considering the system approach and enterprise peculiarities;

4. produce post instructions for international standards (ISO 27001, PCI DSS) implementation.

The ISMS "Matrix" is implemented as a relational database with menus, screen input-output forms and printable reports in MS Access 2000 Database format (*.mdb).

The database itself consists of two main tables, risk list and common classifying elements lists (see fig. 1). The tables are linked on the scheme not by ID fields, but by the names of elements. This is arranged for better flexibility in case of changes in data structures during the ISMS development or customisation.

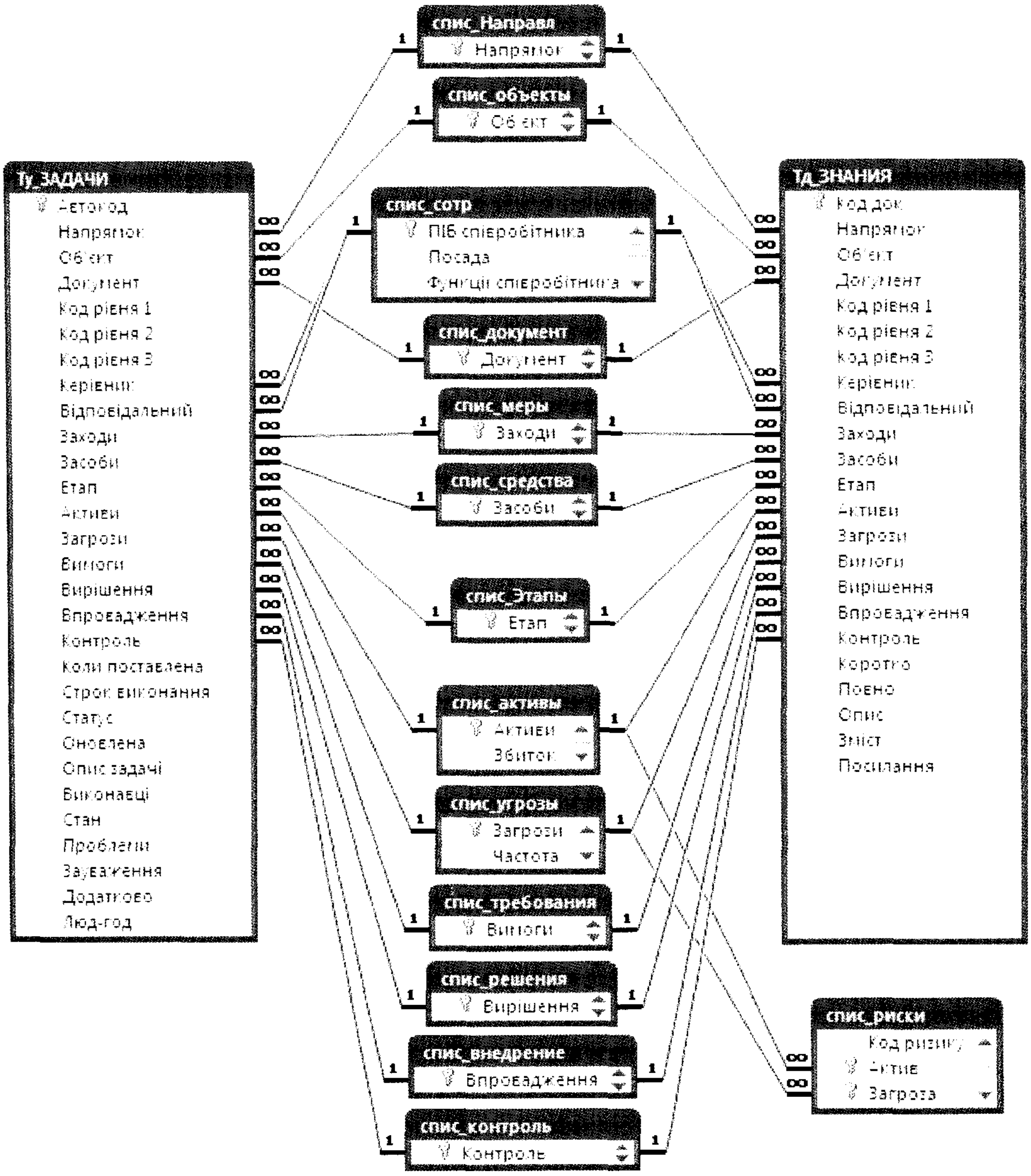

Fig. 1. Database scheme of the ISMS "Matrix"

The first main table "Тд_ЗНАНИЯ" contains the information about the input normative documents and regulations. The second main table "Ту_ЗАДАЧИ" contains the information about all the dispatched tasks: current, planned and archived.

Risk assessment is performed by forming asset-threat relations in "Risk list" table ("спис_риски"). For quantitative estimations, numerical fields are provided in tables of assets ("спис_активы") and threats ("спис_угрозы").

because risk assessment is a dedicated function, providing both detailed risk estimations and pivot charts

8. Limited audit support is resolved by the variety of reports and pivot charts, thus allowing to pass different audits without reassessment.

Application of the ISMS "Matrix"

Presently, ISMS "Matrix" is positioned as an information security management, international IT standard implementation and decision support system. Its development and full support are continuously provided by the authors. System adaptation to the structure and the strategy of a specified organisation, with taking the business processes peculiarities into consideration, is available on demand. The ISMS "Matrix" was applied in the following organisations:

1. "MTN" Ltd., Kyiv: to manage the corporate network security and produce post descriptions based on corporate regulation in 2007–2008.

2. Ukrinbank, Kyiv: to audit the banking security system and facilitate introducing PCI DSS and ISO 27001 standards in 2009-2010.

Conclusion

Using all of its potential, ISMS application allows to:

1. increase the efficiency of management decisions;

2. systematise and unite the forces of different specialists for the achievement of common goal (implementation of one or several IS standards simultaneously);

3. estimate the current state of ISS and its compliance to a certain IS standard;

4. obtain pivot reports on ISS state, current and finished jobs (in extension, updating, etc.)

Due to scarcity of resources devoted to the development of the ISMS "Matrix", wide encompassing of IS management processes is compensated by inability to operate at lower technical levels (for example, collecting or analyzing log files). To compensate these challenges and accelerate the development of the product, it is needed to invest money to support the developed or devote a professional development team.

Presently, the ISMS "Matrix" is distributed freely at the developers' website [6]. Comments, user feedback and inquiries are welcome.

References

1. Постанова правління Національного банку України від 28 жовтня 2010 р. № 474 "Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України".

2. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) : ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [чинний від 28.10.2010]. – К.: Національний банк України, 2010. – 49 с. – (Галузевий стандарт України).

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [чинний від 28.10.2010]. – К.: Національний банк України, 2010. – 163 с. – (Галузевий стандарт України).

4. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев – К.: ООО «ТИД «ДС», 2004. – 992 с.

5. Proctor P. MarketScope for IT Governance, Risk and Compliance Management [Electronic resource] : [Gartner RAS Core Research Note G0017S755]/Paul E. Proctor, Mark Nicolett. – 109KB. – Access mode: http:// www.gartner.com/ Display Document?id=1361628

6. Domarev V. V. Безопасность информационных технологий [Electronic resource]: [Personal website]/ V. V. Domarev – Access mode: http:// www.security.ukrnet.net/ modules/ news/ article.php ?storyid=505.