НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

На правах рукопису

МУХІН ВАДИМ ЄВГЕНІЙОВИЧ

УДК 681.3.06

СПОСІБ ТА ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОЦЕДУР АУТЕНТИФІКАЦІЇ В ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

Спеціальність: 01.05.03 - Математичне та програмне забезпечення обчислювальних машин та систем

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ - 1997

Дисертацією є рукопис
Робота виконана у Національному технічному університеті України
"Київський політехнічний інститут" на кафедрі обчислювальної техніки

Науковий керівник: доктор технічних наук, в. н. с.,
Широчин Валерій Павлович,
професор кафедри обчислювальної
техніки НТУУ "КПІ"

Офіційні опоненти: доктор технічних наук, с. н. с,
Нестеренко Борис Борисович,
зав. лабораторією математичного
моделювання Інституту математики НАНУ

кандидат технічних наук,
Рабчук Віталій Львович,
зав. відділом проектування
ЗАТ "Інфоком - Супутникові Комунікації"

Провідна організація: Інститут кібернетики НАН України,
м. Київ

Захист відбудеться 20.10. 1997 р. о 14.30 годині на засіданні спеціалізованої Ради Д 26.002.02 у Національному технічному університеті України "Київський політехнічний інститут" (м.Київ, пр. Перемоги, 37, корп. 18, ауд. 306)

З дисертацією можна ознайомитись у бібліотеці Національного технічного університету України "КПІ".

Автореферат розіслано "16" 09 1997 р.

Вчений секретар
спеціалізованої Ради,
кандидат технічних наук,
доцент М.М. Орлова

АНОТАЦІЯ

Метою дисертаційної роботи є розробка способу та інструментальних засобів забезпечення підвищенного ступеня захищенності процедур та протоколів аутентифікації на основі ефективного вирішення задачі вибору параметрів й розподілення ключів шифрування у корпоративних обчислювальних мережах, які дозволяють не знизити їх пропускну спроможність.

Для досягнення вказаної мети в дисертації розв'язані наступні задачі :

1.Порівняльний аналіз програмного та математичного забезпечення процедур аутентифікації у сучасних операційних системах та мережевих середовищах.

2. Аналіз та розробка математичних моделей та спеціальних алгоритмів на основі незвертних функцій для формування протокольних повідомлень й цифрових сигнатур в задачах аутентифікації.

3. Розробка способу керування ключами шифрування з урахуванням ступеня захищенності протоколів й систем аутентифікації суб'єктів та повідомлень й пропускної спроможності обчислювальних мереж (ОМ), що реалізують ці протоколи.

4. Розробка інструментального середовища і інтерфейсу адміністратора безпеки для верифікації та цільового проектування процедур аутентифікації.

5. Розробка та дослідження моделі моніторингу безпеки у обчислювальних мережах з метою запобігання перекручень інформації й протокольних повідомлень.

Автор захищає наступні положення та результати:

— Модель та алгоритм формування протокольних повідомлень й цифрових сигнатур на основі адитивно-константних незвертних функцій.

— Архітектуру інструментального середовища для проектування протоколів аутентифікації та аналітичні оцінки їх характеристик.

— Спосіб керування ключами шифрування з адаптацією до необхідного ступеня захищенності процедур й протоколів аутентифікації та пропускної спроможності мереж, що їх реалізують.

— Структуру та математичне забезпечення процесора генерації протокольних повідомлень.

— Модель моніторингу мережевої безпеки на основі аномального статистичного алгоритму.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Нові інформаційні технології, що активно розвиваються у останні роки, дозволили здійснити своєрідну революцію у засобах і методах обробки й передачі інформації. Розробка різних документів, науково-технічної документації для супроводження проектів й проектних рішень,

отримання нової інформації про досягнення світової науки й техніки практично не можливі без використання корпоративних та глобальних інформаційно-обчислювальних мереж та середовищ (INTERNET, FIDONET і т.д.). Розширення меж надання прав користування спеціальною інформацією й периметру відповідальності за цілісність й конфіденційність даних, що передаються, особливо у обчислювальних мережах з широкомовленням від одного суб'єкта до багатьох, вимагає особливих заходів що до організації захисту інформації у відповідності з категоріями доступу, а також ідентифікації й підтвердження справжності (аутентифікації) суб'єктів та повідомлень у обчислювальних мережах.

Глобальне використання інформаційних ресурсів й загальне включення персональних комп'ютерів й автоматизованих робочих місць в локальні, установчі, корпоративні, регіональні й світові інформаційно-обчислювальні мережі та середовища різко загострили проблему інформаційної безпеки, деякі аспекти якої полягають у наступному.

1. Низька захищенність мережевих комунікацій, їх висока потенційна уразливість висувають особливі вимоги до організації передачі інформації, забезпечення її цілісності, захисту від несанкціонованого зчитування, перекручення й знищення, що обумовлює доцільність застосування додаткових засобів криптозахисту при передачах як службової інформації, так і інформації з обмеженим доступом.

2. Підвищення ступеня криптографічного захисту протокольних повідомлень й цифрових сигнатур для підтвердження справжності суб'єктів та повідомлень у обчислювальних мережах забезпечується, перед усім, за рахунок керування довжиною ключів шифрування, що призводить до зниження пропускної спроможності мереж.

3. Існуючі засоби захисту інформації, що розроблюються виробниками, залишаються "закритими" для користувачів й не можуть бути модифіковані (адаптовані) під вимоги конкретних користувачів, установ, корпорацій й можливих спеціальних умов їх застосування.

4. Розробка нових механізмів захисту інформації у обчислювальних мережах вимагає спеціальних оцінок і інструментальних засобів дослідження й визначення ступеня захищенності цих механізмів на основі проведення верифікаційних й сертифікаційних досліджень.

Питанням розробки й дослідження засобів захисту інформації в обчислювальних мережах присвячена ця робота.

Методи досліджень. В дисертаційній роботі використовується математичний апарат теорії складних систем, теорії алгоритмів, теорії ймовірності й математичної статистики, методи теорії обробки спостережень. Основні положення й теоретичні оцінки підтверджені результатами теоретичного аналізу та імітаційного моделювання можливих напрямів "атак" у обчислювальних мережах.

Наукова новизна роботи полягає в розробці:

— математичної моделі протоколу аутентифікації підвищенного ступеня захищенності на базі модифікованого алгоритму кодування, що використовує адитивно-константні , незвертні функції для формування протокольних повідомлень й цифрових сигнатур;

— методики задання параметрів ключів для формування протокольних повідомлень й цифрових сигнатур на основі аналізу необхідного безпечного часу їх використання;

— моделі моніторингу мережевої безпеки на основі аномального статистичного алгоритму.

Практична цінність роботи полягає в розробці методичних основ цільового проектування протоколів аутентифікації підвищенного рівня захищенності та інструментального середовища для верифікації, а в подальшому сертифікації й атестації засобів захисту інформації у обчислювальних мережах.

Розроблен багатовіконний спеціалізований інтерфейс інструментального середовища для модифікації й адаптації протоколів аутентифікації до конкретних умов їх застосування.

Вирогідність наукових результатів й практичних рекомендацій дисертації підтверджується коректним використанням математичного апарату, доведенням теоретичних стверджень, а також результатами експериментів з використанням інструментального середовища, що запропоновано.

Реалізація результатів роботи. Робота виконувалась у відповідності з науковим напрямком кафедри обчислювальної техніки НТУУ "КПІ" в рамках проекту Державної Програми "Розвиток системи технічного захисту інформації України", а і результати впроваджувались під час виконання цілого ряду НДР: шифр "Захист-41" (1994 р.), шифр "Мережа-5" (1995 р.), замовник обох НДР — Державна служба України з питань технічного захисту інформації (ДС ТЗІ), а також НДР " Інформаційне забезпечення комп'ютерних засобів контролю та діагностики потужних енергооб'єктів на основі систем штучного інтелекту майбутніх поколінь" (шифр "Ватра"), замовник Державний Фонд фундаментальних досліджень (1994 - 1995 рр.), та НДР "Дослідження й порівняльний аналіз ефективності цифрових процесорів обробки сигналів" (шифр "Кортик"), замовник НВО "Славутич" м. Київ (1994 р.). Отримані акти про впровадження результатів роботи від відповідних організацій.

Апробація роботи. Основні результати дисертаційної роботи доповідалися й обговорювалися на: міжнародному науковому семінарі "Кібернетика електричних систем" (м. Новочеркаськ, Росія, 1994 р.), міжнародній науково-технічній конференції "Математичне моделювання в електротехниці й електроенергетиці" (Львів, 1995 р.), міжнародному науково-технічному симпозіумі "МЕТРОЛОГІЯ'95" (м.Созополь, Болгарія, 1995 р.), міжнародній науково-технічній конференції "Автоматизація проектування дискретних систем" (м.Мінськ, Білорусь, 1995 р.), Третій Українській конференції з

автоматичного керування "АВТОМАТИКА'96" (м.Севастополь, 1996 р.), Другій міжнародній науково-технічній конференції "Нетрадиційні електромеханічні та електротехнічні системи" (м. Щецин, Польща, 1996 р.).

Публікації. За темою дисертації опубліковано 12 друкованих праць.

Структура роботи. Дисертаційна робота складається з вступу, чотирьох глав, заключної частини, списку літератури із 127 найменувань та додатків. Робота містить 150 сторінок, у тому числі 23 малюнка та 18 таблиць, додатки складають 32 сторінки.

У вступі обгрунтована актуальність теми дисертаційної роботи, формулюється мета та задачі дослідження, наведені основні результати, що виносяться на захист.

У першій главі розглянуті і класифіковані основні види й фактори загроз безпеки у обчислювальних мережах. Визначені потенційні уразливі місця в них та вироблені вимоги до засобів захисту. Виконан порівняльний аналіз особливостей побудування засобів підтвердження справжності суб'єктів та повідомлень у обчислювальних мережах.

У другій главі досліджені адитивно-константні незвертні функції в задачах криптографії й аутентифікації й показано, що алгоритм шифрування, який базується на адитивно-константній незвертній функції, має спеціальні можливості за рахунок введення адитивної складової як індивідуального елементу секретного ключа. Розроблені методика задання параметрів ключів шифрування й спосіб керування ключами на основі оцінки ступеня захищенності протоколів й систем аутентифікації суб'єктів та повідомлень, а також оцінки пропускної спроможності обчислювальних мереж, що їх реалізують. Показано, що за рахунок керування ключами шифрування в процедурах аутентифікації з'являється можливість скоротити витрати на кодування службової інформації, що дозволяє не зменшити пропускну спроможність мереж.

У третій главі розроблене інструментальне середовище для верифікації й цільового проектування процедур аутентифікації суб'єктів та повідомлень у обчислювальних мережах. Показано, що запропонований протокол аутентифікації у обчислювальних мережах з цифровою сигнатурою (сертифікатом) Центру Розподілення Ключів (ЦРК) ключів шифрування суб'єктів на базі адитивно-константних незвертних функцій забезпечує підвищенний ступінь захищенності, а також підвищенний рівень пропускної спроможності мережі. Розроблена структура та математичне забезпечення програмного процесору генерації протокольних повідомлень. Отримані оцінки захищенності протоколів аутентифікації й пропускної спроможності мереж, що їх реалізують.

У четвертій главі розроблена архітектура засобів серверу безпеки обчислювальних мереж, що реалізує функції й механізми підтвердження справжності суб'єктів та повідомлень, а також виконує роль ЦРК. Розроблена та досліджена модель моніторингу мережевої безпеки на основі векторів індикації

аномальних дій потенційних зловмисників у обчислювальних мережах. Модель відрізняється можливістю оцінки ймовірності порушення засобів захисту у кожному сеансі й виявлення наймовірніших порушників згідно рівня підозрілості їх дій.

У заключній частині наведені основні результати дисертаційної роботи.

У додатки включені акти про впровадження результатів дисертаційної роботи, описи та лістинги програмного комплексу інструментального середовища для розробки й дослідження протоколів аутентифікації суб'єктів та повідомлень ОМ, а також лістинги програмного забезпечення процесора генерації повідомлень протокола аутентифікації і моделі моніторингу безпеки обчислювальної мережі.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Висока потенційна уразливість мережевих комунікацій висуває особливі вимоги до організації розподілених систем, забезпеченню цілісності інформації, що передається, захисту її від активного й пасивного перехоплення, що обумовлює актуальність досліджень в галузі спеціальних, у тому числі національних, засобів захисту інформації в обчислювальних системах та мережах. У роботі показано, що одним з напрямків підвищення ефективності механізмів захисту в ОМ є модифікації криптографічних методів та засобів аутентифікації. Відомі декілька проектів міжнародних стандартів реалізації процедур аутентифікації підвищенного рівня захищенності. Міжнародною організацією ISO запропоновані стандарти JTC1.27.18.2 (1992 р., автор В.Фумі, Німеччина), JTC1.27.18.3 (1992 р., автор Р.Руппель, Швейцарія) та ін., що визначають механізми керування ключами при використанні симетричних й асиметричних методів шифрування. Проблемам криптографічного захисту присвячені роботи І.Н. Коваленка, А.В. Спесівцева, Л.С.Беляєвського, О.В. Вербицького, Р.Рівеста, С.Померанса, У.Діффі, О.Голдрейха, Дж. Х. Мур та ін.

Розробка засобів верифікації й сертифікації програмного забезпечення реального часу являє собою фундаментальну задачу. Цім питанням присвячений цілий ряд праць У. Квірка, П. Квітнера, Дж. С. Кінга, Р.Л. Лондона, І.С. Піла, В.І. Пустоварова, Ю.В. Борзова, А.Л. Фуксмана, Б.А. Позіна та ін. Вище згадана задача примикає до проблеми оцінок надійності й безпеки програмного забезпечення, які базуються на моделюванні логіко-часової організації обчислювальних процесів, наприклад, із використанням апарату стохастичних сіток Петрі й на розробці відповідних інструментальних систем й імітаційних моделей. Цій тематиці присвячені праці Г.Тейєра, Г. Майєрса, Е. Нельсона, В. П. Широчина, В.В. Ліпаєва, Є.С. Согомоняна, П.П. Пархоменка та ін.

На основі аналізу проблем, що виникають при розробці засобів захисту інформації у сучасних операційних системах виділен головний напрямок досліджень — *розробка математичного й програмного забезпечення інструментального середовища та інтерфейсу адміністратора безпеки для верифікації й цільової адаптації процедур та протоколів аутентифікації в обчислювальних мережах з метою підвищення рівня захищенності й пропускної спроможності ОМ.*

У відповідності з обраним напрямком для вирішення покладених задач у роботі проведена класифікація та порівняльний аналіз програмного і математичного забезпечення процедур аутентифікації суб'єктів й формування цифрових сигнатур для підтвердження справжності повідомлень у сучасних операційних системах й мережевих середовищах для визначення переваг та недоліків тих чи інших засобів аутентифікації.

Виконан порівняльний аналіз криптографічних методів та засобів, що використовуються в задачах аутентифікації суб'єктів та повідомлень у обчислювальних мережах з метою вибору ефективних алгоритмів шифрування при модифікації чи адаптації протоколів аутентифікації суб'єктів й повідомлень обчислювальних мереж.

Одним з сучасних напрямків формування протокольних повідомлень та цифрових сигнатур є криптографічні системи з відкритими ключами, зокрема, криптосистеми: RSA, Кейда, Ягісави, Макеліса, TMKIF, Луччо-Маццене та ін.

Показано, що адитивні незвертні функції *Add (x)*, які запропоновано до використання в криптографічних системах з відкритими ключами, задовольняють вимогам, що висуваються до класу незвертних функцій й мають наступні загальні властивості:

Властивість 1. Швидкого обчислення прямого перетворення на основі елементарних операцій зведення у ступінь, додавання й обчислення значення функції по *mod B*.

Властивість 2. Складного обчислення зворотнього перетворення на основі ймовірностних алгоритмів *A'*, які можуть звернути функцію *Add(x)* лише з достатньо малою ймовірністю *P*, тобто для кожного як завгодно малого $\varepsilon > 0$ при усіх $x = \{S\}^N$, де $\hat{S}$ - символи алфавіту повідомлення, N - довжина повідомлення, знайдеться позитивне число n — довжина ключа, таке, що для $N > n$ буде виконуватись нерівність:

$$P\,(A'(Add(x)) \in Add^{-1}\,Add(x)) < \varepsilon \qquad (1)$$

Виділен спеціальний клас адитивно-константних незвертних функцій $Add_{c,B,\xi}(x)$ для побудування криптографічних систем й розробки на базі них спеціальних протоколів аутентифікації підвищенного рівня захищенності. Підклас адитивно-константних незвертних функцій визначається як (2):

$$Add_{e,B,\xi}(x) = (x^{e\,(e*d \bmod \Phi(B)=1)} + \xi_{pers}) \bmod B, \qquad (2)$$

де: x — перетворюємо значення (повідомлення), e, d, B — деякі позитивні цілі числа, причому (e,B) — відкритий ключ, а (d,B) — секретний ключ, $\Phi(B)$ — функція Ейлера для вибору елементів ключів e і d як звертних величин в арифметиці відрахувань по модулю B, ξ_{pers} — адитивна складова перетворення.

Показано, що криптографічна система на основі адитивно-константної незвертної функції $Add_{e,B,\xi}(x)$ має наступні особливі властивості.

Властивість 3. Початкове повідомлення x може мати довільне значення в діапазоні $1 < x < B$, де $B = p * q$, причому p і q — прості числа. Шифрований блок-повідомлення y, що відповідає повідомленню x, отримується із перетворення:

$$y = (x^{e\,(e*d \bmod \Phi(B)=1)} + \xi_{pers}) \bmod B, \qquad (3)$$

причому ξ_{pers} - ціле число й $0 < \xi_{pers} < B$.

Властивість 4. Початкове повідомлення x відновлюється із шифрованого блоку y зворотнім перетворенням:

а) якщо $y - \xi_{pers} > 0$, то $x = (y - \xi_{pers})^{d\,(e*d \bmod \Phi(B)=1)} \bmod B$ (4)

б) якщо $y - \xi_{pers} < 0$, то $x = (y - \xi_{pers} + B)^{d\,(e*d \bmod \Phi(B)=1)} \bmod B$. (5)

Адитивна складова ξ_{pers} є елементом секретного ключа, що підвищує захищенність повідомлень, які передаються, та є індивідуальним засобом захисту секретної інформації для окремих користувачів в мережах з широкомовленням.

Обчислювальна складність алгоритмів розкриття шифрованої інформації, що повинні визначити секретний ключ (d,B) по відкритому (e,B) та адитивну складову ξ_{pers}, еквівалентна складності факторизації (розкладення на прості множники) числа B та визначенню складової ξ_{pers} шляхом перебору. Досліджено, що сучасним алгоритмам факторизації для розкладення великих чисел довжиною 200 десяткових знаків необхідно виконати приблизно $1.2 * 10^{23}$ макроопераций, що обумовлює значні витрати часу на виконання факторизації. Обчислювальна складність знаходження адитивної складової ξ_{pers} залежить від значення числа ξ_{pers} й складає 25-35% обчислювальної складності факторизації числа B при умові, що ξ_{pers} достатньо близько до B.

У роботі проведені експериментальні дослідження обчислювальної складності алгоритмів розкриття інформації. З урахуванням відомої оцінки кількості операцій алгоритму факторизації для великих значень кількості десяткових розрядів n $(n > 100)$ числа B ключів шифрування отримана інтегральна оцінка залежності числа операцій $Q(n)$ алгоритму розкриття криптосхем на основі адитивно-константних незвертних функцій

в залежності від значення n в десяткових знаках числа B ключів шифрування (6):

$$Q(n) = 1.27 * 10^{0.001*(-0.0005793*n^3+0.0218*n^2+111.19*n+4604.6)} \quad (6)$$

Час криптостікості $T_{кр}(n)$, необхідний для розкриття захищенної інформації, визначається як:

$$T_{кр}(n) = Q(n) * T_{мо}, \quad (7)$$

де $T_{мо}$ — середній час виконання однієї макрооперації.

У роботі запропонована методика оцінки ефективності застосування і модифікації протоколів аутентифікації. Методика використовує оцінку логарифмічного показника відношення криптостійкості протокольних повідомлень до витрат часу на виконання процедури аутентифікації на основі теоретичних та/або експериментальних даних про ступінь захищенності (криптостійкості) повідомлень протоколу аутентифікації й часу шифрування/дешифрування службової інформації та її передачі у процесі виконання процедури аутентифікації. Витрати часу на аутентифікацію визначаються як:

$$T_{\Sigma_3}(n) = a * T_ш(n) + b * T_д(n) + c * T_п, \quad (8)$$

де a — число змінних, що шифруються, $T_ш(n)$ — середній час шифрування однієї змінної, b - число змінних, що дешифруються, $T_д(n)$ — середній час дешифрування однієї змінної, c — число мережевих передач службової (у т. ч. зашифрованної) інформації у процесі аутентифікації, $T_п$ — час однієї передачі.

Логарифмічний показник ефективності застосування засобів аутентифікації (К) визначається як:

$$K = ln \frac{Q(n)}{T_{\Sigma_3}(n)}, \quad (9)$$

де $Q(n)$ — число операцій, що витрачаються на розкриття зашифрованної інформації у протокольних повідомленнях, $T_{\Sigma_3}(n)$ — сумарні витрати часу на виконання процедури аутентифікації. Модифікація протоколу аутентифікації розглядається як раціональна у тому випадку, якщо час криптостійкості протокольних повідомлень ($T_{кр}(n)$), який пов'язан з числом операцій $Q(n)$ у відповідності з (7), перевищує необхідний час безпечного використання ключів шифрування ($T_{бк}$) повідомлень протоколу аутентифікації, тобто $T_{кр}(n) > T_{бк}$.

У роботі запропонован спосіб керування ключами шифрування з адаптацією до необхідного ступеня захищенності процедур та протоколів аутентифікації й пропускної спроможності мереж, що їх реалізують. Для моделей протоколів аутентифікації, які досліджуються, засобами, що

зображені на *мал. 1*, виконується аналіз ступеня захищенності протокольних повідомлень та цифрових сигнатур з оцінкою часових витрат на їх формування. Згідно способу, оптимальні параметри криптосхем, які використовуються для шифрування інформації в процедурах аутентифікації, вибираються з урахуванням необхідного безпечного часу використання ключа ($T_{бк}$), який визначається індивідуально абонентом мережі у відповідності з конкретними умовами використання та передачі інформації. Для вибору квазіоптимального рішення задається час прийняття рішення *(t)*.

Підвищення ефективності застосування засобів аутентифікації здійснюється наступними двома шляхами: корекцією параметрів (довжин) ключів шифрування та корекцією (модифікацією) алгоритмів шифрування, які використовуються. Корекція (модифікація) алгоритмів шифрування дозволяє скоротити часові витрати на виконання процедури аутентифікації при незмінному ступеню захищенності процедури аутентифікації чи, навпаки, підвищити ступінь захищенності при незмінних часових витратах.

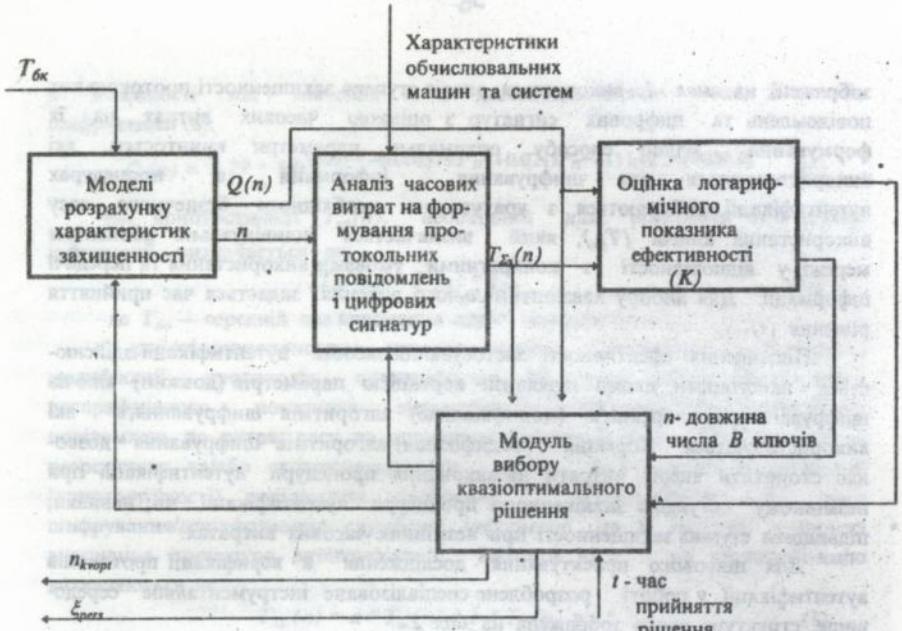
Для цільового проектування, дослідження й верифікації протоколів аутентифікації у роботі розроблене спеціалізоване інструментальне середовище, структура якого зображена на *мал. 2*.

До складу інструментального середовища крім програмно-апаратних засобів протокола аутентифікації суб'єктів та повідомлень ОМ (модуль криптографічних функцій, модуль інтерфейсу адміністратора безпеки, апаратно-програмний модуль підтримки мережевих функцій) також входять: модуль розкриття зашифрованної інформації на базі алгоритму факторизації основ ключів шифрування; програмні засоби для проведення вимірювань-обчислень, що дозволяють отримати кількісні оцінки ступеня захищенності протоколу аутентифікації та пропускної спроможності мереж, які його реалізують.

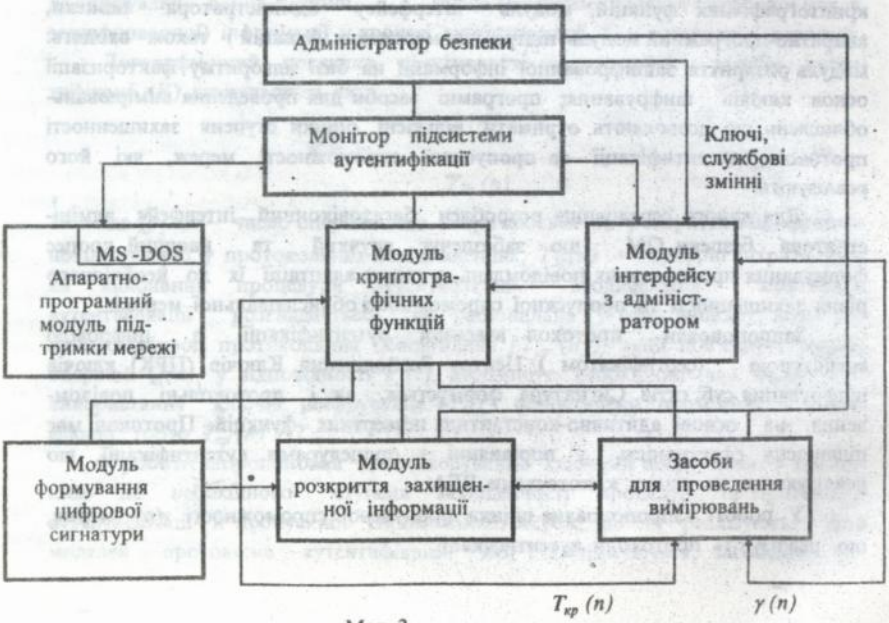
Для даного середовища розроблен багатовіконний інтерфейс адміністратора безпеки ОМ, що забезпечує гнучкий та наочний процес формування протокольних повідомлень, а також адаптації їх до необхідного рівня захищенності та пропускної спроможності обчислювальної мережі.

Запропонован протокол взаємної аутентифікації з цифровою сигнатурою (сертифікатом) Центру Розподілення Ключів (ЦРК) ключів шифрування суб' єктів. Сигнатура формується, як і протокольні повідомлення, на основі адитивно-константних незвертних функцій. Протокол має підвищену ефективність у порівнянні з процедурами аутентифікації, що реалізуються на основі криптосхеми RSA.

У роботі запропонована оцінка пропускної спроможності $\gamma(n)$ мереж, що реалізують протоколи аутентифікації:


Характеристики обчислювальних машин та систем
$T_{бк}$
Моделі розрахунку характеристик захищенності
$Q(n)$
n
Аналіз часових витрат на формування протокольних повідомлень і цифрових сигнатур
$T_{г_i}(n)$
Оцінка логарифмічного показника ефективності (K)
n- довжина числа B ключів
Модуль вибору квазіоптимального рішення
$n_{ключі}$
$\xi_{рег з}$
t - час прийняття рішення

Мал. 1


Адміністратор безпеки
Монітор підсистеми аутентифікації
Ключі, службові змінні
MS -DOS
Апаратно-програмний модуль підтримки мережі
Модуль криптографічних функцій
Модуль інтерфейсу з адміністратором
Модуль формування цифрової сигнатури
Модуль розкриття захищеної інформації
Засоби для проведення вимірювань
$T_{кр}(n)$
$\gamma(n)$

Мал. 2

$$\gamma(n) = \frac{I^* (1 - f_c)}{T_n + T_{\Sigma}(n)}, \qquad (10)$$

де: I — кількість інформації, що передається (Kb), T_n — час її передачі в незахищенній мережі, f_c — середня ймовірність простою і-того абоненту мережі у зв'язку з зайнятістю ЦРК, $T_{\Sigma}(n)$ — сумарні витрати часу на виконання процедури аутентифікації при довжині n числа B ключів шифрування протокольних повідомлень.

Експериментальні дослідження показали підвищення рівня захищенності $Q(n)$ протоколу аутентифікації з сертифікатом ЦРК ключів шифрування та пропускної спроможності $\gamma(n)$ мереж, які його реалізують. Відповідно, логарифмічний показник ефективності його застосування виявився вищим на 35-40%, ніж у протокола з відкритими ключами на основі криптосистеми RSA.

У роботі запропонована мова опису протокольних повідомлень, що дозволяє в уніфікованій формі подавати правила формування протокольних повідомлень, і для даної мови розроблен програмний процесор генерації протокольних повідомлень, що дозволяє настроїти вище згадане інструментальне середовище й програмно-апаратні засоби підтвердження справжності на новий чи модифікований протокол аутентифікації.

Для підвищення ступеня захищенності процедури аутентифікації розроблена модель моніторингу мережевої безпеки на основі векторів індикації аномальних дій потенційних порушників. Модель передбачає формування сеансових векторів X, що відображають деякі події (дії суб'єктів ОМ), які можливо пов'язані з порушенням засобів та механізмів захисту.

За результатами формування сеансових векторів X для N випадкових сеансів зв'язку формується пороговий вектор $X_{max} = \{x_{1max}, ..., x_{kmax}\}$, що визначає діапазон змін атрибутів сеансового вектора. На основі порівняння сеансового й порогового векторів формується бітовий вектор індикації аномальних дій $B = \{b_1, ..., b_k\}$ та розраховується ваговий показник ймовірного вторгнення s-користувача в j-сеансі $(PI_{s,j})$. З урахуванням вагових показників вторгнення розраховуються рівні підозрілості дій (LS_s) кожного суб'єкта протягом декількох сеансів мережевого зв'язку.

Підсистема моніторингу безпеки, що запропонована для виявлення вторгнення порушника у обчислювальну мережу, дозволяє суттєво підвищити захищенність процедури аутентифікації та забезпечити контроль за діями суб'єктів ОМ, що особливо важливо в практичних застосуваннях.

У роботі визначені основні програмно-апаратні засоби серверу безпеки корпоративної мережі, який виступає у процедурах аутентифікації у ролі ЦРК, тобто розподільника й гаранта цілісності ключів шифрування суб' єктів

та включає в себе: підсистему визначення повноважень, підсистему контролю та аналізу несанкціонованих дій, підсистему розподілення ключів, підсистему роботи з сигнатурами, криптографічний процесор, базу даних ключів, базу даних повноважень.

Практичною реалізацією досліджень, які виконані у роботі, є розробка й впровадження в Державній службі України з питань технічного захисту інформації (ДС ТЗІ) елементів концепції та архітектури програмно-технічного комплексу захисту інформації в обчислювальних системах та мережах, який забезпечує аутентифікацію суб'єктів, цілісність інформації, що передається та закриття трафіку в мережі. При розробці макетного зразка комплексу застован протокол взаємної аутентифікації суб'єктів ОМ на основі адитивно-константних незвертних функцій, який є сумісний з протоколом стандарту ISO/IEC 9798-1:1991.

Матеріали дисертації використовуються в НТУУ "КПІ" на кафедрі обчислювальної техніки при викладанні учбового курсу "Основи захисту інформації".

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ

1. Аналіз і класифікація основних видів та факторів загроз безпеки в обчислювальних мережах дозволили визначити їх потенційні уразливі місця й виробити основні вимоги до засобів їх захисту. Показано, що ефективність захисту інформації у обчислювальних мережах суттєво залежить від моделей і алгоритмів формування цифрових сигнатур й протокольних повідомлень, а також від методів та засобів модифікації і адаптації протоколів аутентифікації суб'єктів й повідомлень.

2. На основі дослідження математичних моделей спеціальних процедур блочного шифрування на базі незвертних ступеневих функцій в системах відрахувань по модулю запропонована модель адитивно-константного незвертного перетворення і відповідний алгоритм формування протокольних повідомлень й цифрових сигнатур, що відрізняються підвищенною обчислювальною складністю розкриття та наявністю додаткового індивідуального елементу ключа користувача.

3. Розроблена методика оцінки ефективності застосувань і модифікації протоколів аутентифікації суб'єктів і повідомлень у обчислювальних мережах на основі логарифмічного показника відношення криптостійкості протокольних повідомлень до витрат часу на виконання процедури аутентифікації, а також спосіб керування ключами шифрування з адаптацією до необхідного ступеня захищенності процедур аутентифікації та пропускної спроможності мереж, що їх реалізують. Показано, що для підвищення ефективності застосування засобів захисту інформації доцільно

реалізувати цільову адаптацію протоколів аутентифікації на основі засобів аналізу їх рівней захищенності та пропускної спроможності обчислювальних мереж, які реалізують дані протоколи.

4. Для цільового проектування та верифікації моделей і алгоритмів процедур аутентифікації суб'єктів й повідомлень у обчислювальних мережах розроблене спеціалізоване інструментальне середовище. Проведені експериментальні випробування моделей і алгоритмів засобів захисту показали ефективність запропонованих протоколів аутентифікації, що забезпечують збільшення безпечного часу використання ключів на 25-30%, а також збільшення пропускної спроможності обчислювальних мереж, що реалізують дані протоколи.

5. Запропонована мова опису протокольних повідомлень, яка дозволяє в уніфікованій формі записувати правила формування інформаційних обмінів для підтвердження справжності суб'єктів й повідомлень у обчислювальних мережах й на її базі розроблен програмний процесор генерації протокольних повідомлень, що забезпечує автоматизоване формування протоколів аутентифікації, що дозволяє реалізувати настройку інструментального середовища й програмно-апаратних засобів на нову або модифіковану модель процедури аутентифікації.

6. Для підвищення захищенності процедур аутентифікації й забезпечення контролю за діями суб'єктів ОМ, виявлення і нейтралізації дій порушників, що особливо важливо у практичному застосуванні, розроблена та досліджена модель моніторингу мережевої безпеки на основі векторів індикації аномальних дій потенційних порушників засобів захисту у обчислювальних мережах, що забезпечує оцінку ймовірності порушення засобів захисту в кожному сеансі та розподілення суб'єктів мережі за рівнем підозрілості їх дій.

Основні результати дисертації опубліковані в наступних роботах:

1. Стогний Б.С., Широчин С.В., Мухин В.Е. Механизмы защиты информации и безопасность информационно-вычислительных систем и сетей. // Proceedings of Second International Scientific and Technical Conference "Unconventional Electromechanical and Electrotechnical Systems" (ISBN 83-86359-64-1), Szczecin, Poland,- V.2, 1996, p. 603 - 606.

- автором запропоноване спеціалізоване середовище для розробки засобів захисту інформації у обчислювальних мережах, що передбачає виконання оцінок відлагодженності відповідного програмного забезпечення.

2. Широчин В.П., Кириленко А.В., Мухин В.Е., Коцюба Е.Н. Интеллектуализация компьютерных средств контроля и диагностики мощных энергообъектов на основе средств семиотического моделирования // Proceedings of Second International Scientific and Technical Conference

"Unconventional Electromechanical and Electrotechnical Systems" (ISBN 83-86359-64-1), Szczecin, Poland, -V.2, 1996, p. 607 - 610.

- автором запропоновані елементи інтелектуалізації програмного забезпечення контролю та діагностики на основі засобів семіотичного моделювання.

3. Широчин В.П., Кириленко А.В., Коцюба Е.Н., Мухин В.Е. Механизмы защиты информации и сертификации защищенности вычислительных сетей.// Сб. трудов Международной научно-технической конференции "МЕТРОЛОГИЯ'95" - г. Созополь (Болгария). - 1995 г. - с. 48 - 52.

- автором запропонован спеціалізований механізм аутентифікації для підвищення захищенності обчислювальних мереж.

4. Широчин В.П., Широчин С.В., Мухин В.Е. Угрозы безопасности для управляющих систем и компьютерных сетей.// Сб. трудов Международной научно-технической конференции "МЕТРОЛОГИЯ'95"- г.Созополь(Болгария).- 1995 г. - с. 85-90.

- автором класифіковані загрози безпеки в обчислювальних мережах та запропоновані засоби контролю безпеки обчислювальних мереж.

5. Широчин В.П., Мухин В.Е. Проектирование безопасных протоколов аутентификации с элементами защиты информации. // Сб. тезисов докл. Международной конференции "Автоматизация проектирования дискретных систем", г.Минск, 15 - 17 ноября 1995 г. - с. 100

- автором запропонована методика проектування протоколів аутентифікації підвищенного рівня захищенності.

6. Широчин В.П., Мухин В.Е. Метод сдвига ASCII-кода в задачах аутентификации субъектов в локальных вычислительных сетях. // Сб. тезисов докладов Международной конференции "Автоматизация проектирования дискретных систем ", г.Минск, 15 - 17 ноября 1995 г. - с. 101

- автором розроблен спеціальний метод кодування протокольних повідомлень, що забезпечує підвищенний рівень їх захищенності.

7. Широчин В.П., Коцюба Е.Н., Мухин В.Е. Инструментальная среда моделирования для решения задач контроля, диагностики и диспетчеризации управления в энергетике. // Сб. тезисов докладов Третьей Украинской конференции по автоматическому управлению - "АВТОМАТИКА'96"-г.Севастополь, 9-14 сентября 1996 г. - Т.3, с. 164-165.

- автором запропоноване інструментальне середовище для верифікації та цільової адаптації засобів захисту інформації в обчислювальних мережах.

8. Широчин В.П., Мухин В.Е., Великий В.В. Безопасность подсистемы управления в распределенных вычислительных сетях // Сб. тезисов докл. Третьей Украинской конференции по автоматическому управлению - "АВТОМАТИКА'96" - г.Севастополь, 9 - 14 сентября 1996 г. - Т.3, с. 165 - 166

- автором розроблені аналітичні оцінки безпеки програмного забезпечення, що реалізує механізми захисту інформації в обчислювальних мережах.

9. Стогній Б.С., Широчин С.В., Мухін В.Є. Концепція безпеки інформаційно-обчислювальних систем в енергетиці.// Сб. тез допов. Міжнародної науково-технічної конференції "Математичне моделювання в електротехниці й електроенергетиці", м. Львів, Держуніверситет "Львівська політехніка", вересень 1995 р. - с.151 -152.

- автором запропоновані елементи концепції безпеки інформаційно-обчислювальних систем в енергетиці.

10. Широчин С.В., Коцюба Є.М., Мухін В.Є. Моделювання як метод доказів у задачах сертифікації засобів захисту інформації в автоматизованих системах електроенергетики. // Сб. тез допов. Міжнародної науково-технічної конференції "Математичне моделювання в електротехниці й електроенергетиці", м.Львів, Держуніверс. "Львівська політехніка", вересень 1995 р.- с.159 - 160

- автором розроблена методика доказів відповідності та адекватності засобів захисту інформації відповідним стандартам та моделям, що базується на використанні сіток Петрі.

11. Мухин В.Е. Идентификация субъекта и механизмы подтверждения подлинности. // К.- 1995. - 11 с.- Деп. в ГНТБ Украины, 05.04.95, N 742, Ук-95.

- автором запропоновані спеціалізовані засоби підтвердження справжності суб'єктів в обчислювальних мережах.

12. Мухин В.Е. Многооконный графический интерфейс для генерации сообщений процедуры аутентификации в компьютерных сетях. // К. - 1996. - 7 с. - Деп. в ГНТБ Украины, 16.01.96, N 297, Ук-96.

- автором розроблен багатовіконний інтерфейс адміністратора безпеки обчислювальної мережі, що забезпечує зручний процесс формування протокольних повідомлень протоколів аутентифікації.

Мухін Вадим Євгенійович

Спосіб та засоби підвищення ефективності процедур аутентифікації в обчислювальних мережах.

Роботою є рукопис на здобуття вченого ступеня кандидата технічних наук по спеціальності 01.05.03 — Математичне та програмне забезпечення обчислювальних машин та систем. Національний технічний університет України "КПІ".

м.Київ, 1997 р.

Метою дисертаційної роботи є розробка способу та інструментальних засобів забезпечення підвищенного ступеня захищеності процедур та протоколів аутентифікації на основі ефективного вирішення задачі вибору параметрів й розподілення ключів у корпоративних обчислювальних мережах, які дозволяють не знизити їх пропускну спроможність. У результаті — розроблен спосіб керування ключами шифрування з адаптацією протоколів аутентифікації до необхідного ступеня захищеності, а також архітектура інструментального середовища та інтерфейс адміністратора безпеки для цільового проектування протоколів аутентифікації, оцінки їх рівня захищеності та пропускної спроможності мереж, що їх реалізують.

Ключові слова: аутентифікація, обчислювальні мережі, інструментальне середовище, адитивно-константні незвертні функції, цільова адаптація, верифікація

Мухин Вадим Евгеньевич

Способ и средства повышения эффективности процедур аутентификации в вычислительных сетях.

Работой является рукопись на соискание ученой степени кандидата технических наук по специальности 01.05.03 — Математическое и программное обеспечение вычислительных машин и систем. Национальный технический университет Украины "КПИ".

г.Киев, 1997 г.

Целью диссертационной работы является разработка способа и инструментальных средств обеспечения повышенной степени защищенности процедур и протоколов аутентификации на основе эффективного решения задачи выбора параметров и распределения ключей в корпоративных вычислительных сетях, позволяющих не снизить их пропускную способность. В результате — разработан способ управления ключами шифрования с адаптацией протоколов аутентификации к требуемой степени защищенности, а также архитектура инструментальной среды и интерфейс администратора безопасности для целевого проектирования протоколов аутентификации, оценки их уровня защищенности и пропускной способности реализующих их сетей.

Ключевые слова: аутентификация, вычислительные сети, инструментальная среда, аддитивно-константные необратимые функции, целевая адаптация, верификация

Mukhin Vadim E.

Method and tools for effective authenticating procedures in networks.

This scientific work is the manusciprt to submit a thesis for Ph. D. degree on the speciality: 01.05.03 - Mathematical and software aids for computer systems . National Technical University of Ukraine "KPI".

Kiev, 1997.

The goal of the thesis is to develop a method and tools for the security level improvement of authenticating procedures and protocols along with maintaning high level throughput of networks that realize these protocols. The result is the development of method of cypher keys control allowing to realize an adaptation of authenciating protocols to required security level and tool-making environment and interface of security officer for directed adaptation of authenticating protocols and evaluation of their security and networks throughput levels.

Key words: authentication, computer networks, instrumental environment, additive-constant one-way functions, directed adaptation, verification

КОС, 1997 р.
Замов.- 355 тир.- 100

Автор