються функції передачі повідомлення між програмами і вибраними для операційної системи Windows програми криптосервера CSP.

Криптографічний сервер (CSP) — це сервер, що може виконувати стандартний набір задач, що ініціюються викликом функцій CryptoAPI. Типовий CSP (Cryptographic Service Provider) складається з DLL і файлу підписів, що використовує CryptoAPI для перевірки цілісності та ідентифікації користувачів, що звертаються до сервера. Таким чином, CSP — це змінний модуль програмного забезпечення. Він нагадує драйвери ОС Windows. Можливість використання CSP виникає одразу після його реєстрації, при цьому не потрібно вносити зміни на рівні ОС.

Для того, щоб забезпечити конфіденційність, всі дані, якими маніпулює CSP (особливо ключі), повертаються у викликану програму у формі дескрипторів і залишаються недоступними на рівні ОС. Окрім того, програмне забезпечення не впливає на метод криптоперетворення даних. Роль програми обмежується

передачею даних серверу і вказанням необхідного типу перетворення. Різні сервери можуть використовувати однакові алгоритми, але при цьому приймають різну логіку заповнення і різні розміри ключів [11].

CryptoAPI використовує базу даних ключів. Зберігання ключів (key store) — це база даних для зберігання ключів інціалізуючого вектора, що обслуговується компонетном CSP. Ключі, що зберігаються в ній, використовуються в процесі виклику програми. Створення бази даних ключів гарантує функціональність інтерфейсу CryptoAPI.

Кожний криптосервер (CSP) має асоціативну базу даних для ключових контейнерів, яка містить всі приватні і загальні ключі користувачів, що мають доступ до даного комп'ютера. Модель бази даних ключів забражено на рисунку 3.1.

Рисунок 3.1 — Модель бази даних CryptoAPI

Кожний ключовий контейнер має унікальне ім'я. Без бази даних CryptoAPI будь-які виклики CryptoAPI будуть відхилені. База даних, по замовчуванню, містить контейнер з реєстраційними іменами всіх користувачів. Проте, конкретна програма під час встановлення створює спеціальний ключовий контейнер і пари ключів, присвоюючи їм власне ім'я. Оскільки, тип сервера впливає на алгоритми застосування криптографічних функцій, пов'язані між

собою програми повинні користуватися одним CSP.

Фрагмент опису функції, що використовує контейнери ключів виглядає наступним чином:

```
CryptAcquireContext(phProv      :PHCRYPTPROV;
        pszContainer :LPAWSTR;
        pszProvider  :LPAWSTR;
        dwProvType   :DWORD;
        dwFlags      :DWORD) :BOOL; stdcall;
```

Робота з CryptoAPI починається з виклику цієї функції, яка виконує підключення до криптопровайдера і повертає його дескриптор в параметрі phProv. Криптопровайдер — це незалежний програмний модуль (у вигляді dll), що виконує криптографічні алгоритми. В параметрі pszContainer необхідно вказувати ім’я контейнера ключів, який буде використовуватися. Варто зазначити, що кожний криптопровайдер містить базу даних, в якій зберігаються ключі користувачів. Ці ключі групуються в контейнерах. Ключові пари зберігаються для асиметричних алгоритмів, сеансові ключі не зберігаються. Тому, кожний контейнер містить ім’я і ключ, що використовується при хешуванні.

Параметр dwFlags може приймати значення 0 або одне з насптупних:

— CRYPT_VERIFYCONTEXT — прапорець, що призначений для програм, які не повинні мати доступ до закритих ключів контейнера. Такі програми можуть звертатися тільки до хеш-функції. В цьому параметр pszContainer має дорівнювати nil;

— CRYPT_NEWKEYSET — створює новий контейнер ключів, проте самі ключі не створюються;

— CRYPT_DELETEKEYSET — видаляє контейнер разом із ключами, що в ньому зберігаються. Якщо задано цей прапорець, то підключення до

криптопровайдера не відбувається і параметр phProv є невизначеним;

— CRYPT_MACHINE_KEYSET — по замовчуванню контейнери ключів зберігаються як користувацькі. Цей прапорець можна встановлювати в комбінації з іншими, що дозволяє вказати чи є контейнер машинним.

Функція повертає значення true, якщо не було помилки, в іншому випадку — false. GetLastError повертає код помилки.

Функція для створення хеш-функції виглядає наступним чином:

```
CryptCreateHash(hProv   :HCRYPTPROV;
                Algid   :ALG_ID;
                hKey    :HCRYPTKEY;
                dwFlags :DWORD;
                phHash  :PHCRYPTHASH) :BOOL; stdcall;
```

Функція створює в системі хеш-об’єкт і повертає його дескриптор в параметрі phHash. Дані, що надходять на вхід хеш-об’єкта, перетворюються і зберігаються всередині хеш-об’єкта. В параметрі hProv потрібно вказати дескриптор провайдера, що отриманий за допомогою функції CryptAcquireContext.

Параметр Algid вказує на те, що використовується модифікація алгоритму MD5. Параметр dwFlags зарезервований і дорівнює 0.

У випадку успішного виконання функція повертає значення true, в іншому випадку — false. GetLastError повертає код помилки.

Функція знищення хеш-об’єкта, створеного за допомогою CryptCreateHash, виглядає наступним чином:

```
CryptDestroyHash(hHash :HCRYPTHASH) :BOOL; stdcall;
```

В параметрі hHash вказується дескриптор хеш-об’єкта.

Наступна функція дозволяє додавати дані до об’єкта хеш-функції:

```
CryptHashData(hHash       :HCRYPTHASH;
              const pbData      :PBYTE;
                  dwDataLen   :DWORD;
                  dwFlags     :DWORD) :BOOL; stdcall;
```

Функція може викликатися кілька разів. Дані, з яких обчислюється хеш-функція, розбиті на блоки. В параметрі hHash вказується дескриптор хеш-об’єкта, створеного за допомогою CryptCreateHash. Параметр pbData містить вказівники на дані, а dwDataLen — містить розмір цих даних в байтах.

У випадку успішного виконання функція повертає значення true, в іншому випадку — false. GetLastError повертає код помилки.

Функція CryptSignHash обчислює значення підпису від значення хеша:

```
CryptSignHash(hHash       :HCRYPTHASH;
                  dwKeySpec    :DWORD;
                  sDescription :LPAWSTR;
                  dwFlags      :DWORD;
                  pbSignature  :PBYTE;
                  pdwSigLen    :PDWORD) :BOOL; stdcall;
```

В параметрі hHash вказується дескриптор хеш-об’єкта, створеного за допомогою CryptCreateHash. Параметр dwKeySpec вказує який ключ буде використовуватися для підпису. Цей параметр може приймати значення AT_SIGNATURE або AT_KEYEXCHANGE. Ключі повинні знаходитися в контейнері. Параметр sDescription містить довільну стрічку опису. Ця стрічка додається до хеша. Параметр dwFlags дорівнює 0. Параметр pbSignature вказує на буфер, куди розташовується цифровий підпис, а pdwSigLen — розмір цього

буфера. Якщо розмір наперед невідомий, то можна встановити pbSignature рівним nil, і тоді в параметрі pdwSigLen отримаємо необхідний розмір буфера.

У випадку успішного виконання функція повертає значення true, в іншому випадку — false. GetLastError повертає код помилки.

Функція CryptVerifySignature здійснює перевірку підпису:

```
CryptVerifySignature(hHash        :HCRYPTHASH;
                     const pbSignature  :PBYTE;
                         dwSigLen     :DWORD;
                         hPubKey      :HCRYPTKEY;
                         sDescription :LPAWSTR;
                         dwFlags      :DWORD) :BOOL; stdcall;
```

Параметр hHash — дескриптор хеш-об’єкта, значення якого перевіряються. Параметр pbSignature — вказує на буфер, що містить підпис, dwSigLen — розмір цього буфера. Параметр hPubKey — дескриптор відкритого ключа, за допомогою якого здійснюється перевірка підпису. Відкритий ключ має відповідати закритому, який використовувався для створення підпису. Параметр sDescription і dwFlags повинні відповідати параметрам функції CryptSignHash при здійсненні підпису.

У випадку успішного виконання функція повертає значення true, в іншому випадку — false. GetLastError повертає код помилки.

Визначається також і загальний клас HashTable. Цей клас утворюється від базового класу списків List і забезпечує механізм зберігання з дуже ефективними методами доступу. Допускаються дані будь-якого типу з обмеженням, що для цього типу даних має бути визначений оператор «==». Для того, щоб порівняти ключові поля двох елементів даних, програма має перегрузити оператор «==».

Об’єкт типу HashTable — це список елементів типу T (число). В ньому

реалізовані всі методи, які потребують абстрактного класу List. Програма

задає розмір таблиці і хеш-функцію, перетворюючи елемент T в довге ціле беззнакове число. Опис параметру функції за допомогою типу, що заданий в шаблоні, дозволяє використовувати даний клас для хешування даних будь-якого типу:

```
struct NameRecord
{
  String name;
  int count;
};
HashTable<NameRecord> HF(101,hash);
NameRecord rec;
rec.name = "OPT_MD5";
rec.count = 1;
HF.Insert(rec);
cout << HF.ListSize();
rec.name = "Betsy";
if (HF.Find(rec)
{
  rec.cout += 1;
  HF.Update(rec);
}
else
  cerr << "Помилка: \"Ключ OPT_MD5 має бути в таблиці.\"\n;
```

Методи Insert, Find, Delete і ClearList є базовими методами обробки списків. Наприклад, стрічка HF.Insert(rec) дозволяє вставити текст OPT_MD5 в таблицю. Метод HF.Update(rec) служить для обновлення елемента, що вже знаходиться в таблиці.

Методи ListSize і ListEmpty реалізовані в базовому класі. Елемент даних current завжди вказує на останнє доступне значення даних. Він використовується методом Update і довільними класами, які повинні повертати зсилки.

Метод Insert обчислює значення хеш-функції і шукає об'єкт типу LinkedList для того, щоб перевірити чи є такий елемент даних в таблиці. Якщо є, то Insert обновляє цей елемент даних, встановлює на нього вказівник current і повертає керування. Якщо такого елемента немає в таблиці, то Insert додає його в кінець списку, встановлює на нього вказівник current і збільшує розмір списку.

Метод Find використовує хеш-функцію і переглядає список на предмет співпадіння з вхідним параметром:

```
template <class T>
int HashTable<T>::Find(T& key) {
  int hashval = int(hf(key) % NumBuckets);
  LinkedList<T>& lst = buckets[hashval];
  for (lst.Reset(); !lst.EndOfList(); lst.Next())
    if (lst.Data() == key)
    {
      key = lst.Data();
      current = &lst.Data();
      return 1;
    }
  return 0;
}
```

Якщо співпадіння знайдено, метод копіює дані в змінну key, встановлює вказівник current на відповідний вузол і повертає значення true. В іншому випадку метод повертає значення false.

Клас HashTableIterator дозволяє полегшити обробку даних в хеш-таблиці.

Він здійснює перегляд даних в таблиці. Обхід елементів таблиці починається з пошуку непустого блоку в масиві списків. Знайшовши непустий блок, функція переглядає всі вузли цього списку, а потім розглядає наступний блок. Ітератор повинен бути прив'язаний до списку. В даному випадку змінній hashTable присвоюється адреса конкретного екземпляра класу HashTable. Оскільки, клас HashTableIterator є дружнім по відношенню HashTable, то він має доступ до всіх прихованих даних, включаючи масив buckets і його розмір numBuckets.

Змінна currentBucket є індексом зв'язаного списку, який переглядається в даний момент, а currBucketPtr — вказівник цього списку. Обхід кожного блоку здійснюється інтерпретатором, що вбудований в клас LinkedList.

Метод SearchNextNode викликається для виявлення наступного списку, що підлягає обходу. Переглядаються всі блоки, починаючи з cb до тих пір, поки не зустрінеться непустий блок. Змінній currentBucket присвоюється індекс цього списку, а змінній currBucketPtr — його адреса. Якщо немає пустих списків, то функція повертає значення currentBucket = -1.

Конструктор ініціалізує базовий клас Iterator і присвоює прихованому вказівнику hashTable адресу хеш-таблиці:

```
template <class T>
HashTableIterator<T>::HashTableIterator(HashTable<T>& hf):
      Iterator<T>(hf), HashTable(&hf)
{
  SearchNextNode(0);
}
```

Непустий список виявляється за допомогою виклику SearchNextNode з нульовим параметром. За допомогою метода Next здійснюється просування вперед по поточному списку на один елемент. По досягненні кінця списку функція SearchNextNode настроює ітератор на наступний непустий блок.

Розмір хеш-таблиці має бути достатньо великим, щоб в ній залишалося велике число пустих місць. Чим менша таблиця, тим більший середній час пошуку ключів в ній. Хеш-таблицю можна розглядати як сукупність зв’язаних списків. В міру того, як збільшується таблиця, збільшується кількість списків і, відповідно, середнє число вузлів в кожному списку зменшується.

3.3 Результати роботи програмного комплексу

На вхід програми подається файл, в якому міститься повідомлення різної довжини. Програма обчислює хеш функцію від вхідного повідомлення і записує у файл. Для перевірки ідентичності хеш-функції використовуються саморозпаковуючі файли, що мають однакову хеш-функцію (додаток Г). Нижче наведені результати виконання програмного комплексу:

— використовується три етапи (PASS=3) і файл без і з повідомленям (додаток Д). На виході отримується хеш-функція довжиною 128 і 160 біт (FPTLEN):

PASS=3, FPTLEN=128:
OPT_MD5 ("") = 1BDC556B29AD02EC09AF8C66477F2A87
PASS=3, FPTLEN=160:
OPT_MD5 ("a") = 5E1610FCED1D3ADB0BB18E92AC2B11F0BD99D8ED

— використовується чотири етапи (PASS=4):

PASS=4, FPTLEN=192:
OPT_MD5 ("OPT_MD5") =
74AA31182FF09BCCE453A7F71B5A7C5E80872FA90CD93AE4
PASS=4, FPTLEN=224:
OPT_MD5 ("0123456789") =

144CB2DE11F05DF7C356282A3B485796DA653F6B702868C7DCF4AE76

— використовується п’ять етапів:

PASS=5, FPTLEN=256:

OPT_MD5 ("abcdefghijklmnopqrstuvwxyz") =

1A1DC8099BDAA7F35B4DA4E805F1A28FEE909D8DEE920198185CBCAED

8A10A8D

OPT_MD5 ("ABCDEFGHIJKLMWXYZabcdefghijklmnopqrstuvwxyz0123456

789") = C5647FC6C1877FFF96742F27E9266B6874894F41A08F5913033D9D5

32AEDDB39

З вище наведених результатів видно, що від кількості етапів залежить і хеш-функція. При одному і тому ж вхідному повідомленні значення хеш-функції від 3 до 5 етапів буде різним.

Було здійснено перевірку хеш-функції. В результаті чого файли мали ідентичні імена і однаковий вміст.

В подальшому можна досліджувати модифіковану хеш-функцію MD5 на стійкість до колізій.

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

У даному розділі дипломної роботи проводиться економічне обґрунтування доцільності розробки програмного засобу. Зокрема, здійснюється розрахунок витрат на розробку даного програмного забезпечення, експлуатаційних витрат, ціни на споживання проектного рішення, визначаються показники економічної ефективності нового програмного продукту, обґрунтовуються відповідні висновки.

Розроблений програмний засіб призначений для діагностики комп'ютерних систем.

4.1 Розрахунок витрат на розробку програмного забезпечення

Витрати на розробку і впровадження програмних засобів ($К$) включають:

$$К = К_1 + К_2, \quad (4.1)$$

де $К_1$ — витрати на розробку програмних засобів, грн;

$К_2$ — витрати на відлагодження і дослідну експлуатацію програми рішення задачі на комп'ютері, грн.

Витрати на розробку програмних засобів включають:

– витрати на оплату праці розробників ($В_{ОП}$);

– витрати на відрахування у спеціальні державні фонди ($Вф$);

– витрати на покупні вироби ($Пв$);

– витрати на придбання спецобладнання для проведення експериментальних робіт ($Об$);

– накладні витрати (*Н*);

– інші витрати (*Ів*).

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт у людино-днях та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломант; консультант техніко-економічного розділу (таблиця 4.1).

Таблиця 4.1 — Вихідні дані для розрахунку витрат на оплату праці

№ п/п	Посада виконавців	Місячний оклад, грн.
1	Керівник ДП, доцент	5200
2	Консультант техніко-економічного розділу,доцент	5300
3	Студент	1089

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} , \qquad (4.2)$$

де n_{ij} — чисельність розробників *i*-ої спеціальності *j*-го тарифного розряду, осіб;

t_{ij} —затрачений час на розробку проекту співробітником*i*-ої спеціальності *j*-го тарифного розряду, год;

C_{ij} — годинна ставка працівника*i*-ої спеціальності *j*-го тарифного розряду, грн.

Середньо годинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_{i}}, \qquad (4.3)$$

де C_{ij} — основна місячна заробітна плата розробника *i*-ої спеціальності *j*-го тарифного розряду, грн.;

h — коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ - місячний фонд робочого часу працівника*i*-ої спеціальності *j*-го тарифного розряду, год. (приймаємо 168 год.).

Результати розрахунку записуються до таблиці 4.2.

Таблиця 4.2 — Розрахунок витрат на оплату праці

№ п/п	Посада виконавців	Час розробки, год	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн
1	Керівник ДП, доцент	20,5	30,95	634,47
2	Консультант техніко-економічного розділу, доцент	2	31,5	63
3	Студент	240	6,46	1550,4
Разом				2247,87

Величину єдиного соціального внеску визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 16,4% від суми заробітної плати, тобто $B_{Ф} = \frac{20,5}{100} \cdot 2247,\ 87 = 460,8$ грн.

Витрати на використання комп'ютерної техніки включають витрати на амортизацію комп'ютерної техніки, витрати на користування програмним забезпеченням, витрати на електроенергію, що споживається комп'ютером. За даними обчислювального центру ТНЕУ для комп'ютера типу IBM PC/ATX вартість години роботи становить 5,3 грн. Середній щоденний час роботи на комп'ютері — 2 години.

У таблиці 4.3 наведений перелік купованих виробів і розраховані витрати на них.

Таблиця 4.3 — Розрахунок витрат на матеріали та комплектуючі

Найменування купованих виробів	Одини-ця виміру	Ціна, грн	Кількість купованих виробів	Сума, грн	Транспортні витрати (10% від суми)	Загаль-на сума, Грн.
Папір (формат А4)	уп	80,0	2	160,00	16,0	176,0
Ручка кулькова	шт	4,0	2	8,00	0,8	8,80
Диски CD-R	шт	2,0	2	4,00	0,4	4,40
Зошит, 96 арк	шт	9,50	1	9,50	0,95	10,45
Тонер для принтера	уп	49	1	49	4,9	53,9
Ліцензія середовища розробки	шт	6000	1	6000	0	6000
Разом						6252,55

Розрахунок витрат на використання комп'ютерної техніки приведений в таблиці 4.4.

Таблиця 4.4 — Розрахунок витрат на використання комп'ютерної техніки

№ п/п	Назва етапів робіт, при виконанні яких використовується комп'ютер	Час використання комп'ютера, год.	Витрати на використання комп'ютера грн.
1	Проведення досліджень та оформлення їх результатів	60	270
2	Оформлення техніко-економічного розділу	8	36
4	Оформлення ДП	12	54
Разом		80	360

Накладні витрати проектних організацій включають три групи видатків: витрати на управління, загальногосподарські витрати, невиробничі витрати. Вони розраховуються за встановленими відсотками до витрат на оплату праці. Середньостатистичний відсоток накладних витрат приймемо50% від заробітної плати, тому H=1,5•2247,87=3371,8 (грн.)

Інші витрати є витратами, які не враховані в попередніх статтях. Вони становлять 10% від заробітної плати: I=2247,87•0,1=224,8 (грн.)

Витрати на розробку програмного забезпечення складають $K_1=B_{ОП}+B_Ф+B_{ПВ}+H+I$, тобто:

$$K_1=2247,87+460,8+6252,55+3371,8+224,8=12557,8 \text{ (грн.)}$$

Витрати на відлагодження і дослідну експлуатацію програмного продукту визначаємо за формулою:

$$K_2=S_{м.г.}•t_{від}, \quad (4.4)$$

де $S_{м.г.}$ — вартість однієї машино-години роботи ПК, грн./год.

$t_{від}$ — комп'ютерний час, витрачений на відлагодження і дослідну експлуатацію створеного програмного продукту, год.

Загальна кількість днів роботи на комп'ютері дорівнює 30 днів. Середній щоденний час роботи на комп'ютері — 2 години. Вартість години роботи комп'ютера дорівнює 5,32 грн. Тому K_2= 5,32·60 = 319,2 грн.

На основі отриманих даних складаємо кошторис витрат на розробку програмного забезпечення (таблиця 4.5).

Таблиця 4.5 — Кошторис витрат на розробку програмного забезпечення

Найменування витрат	Сума витрат, грн.
Витрати на оплату праці	2247, 87
Відрахування у спеціальні державні фонди	460,8
Витрати на куповані вироби	6252,55
Накладні витрати	3371,8
Інші витрати	224,8
Витрати на відлагодження і дослідну експлуатацію програмного продукту	319,2
Разом	12877,02

4.2 Визначення експлуатаційних витрат

Для оцінки економічної ефективності розроблюваного програмного продукту слід порівняти його з аналогом, тобто існуючим програмним забезпеченням ідентичного функціонального призначення.

Експлуатаційні одноразові витрати по програмному забезпеченню і

аналогу включають вартість підготовки даних і вартість роботи комп'ютера (за час дії програми):

$$E_n = E_{1n} + E_{2n}, \tag{4.5}$$

де E_n — одноразові експлуатаційні витрати на ПЗ (аналог), грн.;

E_{1n} — вартість підготовки даних для експлуатації ПЗ (аналогу), грн.;

E_{2n} — вартість роботи комп'ютера для виконання проектного рішення (аналогу), грн.

Річні експлуатаційні витрати B_{en} визначаються за формулою:

$$B_{en} = E_n \bullet N_n, \tag{4.6}$$

де N_n — періодичність експлуатації ПЗ (аналогу), раз/рік.

Вартість підготовки даних для роботи на комп'ютері визначається за формулою:

$$E_{1П} = \sum_{l=1}^{n} n_i t_i c_i , \tag{4.7}$$

де i — категорії працівників, які приймають участь у підготовці даних;

n_i — кількість працівників i-ої категорії, осіб.;

t_i — трудомісткість роботи співробітників i-ої категорії по підготовці даних, год.;

c_i — середнього годинна ставка працівника i-ої категорії з врахуванням додаткової заробітної плати, що знаходиться із співвідношення:

$$c_i = \frac{c_i^0 (1+b)}{m}, \tag{4.8}$$

де b — коефіцієнт, який враховує додаткову заробітну плату (приймемо 0,57);

m — кількість робочих годин у місяці, год.

Для роботи з даними як для проектного рішення так і аналогу потрібен один працівник, основна місячна заробітна плата якого складає: c=1089 грн. Тоді: $c_1 = \frac{1089(1+0,57)}{22*8} = 9,7$ грн/год. Трудомісткість підготовки даних для проектного рішення складає 3 год., для аналога 3,5 год. Результати представлені у таблиці 4.6.

Таблиця 4.6 — Розрахунок витрат на підготовку даних та реалізацію проектного рішення на комп'ютері

Час роботи співробітників, год.	Середньогодинна заробітна плата, грн./год.	Витрати , грн.
Проектне рішення		
3	9,7	29,1
Аналог		
3,5	9,7	33,95

Витрати на експлуатацію комп'ютера визначається за формулою:

$$E_{2П} = t * S_{МГ}, \quad (4.9)$$

де t — витрати машинного часу для реалізації проектного рішення (аналогу), год.;

$S_{МГ}$ — вартість однієї години роботи комп'ютера, грн./год.

$E_{2п}$=3·5,32=15,96 грн.; $E_{2а}$=3,5·5,32 =18,62 грн.;

$E_п$=29,1+15,96=45,06 грн.; $E_а$=33,95+18,62 = 52,57 грн.;

$B_{еп}$= 45,06*252=11355,12 грн.; $B_{еа}$=52,57*252=13247,64 грн.

4.3 Розрахунок ціни споживання проектного рішення

Ціна споживання — це витрати на придбання і експлуатацію проектного рішення за весь строк його служби:

$$Ц_{С(П)} = Ц_{П} + В_{(Е)NPV}, \quad (4.10)$$

де $Ц_{П} = К(1+\frac{П_{Р}}{100}) + К_{0} + К_{к}$ — ціна придбання проектного рішення, грн.:

$К$ — кошторисна вартість;

$Пр$ — рентабельність;

$К_{о}$ — витрати на прив'язку та освоєння проектного рішення на конкретному об'єкті, грн.;

$К_{к}$ — витрати на доукомплектування технічних засобів на об'єкті, грн.;

Отже, $Ц_{п}$=12877·(1+0,3) = 16740,1 грн.

Вартість витрат на експлуатацію проектного рішення (за весь час його експлуатації), грн.:

$$В_{епрv} = \sum_{t=0}^{T} \frac{В_{еП}}{(1+R)^{t}}, \quad (4.11)$$

де $В_{еп}$ — річні експлуатаційні витрати, грн.;

$Т$ — строк служби проектного рішення, років;

R — річна ставка проценту банку.

Отже, $В_{епрv} = \sum_{t=1}^{3} \frac{11355,12}{(1+0,08)^{t}} = 31542$ грн; $В_{епрv} = \sum_{t=1}^{3} \frac{13247,64}{(1+0,08)^{t}} = 36799$ грн.

Тоді ціна споживання проектного рішення дорівнюватиме:

$$Ц_{сп} = 16740,1 + 31542 = 48282,1 \text{ грн.}$$

Аналогічно визначається ціна споживання для аналогу:

$$Ц_{са} = 14470,7+36799=51269,7 \text{ грн.}$$

4.4 Визначення показників економічної ефективності

Економічний ефект в сфері проектування рішення:

$$E_{ПР} = Ц_{П} - Ц_{А} = 51269,7 - 48282,1 = 2986,9 \text{ грн.}$$

Річний економічний ефект в сфері експлуатації:

$$E_{КС} = B_{ЕА} - B_{ЕП} = 13247,64 - 11355,12 = 1892,52 \text{ грн.}$$

Додатковий економічний ефект у сфері експлуатації:

$$\Delta E_{екс} = \sum_{t=1}^{T} E_{екс}(1+R)^{T-t} \text{ грн.}$$

$$\Delta E_{екс} = \sum_{t=1}^{3} 1892,52(1+0,08)^{3-1} = 6143,88 \text{ грн}$$

Сумарний ефект складає:

$$E = E_{пр} + \Delta E_{екс} = 9130,78 \text{ грн.}$$

Результати усіх здійснених вище розрахунків представлені в таблиці 4.7.

Таблиця 4.7 — Показники економічної ефективності проектного рішення

Найменування	Одиниці вимірювання	Значення показників	
		Базовий варіант	Новий варіант
Капітальні вкладення	грн.	-	12877,02
Ціна придбання	грн.	14470,7	16740,1
Річні експлуатаційні витрати	грн.	13247,64	11355,12
Ціна споживання	грн.	51269,7	48282,1
Економічний ефект в сфері проектування	грн.	-	2986,9
Економічний ефект в сфері експлуатації	грн.	-	1892,52
Додатковий ефект в сфері експлуатації	грн.	-	6143,88
Сумарний ефект	грн.	9130,78	

Отже, у даному розділі проведено розрахунок витрат на розробку програмного засобу, оплату праці, розрахунок витрат на використання комп'ютерної техніки, а також кошторис витрат на розробку даного програмного забезпечення. Отже, згідно проведеного економічного обґрунтування дане проектне рішення є конкурентноздатним. Отримано економічний ефект у розмірі 9130,78 грн. і тому розробка і впровадження цього проектного рішення є економічно доцільними.

ВИСНОВКИ

В результаті розробки даного дипломного проекту:

1) розглянуто ймовірні загрози в сучасних комп'ютерних системах;

2) проведено аналіз засобів захисту інформації, що дозволяє зробити наступний висновок: захищати необхідно всі компоненти системи: устаткування, програми, дані та персонал;

3) розглянуто особливості застосування хеш-функції в сучасних комп'ютерних системах та наведено структуру основного циклу і однієї операції алгоритму обчислення значення модифікованої хеш-функції MD5;

4) проведено загальний огляд стійкості хеш-функції і визначено наступні властивості хеш-функції: хеш-функція має нескінченну область визначення; хеш-функція має скінченну область значень; вона необоротна; зміна вхідного потоку інформації на один біт змінює близько половини всіх бітів вихідного потоку, тобто результату хеш-функції;

5) для реалізації модифікованої хеш-функції MD5 були підключені методи інтерфейсу CryptoAPI;

6) описано модель бази даних ключів. Кожний криптосервер (CSP) має асоціативну базу даних для ключових контейнерів, яка містить всі приватні і загальні ключі користувачів, що мають доступ до даного комп'ютера;

7) розроблено основні модулі обчислення значення хеш-функції і пошуку наявності об'єкта у списку елементів даних;

8) наведено результати виконання програмного комплексу.

Таким чином, від кількості етапів залежить значення хеш-функції. При одному і тому ж вхідному повідомленні значення хеш-функції від 3 до 5 етапів буде різним. Було здійснено перевірку хеш-функції. В результаті чого файли мали ідентичні імена і однаковий вміст.

Результати розробки мають практичне використання (додаток Б).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про кіберзлочинність [Електронний ресурс] - Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

2. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем / Я.М.Николайчук, Н.Я.Возна, І.Р.Пітух – Тернопіль: ТзОВ «Терно-граф», 2010. – 392 с.

3. Архітектура клієнт-сервер [Електронний ресурс] - Режим доступу: http://www.intelsd.com/?tc=175&sc=197&lvl=2.

4. Васильцов І.В.Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В.Васильцов / За ред. В.П.Широчина – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.

5. Кулаков Ю.О. Комп'ютерні мережі: Підручник. / Ю.О.Кулаков, Г.М.Луцький / За ред. Ю.С.Ковтанюка – К.: Видавництво «Юніор», 2005. – 400 с.

6. Романец Ю.В. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, / Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. - М.: Радио и связь, 1999. -328 с.

7. Широчин В.П. Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях / В.П.Широчин, В.Е.Мухин, А.В.Кулик. - К.: "ВЕК+", 2000. – 112 с.

8. Дудикевич В.Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв'язку / В.Б.Дудикевич, Ю.Л.Пархуць // Інформаційна безпека. – 2011. - №1(5). – С.83-87.

9. Василенко В. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ / В.Василенко, М.Будько. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – Випуск 9. – С.110-120.

10. Тичковський Р.О. Математичне та програмне забезпечення оптимального розподілу ресурсів серед вузлів комп'ютерних мереж: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 01.05.03 «Математичне та програмне забезпечення обчислювальних машин і систем» / Р.О.Тичковський. – Львів, 2010. – 20 с.

11. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. / В.Столлингс. – М.: Изд. Дом «Вильямс», 2001. – 672 с.

12. Безмалый Н.В. Как ломаются пароли / Н.В.Безмалый // Журнал информационных технологий CHIP. – 2008. - №7. – С.124-126.

13. Україна значно піднялася в рейтингу країн з найбільшою кількістю кібер-загроз [Електронний ресурс] - Режим доступу: http://www.rbc.ua/ukr/top/show/

14. Зайчук А.В. Основные пути утечки информации и несанкионированного доступа в корпоративных сетях / А.В.Зайчук // Захист інформації. – 2003. – № 4. – С. 19-24.

15. Чеховский С.А. Побочные излучения и защита информации в локальных сетях. / С.А.Чеховский, Ю.М.Рудаков // Захист інформації. – 2003. – № 4. – С. 30-38.

16. Koeune F. A Tutorial on Physical Security and Side-Channel Attacks/ F.Koeune, F.-X. Standaert : Foundations of Security Analysis and Design III (FOSAD 2004/2005), November 2006. – 2006. - LNCS 3655. – P. 78-108.

17. Заболотний В.І. Класифікація технічних каналів витоку інформації / В.І.Заболотний // Радіотехніка. Тематичний випуск "Інформаційна безпека". - 2003. - № 134. - С.210-218.

18. Журавель Т.Н. Некоторые особенности защиты информации с ограниченным доступом от утечки по виброакустическому каналу / Т.Н.Журавель // Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003. - С.91-95.

19. Васильченко И.И. Магнитоэлектрические виброизлучатели с пониженным уровнем акустического шума для систем технической защиты информации / И.И.Васильченко, И.А.Кравченко / Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003. - С.96-105.

20. Безруков К. Н. Классификация компьютерных вирусов MS DOS и методы защиты от них / К.Н.Безруков.— М.; СПб "ICE", 1990. – 48 с.

21. Brier E. Chemical Combinatorial Attacks on Keyboards / E.Brier, D.Naccache, P.Paillier [Електронний ресурс] - Режим доступу: http://eprint.iacr.org/2003/217.pdf

22. Skorobogatov S. Optical Fault Induction Attacks / S.Skorobogatov, R.Anderson // Cryptographic Hardware and Embedded Systems – CHES 2002): 4th International Workshop, August 13-15, 2002: Proceedings. − San Francisco (USA), 2002.− P.2-12.

23. Горбачёв В. Модель угроз, реализуемых аппаратными ресурсами компьютерных систем / В.Горбачёв, В.Степаненко, Т.Гриценко. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – Випуск 9. – С.75-78.

24. Agrawal D. The EM Side-Channel(s) / D.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi // Cryptographic Hardware and Embedded Systems – CHES 2002): 4th International Workshop, August 13-15, 2002: Proceedings. - San Francisco 2002. - LNCS 2523. - P. 29 - 45.

25. Kocher P. Differential Power Analysis / P.Kocher, J.Jaffe, B.Jun // in Advances in Cryptology (CRYPTO'99): 19th Annual International Cryptology Conf., August 1999: Proceedings. - Santa Barbara, California, USA, 1999. - LNCS 1666. - P.388-397.

26. Гопиенко А.В. Формирование потайных каналов передачи информации в компьютеризированных измерительных системах / А.В.Гопиенко, Ю.В.Куц, Е.В.Монченко // Системи обробки інформації. – 2012. – Вип. 3(101). – Т.1. – С.123-126.

27. Васильцов І.В. Методи захисту проти атак спеціального виду / І.В.Васильцов, Л.О.Дубчак // Вісник Хмельницького національного університету. Технічні науки. – 2007. - №5. – С.174-182.

28. Васильцов І.В. Класифікація сучасних атак спеціального виду на реалізацію / І.В.Васильцов, Л.О.Дубчак // Захист інформації. – 2007. - №4. – С.10-21.

29. Паздрій І.Р. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп'ютерна інженерія/ І.Р. Паздрій – Тернопіль: ТАНГ, 2014. – 37 с.

30. Березький О.М. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня "Бакалавр" напряму підготовки 6.050102 «Комп'ютерна інженерія» фахового спрямування «Комп'ютерні системи та мережі» / О.М. Березький, Л.О.Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2016.– 65 с.