УДК 004.056.5
Кулажський В.І., к.т.н., доцент;
Берестов Д.С.;
Кульчицький О.С.;
Тернавський І.О.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

Вибір засобів криптографічного захисту інформації для захисту ERP-системи від несанкціонованого доступу до її інформаційних ресурсів

Выбор способов криптографической защиты информации для защиты ERP-системы от несанкционированного доступа к ее информационным ресурсам

The choice of ways of cryptographic information protection for defence of ERP-system from unauthorized access to its information resources.

Резюме. В статті розглядаються засоби криптографічного захисту інформації, що 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.

Резюме. В статье 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.

Resume. 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.

Постановка проблеми.

З розвитком інформаційних технологій, які використовуються в ERP-системі, зростає і складність забезпечення її інформаційної безпеки. Забезпечення інформаційної безпеки ERP-системи ґрунтується на глибокому аналізі негативних наслідків впливу на неї різних видів інформаційних загроз. Однією з найбільш поширених і різноманітних інформаційних загроз, яка може завдати суттєву шкоду інформаційній безпеці ERP-системи є 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 є досить уразливою з точки зору НСД. В цих умовах криптографічний захист інформації в ERP-системі вважається найбільш надійним, а для інформації, яка передається по її інформаційно-телекомунікаційним каналам великої протяжності - єдиним засобом захисту інформації від НСД. Тому питання, що пов'язані

з криптографічним захистом ERP-системи від НСД до її інформаційних ресурсів стають досить актуальними [1, 2, 3].

Ступінь розробленості проблеми.

ERP-система представляє собою територіально розподілену інформаційно-телекомунікаційну систему, в якій інформаційні об'єкти інтенсивно взаємодіють між собою за інформацією та управлінням локальними обчислювальними мережами і окремими обчислювальними засобами. При цьому в ERP-системі може використовуватися як імпортне, так і вітчизняне програмне забезпечення, яке працює на імпортних обчислювальних засобах і реалізує сучасні інформаційні технології. Через недоліки, які притаманні сучасним інформаційним технологіям та неухильне зростання складності програмно-апаратних засобів ERP-системи кількість шляхів та способів за якими може здійснюватися НСД до її інформаційних ресурсів постійно збільшується і, отже, збільшується і кількість необхідних для їх нейтралізації засобів криптографічних захисту інформації (ЗКЗІ). В цих умовах при здійсненні ефективного захисту ERP-системи від НСД дуже гостро стає питання щодо їх вибору.

Мета статті.

Аналіз засобів криптографічного захисту інформації, які можуть бути використані при побудові системи захисту в ERP-системі від НСД до її інформаційних ресурсів.

Виклад основного матеріалу.

Створення надійно захищеної ERP-системи від НСД є надзвичайно складним завданням, де під надійно захищеною ERP-системою розуміється система, яка забезпечує її захист у рамках заданого переліку шляхів і способів НСД до її інформаційних ресурсів. Складність цього завдання обумовлена тим, що ERP-система є територіально розподіленою системою, в якій НСД до її інформаційних ресурсів може здійснюватися не тільки по каналах, які характерні для локальних інформаційних систем, але і по каналах, наявність яких обумовлено специфічними особливостями самої системи. Крім цього, складність завдання щодо створення надійно захищеної ERP-системи від НСД обумовлена різноманіттям можливих видів фізичного представлення інформації в самій системі.

Все зазначене зумовлює наявність широкого спектру можливих шляхів НСД з метою впливу на інформаційні ресурси ERP-системи, які при створені надійно захищеної ERP-системи повинні бути надійно перекриті з урахуванням аналізу ризиків, ймовірностей їх реалізації та обґрунтованого раціонального рівня витрат [4]. У зв'язку з цим до систем шифрування, призначених для закриття інформаційних ресурсів ERP-системи, пред'являються ряд вимог, а саме: достатня стійкість, простота шифрування і дешифрування від способу представлення інформації, нечутливість до незначних помилок шифрування, можливість обробки зашифрованої інформації, незначна надмірність інформації за рахунок шифрування і ряд інших. 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 пред'являються підвищені вимоги з безпеки, надійності і швидкодії обробки інформації, яка циркулює в системі. При цьому безпека забезпечується гарантованою стійкістю шифрування і виконанням спеціальних вимог, вибір яких обумовлений криптографічними стандартами. Надійність і швидкість обробки інформації залежать від складу обраної структури АЗКЗІ, яка включає ряд функціональних вузлів і блоків, що забезпечують задану надійність і швидкість. [5, 6].

Крім 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 подібних дій потребує застосування спеціального обладнання, що ускладнює проведення інформаційних атак. Використання спеціалізованого процесора, у вигляді інтегральної мікросхеми, з реалізацією алгоритму роботи повністю знімає проблему порушення цілісності цього алгоритму [7].

Неодмінною компонентою всіх 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 в якості генератора гами використовується регістр зсуву зі зворотними зв'язками. Для підвищення якості послідовності, що генерується, 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.

Підвищення продуктивності криптографічних операцій в сучасних АЗКЗІ може здійснюється шляхом:

застосування в якості ядра АЗКЗІ максимально адаптованих для реалізації більшості криптографічних алгоритмів сучасних високопродуктивних мікропроцесорів;

застосування апаратних прискорювачів, які на апаратному рівні реалізують окремі елементи криптографічних алгоритмів, або повністю криптографічні алгоритми, і які не зовсім оптимально лягають на ядро АЗКЗІ (мікропроцесор) з точки зору витрат на їх виконання;

застосування в окремих випадках багатопроцесорних структур.

Висока захищеність від фізичного впливу на АЗКЗІ забезпечується тим, що вони поміщаються в особливі контейнери, які не дають можливість змінювати схеми їх функціонування. Крім того, чіпи, на яких реалізуються алгоритми шифрування, і здійснюється зберігання ключової інформації, покриваються спеціальним хімічним складом. Спроба подолати цей захисний шар чіпів призводить до самознищення їх внутрішньої логічної структури. Захист АЗКЗІ від електромагнітного випромінювання здійснюється шляхом їх екранування [6].

Апаратні ЗКЗІ є більш зручними в експлуатації, так як дозволяють здійснювати операції шифрування і дешифрування для користувача в прозорому режимі, крім того, їх легко інсталювати. Вони будуються за модульним принципом, що дає можливість комплектувати їх структуру в залежності від вимог, які пред'являються до них як елементу ERP-системи. Однак АЗКЗІ в порівнянні з програмними засобами є у використанні менш гнучкими, і обходяться значно дорожче.

Програмні ЗКЗІ (ПЗКЗІ) легко копіюються, вони прості у використанні, їх легко модифікувати відповідно до конкретних потреб. Поряд із цими перевагами у ПЗКЗІ є й істотні недоліки. Програма, що реалізує деяку функцію захисту інформації, може бути досить просто модифікована. Для усунення загрози модифікації необхідно здійснювати контроль цілісності цієї 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, тому що кінцевий проміжок часу криптографічний ключ, що присутній у пам'яті у відкритому виді може бути з неї витягнутий. Також є ще один недолік, що пов'язаний з програмуванням, наприклад, некоректне використання тимчасових файлів, при якому в них може залишатися інформація що може бути використана для криптографічного аналізу. Досить слабким місцем в ПЗКЗІ є датчик випадкових чисел, який використовується для формування ключа так як жоден метод одержання випадкового числа не може бути визнаний істинно випадковим. У зв’язку із цим при його використанні може бути отриманий слабкий ключ.

З точки зору захисту інформації ПЗКЗІ є більш уразливими, ніж АЗКЗІ. Це обумовлене тим, що при створенні різного роду текстових редакторів, СУБД, комунікаційних програм, архіваторів їх розробники частіше керуються принципом максимальної зручності для користувача та принципом безвідмовного функціонування, а питання гарантованого захисту відсувають на другий план, тому що принципи безвідмовного функціонування та зручності програмних продуктів диктують необхідність ведення різних видів надмірності, зокрема, таких понять як формат носія даних і формат файлу, а це приводить до послаблення криптографічного захисту.

Сучасні ЗКЗІ, що застосовуються в ERP-системі, як правило, є *програмно-апаратними*, тому що вони поєднують у собі гнучкість програмного рішення з надійністю апаратного. При цьому, за рахунок гнучкої програмної компоненти можливо швидко міняти користувацький інтерфейс, кінцеві функції продукту, здійснити його кінцеве настроювання. Апаратна компонента дозволяє захистити від модифікації алгоритм криптографічного перетворення, забезпечити високу захищеність ключового матеріалу й більш високу швидкість роботи.

Аналіз розглянутих вище сучасних ЗКЗІ показує, що звести їх воєдино, знайти для них загальні характеристики, зрівняти й одержати при цьому об'єктивний результат досить складно. На сьогоднішній день, як правило, вибір СКЗІ для ERP-системи здійснюється на підставі таких критеріїв як: надійність криптоалгоритмів (довжина ключа, стійкість

алгоритму); відповідність їх існуючим стандартам і нормативно-правовій базі; наявність сертифікатів державних органів. Крім вибору криптоалгоритму не менш гостро постає питання вибору способу його реалізації: апаратний, програмний або програмно-апаратний. Основним критерієм тут стає 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 можливість комплектувати їх структуру в залежності від вимог, які до них пред'являються, як елементу 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, тому що дозволяють здійснювати операції шифрування і дешифрування для користувача в прозорому режимі, крім того, їх легко інсталювати. Однак АЗКЗІ в порівнянні з ПЗКЗІ є менш гнучкими, і обходяться значно дорожче.

3. Програмні ЗКЗІ легко копіюються, вони прості у використанні, їх легко модифікувати відповідно до конкретних потреб. Поряд із цим ПЗКЗІ мають 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 в ПЗКЗІ є датчик випадкових чисел, який використовується для формування ключа. Тому з точки зору захисту інформації ПЗКЗІ є більш уразливими, ніж АЗКЗІ.

4. Сучасні ЗКЗІ, що застосовуються в ERP-системі, як правило, є програмно-апаратними, оскільки вони за рахунок гнучкої програмної компоненти можуть швидко міняти користувацький інтерфейс, кінцеві функції продукту, робити його кінцеве настроювання, а апаратна компонента дозволяє захистити від модифікації алгоритм криптографічного перетворення, забезпечити високу захищеність ключового матеріалу й найчастіше більш високу швидкість роботи.

5. Проведений аналіз ЗКЗІ показує, що їх вибір для ERP- системи повинен здійснюватися в першу чергу виходячи із завдань, які вони повинні вирішувати, що значно звужує спектр можливих для них технічних рішень. При цьому їх функціональні можливості не повинні превалювати над вартістю й адекватним сервісом їх технічної підтримки.

Напрями подальших наукових досліджень. З розвитком інформаційних технологій удосконалюються шляхи та способи за якими може здійснюватися НСД до інформаційних ресурсів ERP-системи. Тому подальші наукові дослідження доцільно зосередити на розробці нових та удосконалені існуючих засобів криптографічного захисту інформації.

СПИСОК ЛІТЕРАТУРИ.

1. Зырянов Ю. Информационная безопасность ERP-систем. – Режим доступа: http://www.citcity.ru/16501/.
2. Чуйко Ф. Зачем необходимо защищать ERP-систему и как это сделать. – Режим доступа: http://ko.com.ua/zachem_neobhodimo_zashhishhat_erp-sistemu_i_kak_jeto_sdelat_88529.
3. Сердюк В.А. Уязвимость и информационная безопасность ERP-систем. – Режим доступа: http://www.connect.ru/article.asp?id=3167.
4. Проблема защиты информации в ТКС. – Режим доступа: 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. Яковлев А.В. 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.