Анотації

У статті розглядаються принципи обробки реляційних запитів і способи їх реалізації. Як основна операція, що впливає на ефективність виконання запиту, виділена операція з'єднання. Запропоновано варіанти послідовності з'єднання відношень, які мінімізують кількість кортежів у проміжних результатах. Доведено оптимальність таких послідовностей.

В статье рассматриваются принципы обработки реляционных запросов и способы их реализации. В качестве основной операции, влияющей на эффективность выполнения запроса, выделена операция соединения. Предложены варианты последовательности соединения отношений минимизирующих количество кортежей в промежуточных результатах. Доказана оптимальность таких последовательностей.

Principles of processing of relational inquiries and methods of their realization are considered in the article. As a basic operation, influencing on efficiency of implementation of query is select the operation of compound. The variants of sequence of compound of relations of minimizing an amount corteges are offered in intermediate results. The optimumness of such sequences is proved

УДК 65.012.8.

В. В. НОСОВ,
кандидат технічних наук, доцент
професор кафедри інформаційної безпеки
Харківського національного університету внутрішніх справ

МІЖНАРОДНА СТАНДАРТИЗАЦІЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ФІНАНСОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

На сьогодні як у національному, так і в міжнародному нормативному полі стандартизації процесів з інформаційної безпеки в інформаційних системах, і зокрема в фінансових інформаційних системах, відсутня стрункa класифікація наявних та потрібних перспективних стандартів. Тому **актуальним** є завдання системного аналізу опублікованих міжнародних стандартів з інформаційної безпеки у фінансових інформаційних системах та складання їх класифікації за визначеними критерієм, що надасть змогу в майбутнему виявити теоретичні потреби у нових стандартах.

У найбільш загальному вигляді будь-яка економіка складається з процесу виробництва товарів (продуктів, послуг) і комерційної діяльності, основною метою якої є отримання прибутку за допомогою реалізації виробленого товару.

Розвиток натурального товарного обміну (бартеру) привів до виділення з маси товарів одного, який став відігравати роль загального еквіваленту, тобто грошей. Спочатку цим еквівалентом були дорогоцінні метали (в основному золото і срібло). Потім з'явилися карбовані з металу монети. На зміну металевим грошам прийшли «знаки» грошей – паперові гроші. Далі з'явилися інші платіжні засоби.

На цей час як платіжні інструменти можуть використовуватися: готівка (cash) (у формі металевих монет або паперових банкнот); платіжні доручення; платіжні вимоги; вимоги-доручення; векселі; чеки; банківські платіжні картки; інші дебетові й кредитові платіжні інструменти.

Основний грошовий обіг здійснюється в електронних платіжних системах. Структуру типової електронної платіжної системи показано на рис. 1 [1], де основними учасниками системи є:

– **банк-емітент**, який випускає платіжні засоби (наприклад, пластикові картки) і

гарантує виконання фінансових зобов'язань, пов'язаних з їх використанням;

– **банк-еквайєр**, який обслуговує торговельні точки, що приймають до оплати платіжні засоби, і через свої відділення приймає платіжні засоби для обміну на готівку;

– **підприємства торгівлі і сервісу**, які створюють мережу точок обслуговування клієнтів;

– **процесинговий центр**, який обробляє дані про операції, здійснені за допомогою пластикових карток (здійснює обробку запитів на авторизацію; зберігає і пересилає учасникам розрахунків дані про проведені трансакції; фіксує факт операції; підтримує список анульованих платіжних засобів тощо);

– **розрахунковий банк (клірингова організація)**, який проводить взаємні розрахунки між еквайєром та емітентом;

– **тримачі платіжних засобів**;

– **організації-постачальники комунікаційних послуг і центри технічного обслуговування.**

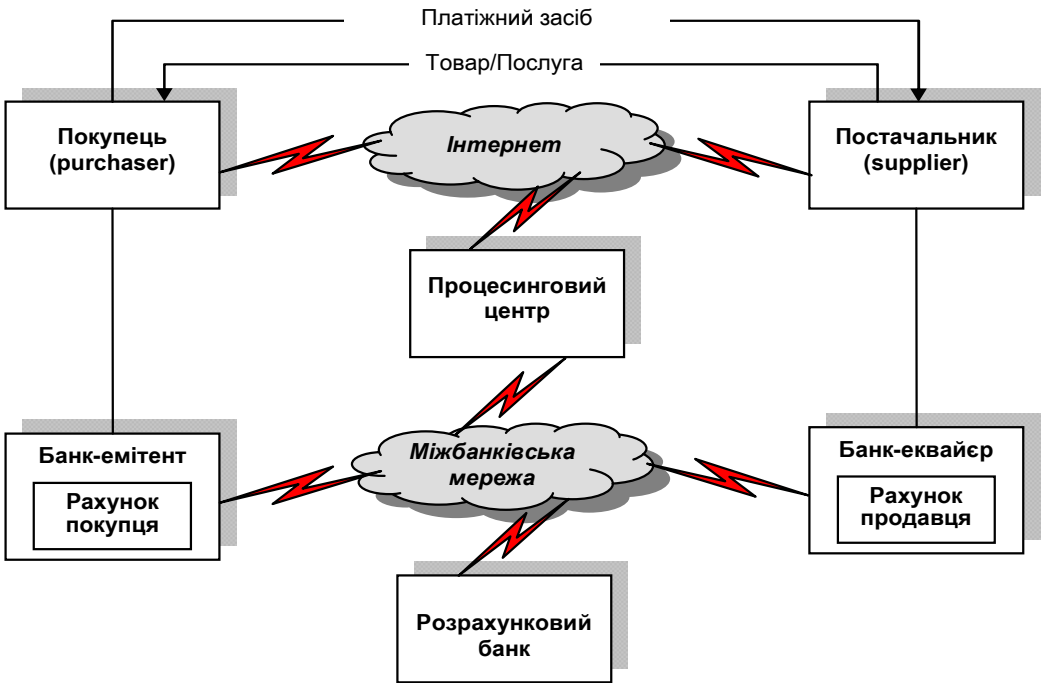

Рис. 1.

Інформаційний тракт трансакції платежу з використанням пластикових карток, у якому здійснюються найбільш поширені загрози фінансовій інформації, представлено на рис. 2 [2].

Рис. 2

Для забезпечення надійної роботи платіжна система має бути захищеною від наявних загроз та вирішувати завдання захисту інформації, основними з яких є:

– аутентифікація учасників інформаційної взаємодії;

– забезпечення конфіденційності і цілісності фінансової інформації при її переданні каналами зв'язку;

– забезпечення неможливості відмови від факту передачі та отримання електронних документів;

– забезпечення юридичної значущості електронних документів, що пересилаються.

Вирішення вказаних завдань неможливе без створення системи захисту інформації. Основою систематизації та структуризації процесів створення, підтримки функціонування й кваліфікаційного аналізу систем захисту інформації є стандарти та інші суміжні документи з інформаційної безпеки.

На сьогодні можна виділити три основні загальновизнані організації, які займаються розробкою міжнародних стандартів, а саме:

– **International Electrotechnical Commission (IEC)** – міжнародна електротехнічна комісія. Розробляє стандарти з електротехніки та відповідні критерії кваліфікаційного оцінювання цих технологій;

– **International Telecommunication Union (ITU)** – міжнародний телекомунікаційний союз. Розробляє стандарти в галузі телекомунікацій;

– **International Organization for Standardization (ISO)** – міжнародна організація стандартизації. Забезпечує розробку стандартів в усіх інших галузях техніки.

Аналіз опублікованих документів зазначених організацій свідчить, що архітектуру безпеки в телекомунікаційних мережах (до яких можна віднести електронні платіжні системи) можна представити як на рис. 3, структуру елементів захисту – як на рис. 4, а організаційні рівні забезпечення інформаційної безпеки – як на рис. 5 [3; 4; 5].

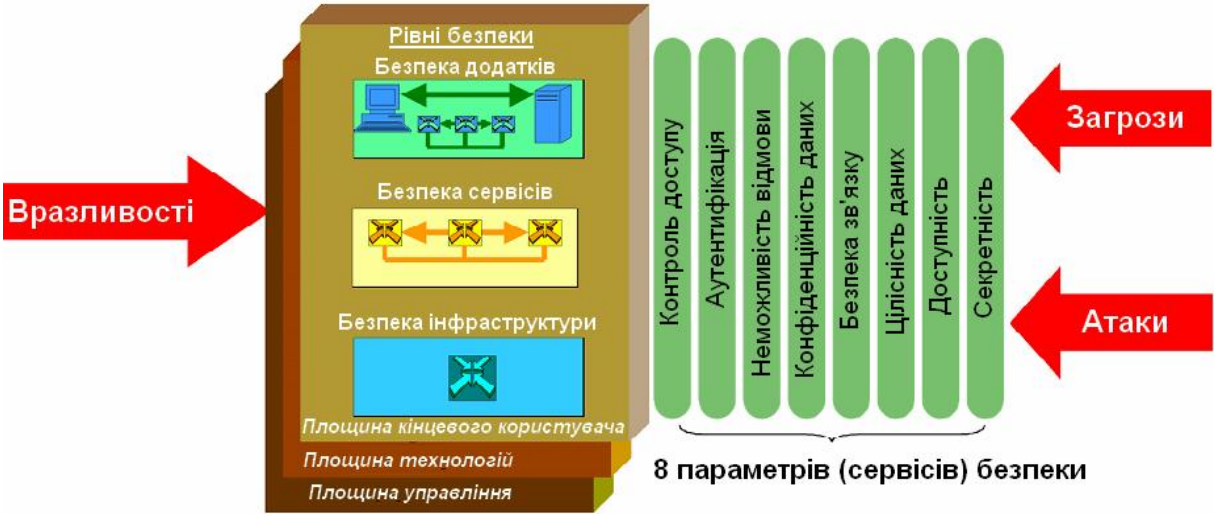

Рис. 3

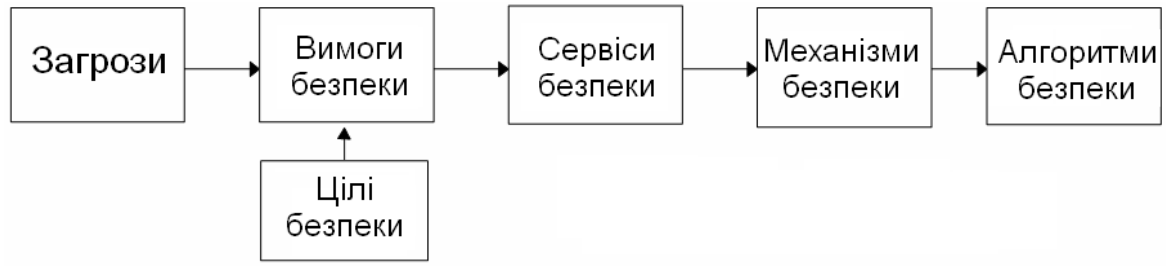

Рис. 4

Регулярний аудит безпеки
Застосування спеціальних засобів безпеки (міжмережеві екрани)
Перевірка безпечності комунікаційного програмного забезпечення
Протоколювання подій та виявлення вторгнень
Забезпечення фізичної безпеки
Наявність адміністратора безпеки

Рис. 5

Окремим аспектам забезпечення інформаційної безпеки у фінансових інформаційних системах ISO присвятило приблизно три десятки документів, які регламентують:

– для сервісу аутентифікації:

1) принципи, вимоги, керівництва використання й алгоритми шифрування Personal Identification Number (PIN) (ISO 9564-1:2002, ISO 9564-2:2005, ISO 9564-3:2003, ISO/TR 9564-4:2004);

2) вимоги до аутентифікаційних повідомлень (ISO 16609:2004);

3) застосування біометрії (ISO 19092:2008);

4) систему міжнародної безпечної нумерації International Securities Identification Numbering System (ISIN) (ISO 6166:2001);

– для сервісів аутентифікації і безпеки комунікацій:

1) принципи та механізми розподілу ключів шифрування (ISO 11568-1:2005, ISO 11568-2:2005, ISO 11568-4:2007, ISO 13492:2007);

2) вимоги до цифрових сертифікатів (ISO 15782-1:2003, ISO 15782-2:2001);

3) практику та політику використання відкритих ключів (ISO 21188:2006);

4) режими і параметри шифрування (ISO/TR 19038:2005);

– для безпеки інфраструктури принципи, вимоги й методи оцінки апаратних криптографічних засобів (ISO 13491-1:2007, ISO 13491-2:2005);

– загальні підходи до інформаційної безпеки для фінансових сервісів (ISO/TR 13569:2005);

– безпеку передачі файлів (ISO 15668:1999);

– специфічні коди обміну, ринків (MIC), платіжних засобів (CFI) (ISO 10383:2003, ISO 10962:2001);

– схему, поля даних, структуру, каталоги, повідомлень (ISO 15022-1:1999, ISO 15022-2:1999);

– оцінку загроз секретності (ISO 22307:2008).

Зазначені документи можна класифікувати відповідно до архітектури безпеки ITU-T X.805 (див. табл. 1).

Окрім загальновідомих організацій IEC, ITU та ISO, у галузі стандартизації процесів з інформаційної безпеки для фінансових інформаційних систем існує ще одна міжнародна організація. У 2006 р. відомими компаніями із забезпечення фінансових послуг American Express, Discover Financial Services, JCB International, MasterCard Worldwide та Visa Inc. було засновано **Раду Стандартів Безпеки в Галузі Платіжних Карт (Payment Card Industry Security Standards Council (PCI SSC))**.

Таблиця 1

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">Рівні безпеки мережі</td></tr>
<tr><td>додатки</td><td>сервіси</td><td>інфраструктура</td></tr>
<tr><td rowspan="7">Площина розгляду мережі</td><td rowspan="5">користувач</td><td rowspan="2">Аутентифікація:
PIN: ISO 9564-1:2002,
ISO 9564-2:2005,
ISO 9564-3:2003,
ISO/TR 9564-4:2004;
біометрія:
ISO 19092:2008
аутентифікаційні повідомлення:
ISO 16609:2004</td><td>Режими і параметри шифрування ISO/TR 19038:2005</td><td rowspan="5">Апаратні криптографічні засоби:
ISO 13491-1:2007,
ISO 13491-2:2005</td></tr>
<tr><td rowspan="4">Структура повідомлень:
ISO 15022-1:1999,
ISO 15022-2:1999</td></tr>
<tr><td>Керівництво з безпеки ISO/TR 13569:2005</td></tr>
<tr><td>Безпека передачі файлів ISO 15668:1999</td></tr>
<tr><td>Специфічні коди обміну, ринків, платіжних засобів: ISO 10383:2003,
ISO 10962:2001</td></tr>
<tr><td>Оцінка загроз секретності ISO 22307:2008</td><td></td><td></td></tr>
<tr><td>технології</td><td></td><td>Система міжнародної безпечної нумерації (ISIN) ISO 166:2001</td><td></td></tr>
<tr><td rowspan="3">управління</td><td>Безпека комунікацій - розподіл ключів шифрування:
ISO 11568-1:2005,
ISO 11568-2:2005,
ISO 11568-4:2007</td><td rowspan="3">Безпека комунікацій - елементи ключів шифрування
ISO 13492:2007</td><td rowspan="3"></td></tr>
<tr><td>Безпека комунікацій - цифрові сертифікати:
ISO 15782-1:2003,
ISO 15782-2:2001</td></tr>
<tr><td>Політика використання відкритих ключів
ISO 21188:2006</td></tr>
</table>

PCI SSC розробила і підтримує розвиток трьох складників загального стандарту захисту даних тримачів платіжних карток Payment Card Industry Security Standard (рис. 6 [2]), які адресовані:

– **PCI PED** - виробникам Пристроїв вводу PIN (manufacturers PIN Entry Devices);

– **PCI PA-DSS** - розробникам і постачальникам платіжних додатків (software developers Payment Application Vendors);

– **PCI DSS** - торговцям і процесорам (merchants&processors), які оперують даними тримачів платіжних карток.

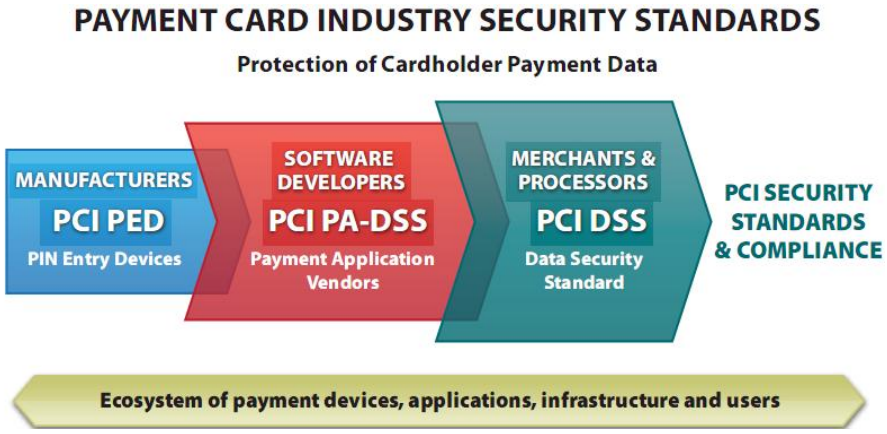

Рис. 6.

Об'єктами захисту в стандарті є елементи:
- даних тримачів карток;
- критичних аутентифікаційних даних.

Таблиця 2 ілюструє найбільш часто використовувані елементи цих даних, які або дозволено, або заборонено зберігати в системі, та визначено, наявності чи відсутності вимог щодо захисту цих елементів.

Таблиця 2

	Елемент даних	Зберігання дозволено	Потрібний захист	Вимога 3.4 PCI DSS
Дані тримача картки	Номер платіжної картки (PAN)	ТАК	ТАК	ТАК
	Ім'я тримача картки (Cardholder Name)[1]	ТАК	ТАК[1]	НІ
	Сервісний код (Service Code)[1]	ТАК	ТАК[1]	НІ
	Дата закінчення терміну дії картки (Expiration Date)[1]	ТАК	ТАК[1]	НІ
Критичні аутентифікаційні дані[2]	Вся магнітна доріжка картки[3]	НІ	Не визначено	Не визначено
	CAV2/CVC2/ CVV2/CID	НІ	Не визначено	Не визначено
	PIN / PIN Block	НІ	Не визначено	Не визначено

[1] Вказані елементи даних мають бути захищені, якщо зберігаються спільно з PAN. Цей захист повинен відповідати вимогам PCI DSS щодо безпеки середовища даних тримачів карток. Інші вимоги законодавства (наприклад, що стосуються захисту персональних даних клієнтів, охорони особистих відомостей, крадіжки особи або безпеки даних) можуть полягати у додатковому захисті цих даних або розкритті вживаних компанією методів, якщо персональні дані споживачів накопичуються компанією. Вимоги PCI DSS, незважаючи на це, не застосовуються, якщо PAN не зберігається, не обробляється і не передається

[2] Критичні аутентифікаційні дані не повинні зберігатися після авторизації (навіть у зашифрованому вигляді)

[3] Всі дані з магнітної доріжки картки, образу магнітної доріжки чіпу або іншого пристрою

У таблиці 2 скорочення мають таку розшифровку:

- CID – Card Identification Number (American Express and Discover payment cards);
- CAV2 – Card Authentication Value 2 (JCB payment cards);
- CVC2 – Card Validation Code 2 (MasterCard payment cards);
- CVV2 – Card Verification Value 2 (Visa payment cards).

PCI SSC запровадила систему сертифікації платіжних систем компаній, які надають послуги електронних платежів і відповідають стандарту безпеки індустрії платіжних карток PCI DSS. Процес сертифікації інформаційних систем компаній складається з трьох кроків:

- **оцінювання (Assess)**: ідентифікуються дані тримачів платіжних карток, проводиться інвентаризація інформаційних ресурсів і бізнес-процесів, що беруть участь у процесингу платіжних карток, аналізуються наявні недоліки, через які можуть бути реалізовані загрози до даних тримачів платіжних карток;
- **вдосконалення (Remediate)**: усуваються недоліки та виключається зберігання в системі даних тримачів платіжних карток там, де це можливо;
- **видача сертифіката відповідності (Report)** – опис, оформлення та затвердження усіх попередніх кроків із виданням відповідного сертифіката компаніям, які надають послуги електронних платежів і відповідають стандарту безпеки індустрії платіжних карт PCI DSS.

Кожний основний член PCI SSC встановлює свій порядок сертифікації систем електронних платежів із картками власного бренду на відповідність вимогам PCI DSS.

PCI SSC для перевірки на відповідність вимогам PCI DSS визначає:

- **Акредитованих оцінювальників безпеки** (Qualifed Security Assessor (QSA)) – організації, які уповноважені PCI SSC проводити аудит щодо відповідності вимогам PCI DSS;
- **Акредитованих оцінювальників безпеки платіжних додатків** (Payment Application Qualified Security Assessors (PA-QSAs)) - організації, які уповноважені PCI SSC проводити аудит платіжних додатків щодо відповідності вимогам PCI PA-DSS;
- **Сертифіковані компанії, що здійснюють сканування** (Approved Scanning Vendor (ASV)), – компанії, які уповноважені PCI SSC проводити перевірку на відповідність вимогам PCI DSS шляхом зовнішнього сканування з інтернет-мереж торгових організацій та постачальників послуг.

Також PCI SSC представляє для організацій торгівлі та сервіс-провайдерів (merchants and service providers) комплекс документів під загальною назвою PCI Data Security Standard Self-Assessment Questionnaire (PCI DSS SAQ) – **Опитувальник (анкета) для самооцінювання на відповідність вимогам PCI DSS**.

PCI DSS SAQ складається із таких компонентів:

- таблиця визначення типу інформаційної системи організації торгівлі та сервіс провайдера, яка буде перевірятися;
- чотири типи (від A до D) Опитувальників PCI DSS SAQ для відповідних інформаційних систем.

Структуру документів стандарту захисту даних тримачів платіжних карток Payment Card Industry Security Standard наведено на рис. 7.

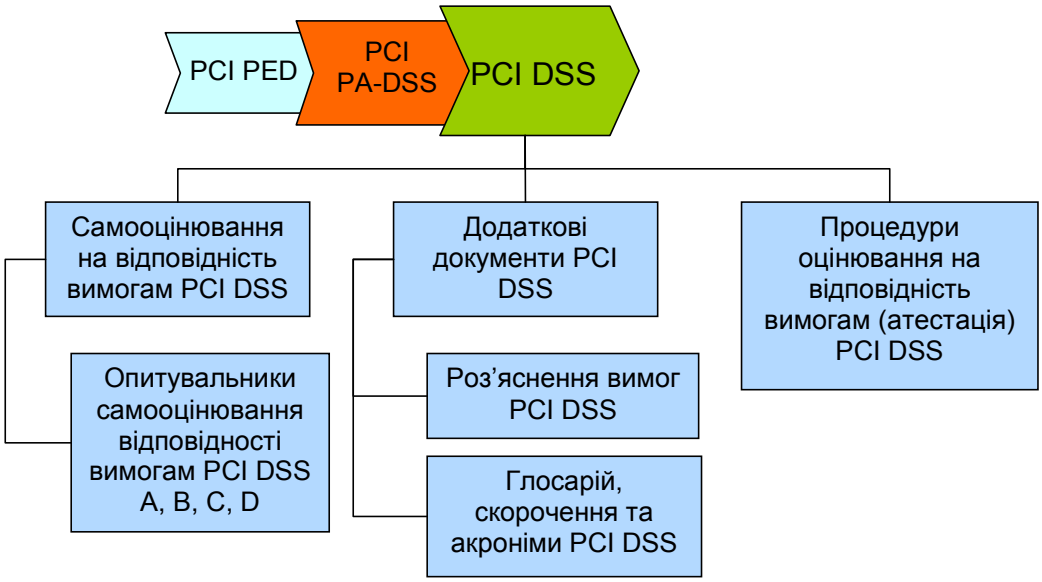

Рис. 7

Власне PCI DSS описує 12 загальних вимог (які об'єднано в 6 логічно зв'язаних груп) до сервісів безпеки інформаційних систем торгових організацій, провайдерів послуг та фінансових інституцій, які обробляють, зберігають і передають дані тримачів платіжних карток. Ці вимоги також можна класифікувати відповідно до архітектури безпеки ITU-T X.805 (див. табл. 3).

Таблиця 3

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">Рівні безпеки мережі</th></tr>
<tr><th>додатки</th><th>сервіси</th><th>інфраструктура</th></tr>
<tr><td rowspan="6">Площина розгляду мережі</td><td rowspan="6">користувач</td><td>Вимога 3. Забезпечити безпеку даних тримачів карток, що зберігаються</td><td rowspan="2"></td><td rowspan="6"></td></tr>
<tr><td>Вимога 4. Шифрувати дані тримачів карток при передачі їх через відкриті загальнодоступні мережі</td></tr>
<tr><td colspan="2">Вимога 6. Розробити і підтримувати безпечні системи і додатки</td></tr>
<tr><td>Вимога 7. Обмежити доступ до даних тримачів карток лише службовою необхідністю</td><td rowspan="2">Вимога 8. Призначити унікальний ідентифікатор кожній особі, що має доступ до комп'ютерної мережі</td></tr>
<tr><td>Вимога 9. Обмежити фізичний доступ до даних тримачів карток</td></tr>
</table>

<table>
<tr><td rowspan="5"></td><td></td><td colspan="3">Рівні безпеки мережі</td></tr>
<tr><td></td><td>додатки</td><td>сервіси</td><td>інфраструктура</td></tr>
<tr><td>технології</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">управління</td><td colspan="2">Вимога 2. Не використовувати встановлені виробником системні паролі та інші параметри безпеки</td><td rowspan="3">Вимога 1. Розробити й забезпечити підтримку конфігурацій міжмережевих екранів для захисту даних тримача карти</td></tr>
<tr><td>Вимога 5. Використовувати й регулярно оновлювати антивірусне програмне забезпечення</td><td>Вимога 11. Регулярно перевіряти системи і процеси забезпечення безпеки</td></tr>
<tr><td colspan="2">Вимога 10. Відстежувати і контролювати будь-який доступ до мережевих ресурсів і даних тримачів карт</td></tr>
<tr><td colspan="3">Вимога 12. Підтримувати політику, що визначає правила інформаційної безпеки для співробітників і партнерів</td></tr>
</table>

Таким чином, отримані класифікації відповідно до архітектури безпеки ITU-T X.805 дають змогу системно представити ступінь охоплення стандартизації інформаційної безпеки у фінансових інформаційних системах та виявити теоретичні потреби в нових стандартах.

Література

1. Деднев М. А. Защита информации в банковском деле и электронном бизнесе / Деднев М. А., Дыльнов Д. В., Иванов М. А. – М. : КУДИЦ-ОБРАЗ, 2004. – 512с. – (СКБ – специалисту по компьютерной безопасности).
2. Офіційний сайт Payment Card Industry Security Standards Council (PCI SSC) [Електронний ресурс]. – Режим доступу : www.pcisecuritystandards.org.
3. ITU-T X.805. Security architecture for systems providing end-to-end communications [Електронний ресурс]. – Режим доступу : http://www.itu.int.
4. ISO/IEC 18028-2. Information technology – Security techniques – IT network security – IT network security. Part 2: Network security architecture [Електронний ресурс]. – Режим доступу : http://www.iec.ch.
5. ITU-T E.408. Telecommunication networks security requirements [Електронний ресурс]. – Режим доступу : http://www.itu.int.

Надійшла до редколегії 04.06.2009

Анотації

Стисло описана структура типової фінансової інформаційної системи та основні завдання забезпечення в ній інформаційної безпеки. За результатами аналізу опублікованих стандартів міжнародних організацій IEC, ITU, ISO та PCI SSC, які стосуються фінансових інформаційних систем, та з метою виявлення теоретичних потреб у нових стандартах розроблено та наведено класифікації наявних стандартів у відповідності з архітектурою безпеки ITU-T X.805.

Кратко описана структура типовой финансовой информационной системы и основные задачи обеспечения в ней информационной безопасности. По результатам анализа опубликованных стандартов международных организаций IEC, ITU, ISO и PCI SSC, которые касаются финансовых информационных систем, и с целью выявления теоретических потребностей в новых стандартах разработаны и приведены классификации существующих стандартов в соответствии с архитектурой безопасности ITU-T X.805.

The structure of the model financial IT system is briefly described. For it the basic tasks of IT security are indicated. For the proper documents of IEC, ITU, ISO and PCI SSC is developed and resulted to classification of existent standards in accordance with security architecture ITU-T X.805. It will help to define theoretical requirements in new standards.