УДК 004.056

К.О. Кравченко, Б.Б. Самотокін

# ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМАХ КОМПЛЕКСНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ

*Анотація:* Дослідження та оцінка методів шифрування даних і формування ЕЦП для удосконалення методів безпеки системи "IT-Підприємство".

*Ключові слова:* інформаційна безпека, системи комплексного управління підприємством, захист від несанкціонованого доступу, шифрування даних, ЕЦП.

## Вступ

ERP-система – інтегрована система на базі IT для управління внутрішніми і зовнішніми ресурсами підприємства (значущі фізичні активи, фінансові, матеріально-технічні та людські ресурси). Мета системи - сприяння потокам інформації між усіма господарськими підрозділами (бізнес-функціями) всередині підприємства та інформаційна підтримка зв'язків з іншими підприємствами.

ERP-система формує стандартизований єдиний інформаційний простір підприємства на основі централізованої бази даних. Тому інформація щодо діяльності підприємства є однією з найважливіших складових такої системи. Це ядро, яке забезпечує її існування та функціонування. Саме тому захист корпоративної інформації є першочерговою задачею розробників ERP-систем.

У даній статті буде розглянуто систему комплексного управління підприємством "IT-Підприємство".

Система "IT-Підприємство" – це ERP система, що спеціалізується на автоматизації виробництва великих та середніх промислових підприємств і корпорацій. [7]

ERP-система "IT-Підприємство" охоплює всі сторони виробничої, фінансової та господарської діяльності підприємства і складається з безлічі модулів, кожен з яких автоматизує певні завдання.

Умовно всі модулі групуються в такі контури управління:

1. управління виробництвом;
2. логістика;
3. бюджетування та контролінг;
4. управління персоналом;
5. аналіз та оптимізація діяльності;
6. бухгалтерський і податковий облік;
7. адміністрування системи;
8. інструментальні засоби розвитку системи.

“IT-Підприємство” – розподілений додаток, виконаний в трирівневій архітектурі. При цьому виділяється три рівня виконання програми:

Рівень бази даних. З даними працює тільки один процес - сервер бази даних. Як сервер бази даних використовується Microsoft SQL Server 2005/2008 [R2] або Oracle Database 10g / 11g R2.

Рівень сервера додатків. У сервері додатків зосереджена вся бізнес-логіка обробки даних. Сервер додатків формує запити до сервера бази даних, виконує розрахунки і пересилає готові результати розрахунків клієнта. Кількість серверів додатків не обмежена, що забезпечує масштабованість системи.

Рівень клієнта. Клієнтське ПО розташоване на кожній кінцевій клієнтській робочій станції. Клієнтське ПО обмінюється даними з одним із серверів додатків. Завдяки такій побудові система може працювати не тільки в локальній сітці підприємства, а й через Internet.

Схема архітектури системи “IT-Підприємство” наведена на рис. 1.

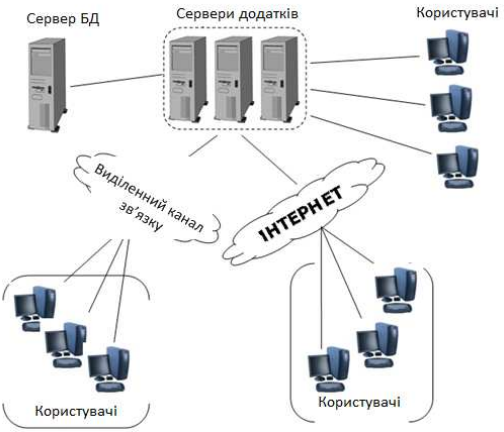


Рис. 1 – Архітектура системи “IT-Підприємство”

## Постановка задачі

Для підвищення ефективності роботи системи “IT-Підприємство” необхідно дослідити її систему захисту та провести оптимізацію обробки передачі інформаційних потоків системи за наступними критеріями:швидкість; захищеність даних; конфіденційність; захист від тупиків.

Отже необхідно вирішити наступні задачі:

1. формування вимог щодо безпеки корпоративної інформації та критеріїв оцінки ступеню захисту інформації;
2. дослідження методів забезпечення інформаційної безпеки, реалізованих у системі “IT-Підприємство” (у даній статті буде приділено

 ISSN 1560-8956

увагу методам шифрування та формування ЕЦП, решту методів буде розглянуто у наступних публікаціях);

3. оцінка рівня інформаційної безпеки системи "ІТ-Підприємство";
4. аналіз існуючих проблем безпеки;
5. формування вимог до усунення існуючих проблем та визначення шляхів вдосконалення системи.

## Формування вимог забезпечення захисту інформації та критеріїв оцінки ступеню безпеки

Для оцінки ступеню захисту інформації візьмемо за основу міжнародний стандарт ISO/IEC 15408:1999 "Критерії оцінки безпеки інформаційних технологій" (Evaluation criteria for IT security), який часто називають "Загальні критерії" (ЗК).[5]

Цей стандарт містить перелік основних вимог по забезпеченню захисту інформації:

1. Безпечна передача даних:*захист від прослуховування; захист від активних атак; шифрування; використання ЕЦП; захист від тупиків.*
2. Аудит роботи користувачів – вимоги до відбору, протоколювання (реєстрації), зберігання та аналізу даних про дії та події, які зачіпають безпеку об'єкта оцінки;
3. Ідентифікація та аутентифікація – вимоги до функцій встановлення та перевірки достовірності заявленого ідентифікатора користувача, а також зв'язування атрибутів безпеки з уповноваженим користувачем;
4. Управління доступом – вимоги по забезпеченню розмежування доступу користувачів до даних.

Другий за важливістю документ (після "Загальних критеріїв"), підготовлений в рамках "Проекту ЗК" – "Загальна методологія оцінки безпеки інформаційних технологій" [6].

Згідно цьому документу, аналіз вразливостей застосовується до всіх функцій безпеки; при цьому не робиться будь-яких припущень щодо коректності їх реалізації, збереження цілісності, можливості обходу тощо.

У таблиці 1 містяться умовні бали, що привласнюються параметрам уразливості в залежності від того, в який діапазон або на який рівень вони потрапляють [6]. Для отримання загального рейтингу потрібно вибрати по одному значенню з обох числових стовпців таблиці і скласти ці десять чисел. При оцінці стійкості функцій безпеки фаза ідентифікації не розглядається (передбачається, що уразливість відома), тому досить вибрати і скласти п'ять чисел з останніх шпальт.

Якщо уразливість можна ідентифікувати і/або використовувати кількома способами, для кожного з них обчислюється клас і з отриманих значень вибирається мінімальне, тобто вразливість характеризується самим простим методом успішного нападу.

Таблиця 1.

Умовні бали, що привласнюються уразливості в залежності від критеріїв, які необхідні для її ідентифікації і використання.

| **Діапазон/Рівень** | **Ідентифікація вразливості** | **Використання вразливості** |
|---|---|---|
| **час для ідентифікації і використання вразливості** | | |
| $<$ 0,5 год | 0 | 0 |
| $<$ доби | 2 | 3 |
| $<$ місяця | 3 | 5 |
| $>$ місяця | 5 | 8 |
| **рівень кваліфікації зловмисника** | | |
| любитель | 0 | 0 |
| спеціаліст | 2 | 2 |
| експерт | 5 | 4 |
| **рівень знань зловмисника про об'єкт оцінки** | | |
| відсутність знань | 0 | 0 |
| загальнодоступні знання | 2 | 2 |
| конфіденційні знання | 5 | 4 |
| **час доступу до об'єкта оцінки** | | |
| $<$ 0,5 год або не помічено | 0 | 0 |
| $<$ доби | 2 | 4 |
| $<$ місяця | 3 | 6 |
| $>$ місяця | 4 | 9 |
| **апаратно-програмні та інші ресурси (устаткування), необхідні для ідентифікації і використання вразливості** | | |
| відсутність обладнання | 0 | 0 |
| стандартне обладнання | 1 | 2 |
| спеціальне обладнання | 3 | 4 |
| заказне обладнання | 5 | 6 |

У табл.2 наведено діапазони рейтингу, які характеризують стійкість функції безпеки.

Таблиця 2.

Діапазони рейтингу, що характеризують стійкість функції безпеки.

| **Діапазон** | **Стійкість функції безпеки** |
|---|---|
| 10-17 | Базова |
| 18-24 | Середня |
| $>$ 24 | Висока |

Згідно з "Загальної методології ", потенціал нападу оцінюється загалом і в цілому по тій же схемі, що і ступінь ризику від наявності вразливостей, з деякими очевидними відмінностями (наприклад, з декількох сценаріїв

 ISSN 1560-8956

нападу вибирається гірший, з найбільшим потенціалом). Вважається, що він є функцією рівня мотивації зловмисника, його кваліфікації і наявних ресурсів. Мотивація впливає час, необхідний для атаки і, можливо, на ресурси і підбір нападників.

У табл.3 наведено діапазони рейтингу, що ілюструють певний потенціал нападу.

Напад може бути успішним, тільки якщо його потенціал не менше рейтингу уразливості. Звідси випливає, зокрема, що уразливості з рейтингом вище 24 стійкі до нападу з високим потенціалом, тому їх практичне використання зловмисниками видається нереальним.

Таблиця 3.

Діапазони рейтингу, що характеризують потенціал нападу.

| **Діапазон** | **Потенціал нападу** |
|---|---|
| < 10 | Низький |
| 10-17 | Середній |
| 18-24 | Високий |
| > 24 | Дуже високий |

## Дослідження методів захисту інформації системи "IT-Підприємство"

У даній статті буде досліджено методи шифрування та формування ЕЦП, реалізовані у системі "IT-Підприємство" (інші методи забезпечення захисту інформації буде досліджено у наступних публікаціях).

### Шифрування даних

Існує два основних способи шифрування даних: симетричне та асиметричне шифрування.

В алгоритмах шифрування з симетричним ключем використовується один ключ, за допомогою якого здійснюється як шифрування, так і розшифрування з використанням одного і того ж алгоритму симетричного шифрування [1].

Таблиця 4.

Відповідність між довжинами ключів

| **Довжина симетричного ключа** | **Довжина відкритого ключа** |
|---|---|
| 56 біт | 384 біт |
| 64 біта | 512 біт |
| 80 біт | 768 біт |
| 112 біт | 1792 біта |
| 128 біт | 2304 біта |

Асиметричне шифрування засноване на парі криптографічних ключів: один ключ є приватним, і відомий тільки кінцевим користувачам, в той час як інший - публічний, і може бути доступний усім. Хоча можна

шифрувати і розшифровувати обома ключами, дані, зашифровані одним ключем, можуть бути розшифровані тільки іншим ключем [1].

Усі асиметричні криптосистеми є об‘єктом атак шляхом прямого перебору ключів, і тому в них повинні використовуватися набагато довші ключі, ніж ті, що використовуються в симетричних криптосистемах, для забезпечення еквівалентного рівня захисту.

У системі “ІТ-Підприємство” реалізовано два алгоритми симетричного шифрування: AES (розмір блоку 128 біт, ключ 128/192/256 біт) та RC2 (розмір блоку 64 біт, ключ 128 біт).

Для оцінки мінімальної стійкості алгоритмів симетричного шифрування, реалізованих у системі будемо вважати, що довжина ключа постійна і дорівнює 128 бітам.

Оцінка стійкості системи до криптоаналізу наведена у таблиці 5:

Отже система має середній рівень захисту від криптоаналізу симетричних шифрів та високий рівень захисту від криптоаналізу асиметричних шифрів.

## Використання ЕЦП

Особливості математичного алгоритму створення й перевірки ЕЦП гарантують неможливість підробки такого підпису сторонніми особами (незаперечність авторства).

У системі “ІТ-Підприємство” ЕЦП реалізовано на базі алгоритмів шифрування RSA і DSA (довжина ключа 1024 біта); для хешування використовуються алгоритми MD5 та SHA1.

Можливі наступні загрози цифрового підпису, при яких зловмисник може: підробити підпис для обраного ним документа; підібрати документ до даного підпису, щоб підпис до нього підходив; підмінити відкритий ключ на свій власний, видаючи себе за власника; обманом змусити власника підписати будь-який документ, наприклад, використовуючи протокол сліпого підпису; підписати будь-який документ від імені власника ключа, якщо закритий ключ вже вкрадено [4].

При використанні надійної хеш-функції обчислювально складно створити підроблений документ з таким же хешем, як і у справжнього. Однак ці загрози можуть реалізуватися через слабкість конкретних алгоритмів хешування, підпису або помилок в їх реалізаціях. Зокрема, таким чином можна провести атаку на SSL-сертифікати і алгоритм хешування MD5.

У загальному випадку злам ЕЦП – це фактично злам алгоритму шифрування, на базі якого реалізована ЕЦП.

Стійкість системи до зламу алгоритму RSA була визначена у попередньому розділі: 26 балів (високий рівень захисту). Проте використання алгоритму хешування MD5 понижує стійкість системи до зламу до 22 балів, тобто до середнього рівня.

 ISSN 1560-8956

Таблиця 5

Стійкість системи до криптоаналізу

| **Симетричне шифрування** | | | |
|---|---|---|---|
| Атака | Критерій оцінки | Оцінка ідентифікації | Оцінка використання |
| *Повний перебір* | час проведення атаки | 0 | 8 |
| | рівень кваліфікації зловмисника | 0 | 2 |
| | рівень знань зловмисника про систему | 5 | 0 |
| | час доступу до системи | 2 | 0 |
| | апаратно-програмні ресурси | 3 | 4 |
| | $\sum$ | 24 | |
| *Лінійний криптоаналіз* | час проведення атаки | 0 | 5 |
| | рівень кваліфікації зловмисника | 0 | 4 |
| | рівень знань зловмисника про систему | 5 | 0 |
| | час доступу до системи | 2 | 0 |
| | апаратно-програмні ресурси | 3 | 4 |
| | $\sum$ | 23 | |
| *Диференційний криптоаналіз* | час проведення атаки | 0 | 5 |
| | рівень кваліфікації зловмисника | 0 | 4 |
| | рівень знань зловмисника про систему | 5 | 0 |
| | час доступу до системи | 2 | 0 |
| | апаратно-програмні ресурси | 3 | 4 |
| | $\sum$ | 23 | |
| ***Рівень захисту*** | | ***23*** | |
| **Асиметричне шифрування** | | | |
| Атака | Критерій оцінки | Оцінка ідентифікації | Оцінка використання |
| *Повний перебір* | час проведення атаки | 0 | 8 |
| | рівень кваліфікації зловмисника | 0 | 2 |
| | рівень знань зловмисника про систему | 5 | 0 |
| | час доступу до системи | 2 | 0 |
| | апаратно-програмні ресурси | 3 | 4 |
| | $\sum$ | 24 | |
| *Розклад модуля n на прості співмножники* | час проведення атаки | 0 | 8 |
| | рівень кваліфікації зловмисника | 0 | 2 |
| | рівень знань зловмисника про систему | 5 | 0 |
| | час доступу до системи | 2 | 0 |
| | апаратно-програмні ресурси | 3 | 4 |
| | $\sum$ | 24 | |
| ***Рівень захисту*** | | ***24*** | |

## Аналіз існуючих проблем та пошук шляхів для їх вирішення

Результати дослідження методів шифрування та створення ЕЦП, реалізованих у системі “IT-Підприємство” наведені у таблиці 6.

Варто зазначити, що дані, які зберігаються у системі є неоднорідними

Таблиця 6.

Результати дослідження методів безпеки системи "ІТ-Підприємство"

| Аспект безпеки | | Оцінка (умовні бали) | Рівень безпеки | Стійкість до атак з потенціалом |
|---|---|---|---|---|
| Шифрування даних | Симетричне | 23 | середній | середній |
| | Асиметричне | 24 | високий | середній |
| Використання ЕЦП | Асиметричне | 22 | середній | середній |

за ступенем важливості. Отже для проведення якісного аналізу необхідно виділити основні категорії захисту:

1. *Мінімальний рівень захисту* – використовується для звичайної (загальнодоступної) інформації. Функції, що забезпечують захист на цьому рівні повинні мати базовий рівень безпеки (10-17 балів за табл..2);
2. *Середній рівень захисту* – використовується для захисту важливої, але не критичної інформації. Рівень безпеки функцій захисту – середній (18-24 балів за табл..2);
3. *Максимальний рівень захисту* – використовується для захисту найбільш важливої та секретної інформації корпорації. Рівень безпеки функцій захисту – високий (> 24 балів за табл.2).

**Аналіз захисту даних за допомогою ЕЦП**

За даними таблиці 6 рівень захисту даних за допомогою ЕЦП знаходиться на середньому рівні. Це пов'язано з використанням алгоритму хешування MD5, що дозволяє отримати два документи з однаковим підписом (колізія другого роду).

Тож для підвищення ступеню захисту даних необхідно замінити використання MD5 іншим алгоритмом хешування, що не дозволить проводити подібні атаки (наприклад, MD6).

**Аналіз захисту даних при використанні шифрування**

За даними таблиці 6 система має наступний рівень захисту при використанні шифрування:

- середній рівень при симетричному шифруванні
- високий рівень при асиметричному шифруванні

При передачі у межах локальної мережі ризик втрати менший, ніж при передачі через Internet, а використання шифрування суттєво сповільнює роботу системи. Тому для передачі секретної інформації використовувати шифрування не обов'язково, а для надійної передачі дуже секретних даних буде достатньо існуючого рівня захисту.

 ISSN 1560-8956

Інша справа – передача секретних та дуже секретних даних через Internet. У цьому разі середнього рівня захисту при використанні симетричного шифрування буде недостатньо, а використання асиметричного шифрування значно зменшить швидкість передачі даних та роботи системи взагалі.

Тому замість використання окремо симетричних та асиметричних методів доцільно використовувати комбіновані методи шифрування, що значно підвищить стійкість шифру.

Комбінована криптосистема - це система шифрування, що поєднує переваги криптосистеми з відкритим ключем з продуктивністю симетричних криптосистем. Симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа, інакше це називається числовою упаковкою.[1]

Більшість гібридних систем працюють таким чином. Для симетричного алгоритму (3DES, IDEA, AES або будь-якого іншого) генерується випадковий сеансовий ключ. Такий ключ як правило має розмір від 128 до 512 біт (залежно від алгоритму). Потім використовується симетричний алгоритм для шифрування повідомлення. У разі блокового шифрування необхідно використовувати режим шифрування (наприклад CBC), що дозволить шифрувати повідомлення з довжиною, що перевищує довжину блоку. Що стосується самого випадкового ключа, він повинен бути зашифрований за допомогою відкритого ключа одержувача повідомлення, і саме на цьому етапі застосовується криптосистема з відкритим ключем (RSA або Алгоритм Діффі - Хеллмана). Оскільки сеансовий ключ короткий, його шифрування займає небагато часу. Шифрування набору повідомлень за допомогою асиметричного алгоритму - це завдання обчислювально більш складна, тому тут краще використовувати симетричне шифрування. Потім достатньо відправити повідомлення, зашифроване симетричним алгоритмом, а також відповідний ключ у зашифрованому вигляді. Одержувач спочатку розшифровує ключ за допомогою свого таємного ключа, а потім за допомогою отриманого ключа отримує і все повідомлення.

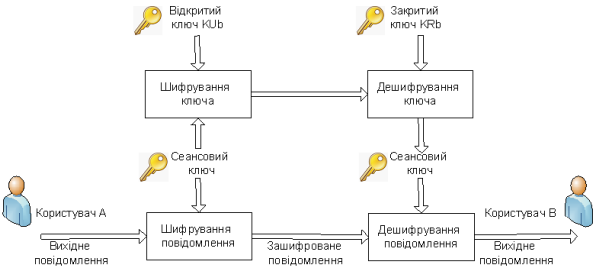


Рис. 2 – Схема комбінованого шифрування

## Висновки

У даній статті було досліджено методи шифрування та формування ЕЦП, реалізовані у системі "IT-Підприємство", та проведено оцінку ступеню безпеки системи. У результаті проведеного аналізу результатів дослідження було виявлено слабкі місця у системі безпеки та сформовано шляхи для вдосконалення системи.

## Література

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.: Наука и техника, 2000. — 187с
2. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа – СПб.: "Наука и техника", 2004. – 384 с.
3. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире – СПб.: Питер, 2003 – 368 с.: ил.
4. Ховард М., Лебланк Д. Защищенный код – М.: "Русская редакция", 2003. – 704 с.: ил.
5. Основные понятия и идеи "Общих критериев", http://www.intuit.ru/department/security/secst/2/2.html
6. Основные понятия и идеи "Общей методологии оценки безопасности информационных систем", http://www.intuit.ru/department/security/secst/2/3.html
7. Корпоративная система управления "IT-Предприятие". Функциональная структура системы, http://www.it.ua/products.php

Отримано 02.03.2011 р.

 ISSN 1560-8956