Якщо про вагові коефіцієнти λ відомо тільки те, що вони належать множині

$$\Delta_\lambda = \left\{ \frac{\lambda}{\lambda_k} \geq 0,\ k = 1, 2, \ldots, s;\ \sum_{k=1}^{s} \lambda_k = 1 \right\},$$

то узагальнений критерій оптимальності можна подати так:

$$Q(x) = \max_{\lambda \in \Delta_\lambda} \sum_{k=1}^{s} \lambda_k Q_k(x). \qquad (14)$$

Розв'язавши задачу нелінійної оптимізації з критерієм оптимальності (14), дістанемо найкращий розв'язок x^* для найгіршого розкладу вагових коефіцієнтів λ_k.

ВИСНОВКИ

Описано різні методи синтезу оптимальних систем і наведено алгоритм та результат розрахунку оптимальної системи управління телекомунікаційними мережами за двома і трьома показниками якості.

Здійснюючи вибір кількості критеріїв при розв'язуванні задачі синтезу оптимальної системи управління, маємо враховувати, що збільшення кількості параметрів, які являють собою частинні критерії оптимальності, з одного боку, допомагає знайти досконалішу систему, а з другого боку, утруднює отримання результуючого критерію оптимальності без введення додаткових обмежень.

Література

1. **Постановка** *завдання створення інтелектуальної мережі в Україні / [Л. Н Беркман, В. Г. Бондаренко, В. Г. Климов, Ю. А. Лев] // Зв'язок.— 1995.— № 1.— С. 25–27.*

2. **Зурман, А. Р.** *Практика проектирования сетей с оборудованием синхронной цифровой иерархии / А. Р. Зурман // Электросвязь.— 1997.— № 1.— С. 11–13.*

3. **Стеклов, В. К.** *Многокритериальная оптимизация системы управления телекоммуникационными сетями / В. К. Стеклов, Л. Н. Беркман, Н. Ф. Карпенко // Зв'язок.— 1999.— № 6.— С. 13–16.*

4. **Беркман, Л. Н.** *Построение интеллектуальной сети / Л. Н. Беркман // Зв'язок.— 1998.— № 2.— С. 14–16.*

5. **Беркман, Л. Н.** *Инвариантные системы управления сетями связи / Л. Н. Беркман // Зв'язок.— 2000.— № 2.— С. 30.*

Рецензент: доктор техн. наук, професор **М. М. Климаш**, Національний університет «Львівська політехніка».

Л. Н. Беркман, Л. П. Крючкова, И. И. Борисенко, С. А. Федюнин, Т. В. Уварова

ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ ОПТИМИЗАЦИИ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ

Рассмотрены критерии оптимизации для систем управления информационно-коммуникационной инфраструктурой. Поставлена задача оптимизации системы управления телекоммуникационной сетью и рассмотрены подходы к ее решению при помощи методов объединения частных критериев.

Ключевые слова: критерии оптимизации; системы управления телекоммуникационной сетью.

L. N. Berkman, L. P. Kryuchkova, I. I. Borysenko, S. A. Fedyunin, T. V. Uvarova

DEFINING OPTIMIZATION CRITERIA FOR CONTROL SYSTEMS

The article describes the optimization criteria for control of information and communication infrastructure. Tasked to optimize the telecom network management system and the possibilities of its solutions with the help of partial criteria combining methods.

Keywords: optimization criteria; telecommunication network management system.

УДК 004.056.53

М. М. СТЕПАНОВ, доктор техн. наук, доцент;
В. В. ВИШНІВСЬКИЙ, доктор техн. наук, професор;
В. Л. БУРЯЧОК, доктор техн. наук, доцент;
І. Р. ПАРХОМЕЙ, доктор техн. наук, доцент,
Державний університет телекомунікацій, Київ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В ІНФОРМАЦІЙНИХ РЕСУРСАХ *ERP*-СИСТЕМ

Розглядаються засоби криптографічного захисту інформації, які можуть бути використані при побудові системи захисту ERP-системи від несанкціонованого доступу до її інформаційних ресурсів.

Ключові слова: ERP-система; несанкціонований доступ; інформаційні ресурси; криптографічний захист інформації; криптографічні операції; апаратні засоби криптографічного захисту інформації; програмні засоби криптографічного захисту інформації.

Постановка проблеми

Із розвитком інформаційних технологій, використовуваних у ERP-системі, зростає і складність забезпечення її інформаційної безпеки, що потребує всебічного аналізу можливих негативних наслідків впливу на неї різних видів інформаційних загроз. До найбільш поширених і різноманітних інформаційних загроз, здатних завдати істотної шкоди інформаційній безпеці ERP-системи, належить несанкціонований доступ (НСД) до її

інформаційних ресурсів. Досвід експлуатації ERP-систем показує, що, незважаючи на тенденцію до підвищення рівня її інформаційної захищеності та постійне розширення інформаційно-телекомунікаційних мереж, вона досить уразлива з погляду НСД. За цих умов криптографічний захист інформації в ERP-системі вважається найбільш надійним, а для інформації, яка передається по її інформаційно-телекомунікаційних каналах великої протяжності — єдиним засобом захисту інформації від НСД. Тому питання, пов'язані з криптографічним захистом ERP-системи від НСД до її інформаційних ресурсів, стають дедалі актуальніші [1–3].

Ступінь розробленості проблеми

ERP-система являє собою територіально розподілену інформаційно-телекомунікаційну систему, в якій інформаційні об'єкти інтенсивно взаємодіють між собою щодо інформації та управління локальними обчислювальними мережами і окремими обчислювальними засобами. При цьому в ERP-системі може використовуватися як імпортне, так і вітчизняне програмне забезпечення, що працює на імпортних обчислювальних засобах і реалізує сучасні інформаційні технології. Через недоліки, притаманні сучасним інформаційним технологіям, та неухильне зростання складності програмно-апаратних засобів ERP-системи кількість шляхів і способів здійснення НСД до її інформаційних ресурсів постійно зростає, а отже, примножується і кількість необхідних для їх нейтралізації засобів криптографічного захисту інформації (ЗКЗІ). Тому для ефективного захисту ERP-системи від НСД важливого значення набуває їх правильний вибір.

Мета статті — аналіз тих ЗКЗІ, які можуть бути використані при розробці засобів захисту в ERP-системі від НСД до її інформаційних ресурсів.

Основна частина

Створення надійно захищеної від НСД ERP-системи — надзвичайно складне завдання. Варто наголосити, що під ***надійно захищеною ERP-системою*** розуміється система, забезпечена захистом у рамках заданого переліку шляхів і способів НСД до її інформаційних ресурсів. Складність цього завдання зумовлена, зокрема, тим, що ERP-система є територіально розподілена система, в якій НСД до її інформаційних ресурсів може здійснюватися не тільки по каналах, характерних для локальних інформаційних систем, а й по каналах, наявність яких спричиняється специфічними особливостями самої системи. До того ж, складність завдання зі створення надійно захищеної від НСД ERP-системи зростає внаслідок урізноманітнення можливих видів фізичного подання інформації в самій системі.

Отже, маємо надзвичайно широкий спектр можливих шляхів НСД із метою впливу на інформаційні ресурси ERP-системи, тоді як для створення надійно захищеної ERP-системи зазначені шляхи мають бути практично перекриті з урахуванням аналізу ризиків, імовірностей їх реалізації та обґрунтованого раціонального рівня витрат [4]. Саме тому до систем шифрування, призначених для закриття інформаційних ресурсів ERP-системи, висуваються жорсткі вимоги. Передусім потрібні достатня стійкість, простота шифрування і дешифрування (з урахуванням способу внутрішньомашинного подання інформації), нечутливість до незначних помилок шифрування, можливість внутрішньомашинної обробки зашифрованої інформації, незначна надмірність інформації за рахунок шифрування тощо. Кожна система шифрування може бути реалізована ***апаратними***, ***програмними*** та ***програмно-апаратними*** ЗКЗІ.

Апаратні ЗКЗІ **(АЗКЗІ)** широко застосовуються в ERP-системі, коли необхідно максимально підвищити рівень захисту її інформації від НСД. До них висуваються підвищені вимоги з безпеки, надійності та швидкодії обробки інформації, яка циркулює в системі. При цьому безпека забезпечується гарантованою стійкістю шифрування і виконанням спеціальних вимог, вибір яких диктується криптографічними стандартами. Надійність і швидкість обробки інформації залежать від складу обраної структури АЗКЗІ, яка включає в себе ряд функціональних вузлів і блоків, що забезпечують задану надійність і швидкість [5; 6].

Окрім цього, використання АЗКЗІ в ERP-системі дозволяє зняти таке питання, як забезпечення цілісності її системи захисту інформації. У більшості сучасних систем захисту від НСД до інформаційних ресурсів ERP-системи застосовується зашивання програмного забезпечення в постійний запам'ятовувальний пристрій (ПЗП) або в аналогічну мікросхему. Таким чином, для внесення змін до ПЗП необхідно отримати доступ до відповідної плати і замінити мікросхему. У разі використання універсального процесора реалізація таких дій потребує застосування спеціального обладнання, що ускладнює проведення інформаційних атак. Використання спеціалізованого процесора у вигляді інтегральної мікросхеми повністю знімає проблему порушення цілісності системи захисту [7].

Неодмінним компонентом усіх реалізованих в АЗКЗІ систем шифрування є гамування, тобто накладення за певним законом гами шифру на відкриті дані. Це пояснюється тим, що метод гамування поєднує в собі високу криптостійкість і простоту реалізації. Найчастіше як генератор гами використовується регістр зсуву зі зворотними

зв'язками. Для підвищення якості генерованої послідовності, як правило, використовується спеціальний блок керування роботою регістра зсуву. Інша можливість поліпшення якості гамування полягає у використанні нелінійних зворотних зв'язків. При цьому поліпшення досягається не за рахунок збільшення довжини гами, а за рахунок ускладнення закону її формування.

Для підвищення продуктивності криптографічних операцій у сучасних АЗКЗІ застосовують такі заходи:

- використовують як ядро АЗКЗІ максимально адаптовані для реалізації більшості криптографічних алгоритмів сучасні високопродуктивні мікропроцесори;
- залучають апаратні прискорювачі, які на апаратному рівні реалізують окремі елементи криптографічних алгоритмів (або повністю криптографічні алгоритми), які не зовсім оптимально лягають на ядро АЗКЗІ (мікропроцесор) із погляду витрат на їх виконання;
- в окремих випадках вводять у дію багатопроцесорні структури.

Висока захищеність від фізичного впливу на АЗКЗІ забезпечується тим, що вони містяться в особливих контейнерах, які не дають змоги змінювати схеми їх функціонування. Крім того, чіпи, на яких реалізуються алгоритми шифрування і здійснюється зберігання ключової інформації, покриваються речовиною спеціального хімічного складу. Спроба подолати цей захисний шар чіпів призводить до самознищення їхньої внутрішньої логічної структури. Захист АЗКЗІ від електромагнітного випромінювання здійснюється їх екрануванням [6].

Апаратні ЗКЗІ зручніші в експлуатації, оскільки дозволяють здійснювати операції шифрування і дешифрування для користувача в прозорому режимі. Більш того, їх легко інсталювати. Вони будуються за модульним принципом, що дозволяє комплектувати їх структуру згідно з вимогами, які ставляться до них як елемента ERP-системи. Проте порівняно з програмними засобами АЗКЗІ менш гнучкі у використанні і обходяться значно дорожче.

Програмні ЗКЗІ **(ПЗКЗІ)** легко копіюються, прості у використанні, їх легко модифікувати відповідно до конкретних потреб. Поряд із цими перевагами ПЗКЗІ мають і важливі недоліки. Програма, що реалізує деяку функцію захисту інформації, може бути досить просто модифікована. Для усунення загрози модифікації необхідно здійснювати контроль цілісності даної програми, а це можливо тільки за допомогою іншої програми. Перевірка цілісності одних програм за допомогою інших не є надійною [7].

Крім того, суттєвим недоліком ПЗКЗІ є використання оперативної пам'яті ERP-системи для операцій із криптографічним ключем, бо протягом певного проміжку часу криптографічний ключ присутній у пам'яті у відкритому вигляді, а отже, може бути з неї витягнутий. Існує ще один недолік, пов'язаний із програмуванням. Це некоректне використання тимчасових файлів, через яке в них може залишатися інформація, придатна для криптографічного аналізу. Досить слабким місцем в ПЗКЗІ є датчик випадкових чисел, використовуваний для формування ключа. Адже жодний метод одержання випадкового числа не може бути визнаний істинно випадковим. У зв'язку із цим при його використанні може бути отриманий слабкий ключ.

Стосовно захисту інформації ПЗКЗІ більш уразливі, ніж АЗКЗІ. Річ у тім, що при створенні різного роду текстових редакторів, СУБД, комунікаційних програм та архіваторів їх розробники керуються передусім міркуваннями максимальної зручності для користувача та принципом безвідмовного функціонування. Тоді питання гарантованого захисту відходять на другий план. Та й загалом принципи безвідмовного функціонування та зручності програмних продуктів змушують вдаватися до різних надмірностей, таких, скажімо, як формат носія даних і формат файла, а це, у свою чергу, послаблює криптографічний захист.

Сучасні ЗКЗІ, застосовувані в ERP-системі, є, як правило, ***програмно-апаратними***, оскільки поєднують у собі гнучкість програмного вирішення з надійністю апаратного. При цьому за рахунок гнучкого програмного компонента можна швидко змінювати користувацький інтерфейс і кінцеві функції продукту, здійснювати його остаточне настроювання. Що ж до апаратного компонента, то він дозволяє захистити від модифікації алгоритм криптографічного перетворення, забезпечити високу захищеність ключового матеріалу та підвищити швидкість роботи.

Аналіз розглянутих сучасних ЗКЗІ показує, що звести їх воєдино, знайти спільні для всіх їх характеристики, виконати порівняння й отримати зрештою об'єктивний результат надзвичайно складно. Сьогодні вибір СКЗІ для ERP-системи здійснюється, здебільшого, на підставі таких критеріїв, як надійність криптоалгоритмів (довжина ключа, стійкість алгоритму); відповідність їх існуючим стандартам і нормативно-правовій базі; наявність сертифікатів державних органів. Поряд із вибором криптоалгоритму не менш гостро постає питання про спосіб його реалізації: апаратний, програмний або програмно-апаратний. Основний критерій тут — вартість як самих ЗКЗІ, так і їх експлуатація.

Висновки

1. Апаратні ЗКЗІ широко застосовуються в ERP-системі, коли необхідно максимально підвищити рівень захисту інформації від НСД. Апаратні ЗКЗІ будуються за модульним принципом, що дає змогу комплектувати їх структуру згідно з вимогами, які висуваються до них як до елемента ERP-системи. Вони захищені від фізичного впливу та від електромагнітного випромінювання.

2. Використання АЗКЗІ в ERP-системі дозволяє забезпечити цілісність системи захисту інформації. Підвищена надійність АЗКЗІ забезпечується за рахунок їх резервування (дублювання). Апаратні ЗКЗІ більш зручні в експлуатації, бо дозволяють здійснювати операції шифрування і дешифрування для користувача в прозорому режимі. Важливо також, що їх легко інсталювати. Утім АЗКЗІ менш гнучкі, ніж ПЗКЗІ та значно дорожчі.

3. Програмні ЗКЗІ легко копіюються, прості у використанні, їх легко модифікувати відповідно до конкретних потреб, проте мають вони й істотні недоліки. Програма, що реалізує деяку функцію захисту інформації, може бути досить просто модифікована. Також суттєвим недоліком є використання оперативної пам'яті ERP-системи для операцій із криптографічним ключем. Досить слабким місцем у ПЗКЗІ є датчик випадкових чисел, використовуваний для формування ключа. Тому з погляду захисту інформації ПЗКЗІ є більш уразливими, ніж АЗКЗІ.

4. Сучасні ЗКЗІ, застосовувані в ERP-системі, як правило, програмно-апаратні. За рахунок гнучкого програмного компонента вони можуть швидко змінювати користувацький інтерфейс та кінцеві функції продукту, здійснювати його остаточне настроювання. При цьому апаратний компонент дозволяє захистити від модифікації алгоритм криптографічного перетворення, забезпечити високу захищеність ключового матеріалу, а також, здебільшого, високу швидкість роботи.

Напрямки подальших наукових досліджень. З розвитком інформаційних технологій удосконалюються шляхи та способи здійснення НСД до інформаційних ресурсів ERP-системи. Тому подальші наукові дослідження доцільно зосередити на вдосконаленні існуючих та розробці нових засобів криптографічного захисту інформації.

Література

*1. **Зырянов, Ю.** Информационная безопасность ERP-систем [Електронний ресурс] / Ю. Зырянов.— Режим доступу:*

http://www.citcity.ru/16501/.

*2. **Чуйко, Ф.** Зачем необходимо защищать ERP-систему и как это сделать [Електронний ресурс] / Ф. Чуйко.— Режим доступу:*

http://ko.com.ua/zachem_neobhodimo_zashhishhat_erp-sistemu_i_kak_jeto_sdelat_88529.

*3. **Сердюк, В. А.** Уязвимость и информационная безопасность ERP-систем [Електронний ресурс] / В. А. Сердюк.— Режим доступу:*

http://www.connect.ru/article.asp?id=3167.

*4. **Проблема** защиты информации в ТКС [Електронний ресурс].— Режим доступу:*

library.tuit.uz/skanir_knigi/book/informacionnaya.../glav_3_4.htm

*5. **Жданов, О. Н.** Методы и средства криптографической защиты: учеб. пособие / О. Н. Жданов, В. В. Золотарев; СибГАУ.— Красноярск, 2007. — 217 с.*

*6. **Криптографическая** защита информации: учеб. пособие / [А. В. Яковлев, А. А. Безбогов, В. В. Родин, В. Н. Шамкин].— Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006.— 140 с.*

*7. **Варлатая, С. К.** Программно-аппаратная защита информации: учеб. пособие / С. К. Варлатая, М. В. Шаханова.— Владивосток: Изд-во ДВГТУ, 2007.— 318 с.*

М. Н. Степанов, В. В. Вишневский, В. Л. Бурячок, И. П. Пархомей

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ИНФОРМАЦИОННЫХ РЕСУРСАХ ERP-СИСТЕМ

Рассматриваются средства криптографической защиты информации, которые могут быть использованы при построении системы защиты ERP-системы от несанкционированного доступа к ее информационным ресурсам.

Ключевые слова: ERP-система; несанкционированный доступ; информационные ресурсы; криптографическая защита информации; криптографические операции; аппаратные средства защиты информации; программные средства защиты информации.

M. M. Stepanov, V. V. Vyshnivski, V. L. Buriachok, I. R. Parchomei

THE CRYPTOGRAPHIC PROTECTION OF INFORMATION CIRCULATING IN ERP-SYSTEMS RESOURCES

The article considers the cryptographic protection of information that can be used in constructing a system ERP-system protection against unauthorized access to its information resources.

Keywords: ERP-system; unauthorized access; information resources; cryptographic protection; cryptographic operations; hardware protection; software protection.