Коломиец Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ»
E-mail: box144a@ukr.net
Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ»
Kolomytsev Mikhail, Ph.D., Associate Professor of Physics and Technical Institute of NTU "KPI"

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ»
E-mail: svetlana@pti.kpi.net
Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ»
Nosock Svetlana, Ph.D., Associate Professor of Physics and Technical Institute of NTU "KPI"

Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент Фізико-технічного інституту НТУУ «КПІ»
E-mail: graiv@voliacable.com
Грайворонский Николай Владленович, кандидат физико-математических наук, доцент Физико-технического института НТУУ «КПИ»
Graivoronsky Nikolay, the candidate of physical and mathematical sciences, associate professor of Physical and Technical Institute of NTU "KPI"

УДК 004.021:004.056

МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ СУІБ «МАТРИЦЯ»

Дмитро Домарєв, Валерій Домарєв, Сергій Прокопенко

Обґрунтована актуальність питань оцінювання захищеності інформаційних систем. Наведено область застосування, призначення і процедуру пропонованої методики. Власне процедура пропонованої методики складається з первинного опитування клієнта, визначення активів, визначення важливості активів за словесною шкалою, пошуку вразливостей визначених активів, визначення загроз, що походять від знайдених вразливостей, визначення ступеня небезпеки знайдених загроз за словесною шкалою, переводу важливості активів та ступеня небезпеки загроз у кількісні оцінки, підрахування оцінок ризиків, ранжування за сумарними оцінкам ризиків, визначення найбільш вразливих активів та найбільш небезпечних загроз, ранжування вразливостей кожного активу, складання рекомендацій щодо усунення вразливостей, оформлення звіту. Для практичної реалізації пропонованої методики застосовано систему управління інформаційною безпекою «Матриця». Зроблено висновки про переваги пропонованої методики.
Ключові слова: *оцінювання захищеності інформаційних систем, аудит інформаційної безпеки, оцінювання ризиків ІБ, оцінка ризику ІБ, управління інформаційною безпекою, СУІБ «Матриця».*

Вступ. Актуальність питань оцінки захищеності інформаційних систем (ІС) в Україні почала зростати у 2005 р. з появою міжнародних стандартів з управління інформаційною безпекою (ІБ), більшість з яких містять вимоги щодо оцінювання стану ІБ. Виникла потреба у сертифікації на відповідність стандартам ІБ для зміцнення авторитету організацій серед партнерів та клієнтів. Процедура сертифікації неодмінно передбачає аудит стану ІБ організації.

Методика, запропонована в даній статті спирається на дослідження в області ІБ [1, 2], українські та міжнародні стандарти з управління інформаційною безпекою [3, 4, 7, 8] та методики оцінювання ІБ [5, 9]. Для практичної реалізації пропонованої методики авторами була застосована система управління інформаційною безпекою (СУІБ) «Матриця» [6].

Областю застосування пропонованої методики є аудит ІБ та оцінювання захищеності комп'ютерних систем.

Призначеннями пропонованої методики є оцінювання загального рівня захищеності комп'ютерної системи, Виявлення найбільш вразливих активів і найбільш небезпечних загроз для конкретної організації, визначення пріоритетів в усуненні вразливостей ІБ.

Процедура пропонованої методики заснована на оцінці ризиків ІБ та є наступною:

1. Первинне опитування клієнта;

2. Визначення активів;
3. Визначення важливості активів за словесною шкалою;
4. Пошук вразливостей визначених активів;
5. Визначення загроз, що походять від знайдених вразливостей;
6. Визначення ступеня небезпеки знайдених загроз за словесною шкалою;
7. Перевод важливості активів та ступеня небезпеки загроз у кількісні оцінки;
8. Підрахування оцінок ризиків;
9. Ранжування за сумарними оцінкам ризиків. Визначення найбільш вразливих активів та найбільш небезпечних загроз;
10. Ранжування вразливостей кожного активу;
11. Складання рекомендацій щодо усунення вразливостей та оформлення звіту.

Кожен з наведених етапів описаний нижче.

Первинне опитування клієнта

На цьому етапі необхідно з'ясувати та визначити наступне:

1. Структура мережі: фізична і логічна, розміщення устаткування, в т.ч. характеристика приміщень;
2. Набір перевірок безпеки: бажані та рекомендовані;
3. Активи: перелік та їх важливість для клієнта;
4. Загрози: перелік та рівень небезпеки для клієнта;
5. Облікові записи (необхідні для виконання обраних перевірок): імена користувачів, паролі, точки входу.

Визначення активів

Щоб визначити список активів цільової організації, слід перелічити усі малі об'єкти клієнта, що схильні до загроз інформаційної безпеки (а отже спричиняють ризики). Список активів повною мірою залежить від структури і особливостей цільової організації.

Активами можуть бути не лише фізичні об'єкти (сервери, термінали, камери, друковані документи і т.п.), але й інформація (файли, згенеровані ключі і т.п.)

Експерти перевіряючої сторони складають остаточний список активів на підставі первинного опитування.

Визначення важливості активів за словесною шкалою

Визначення важливості активів відбувається за словесною шкалою.

Дані первинного опитування клієнта рецензуються на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft).

Наприкінці цього етапу кожен актив повинен мати словесну оцінку важливості. *Рекомендовані ступені важливості:* Критичний, Важливий, Рядовий, Маловажливий, Неважливий.

Приклад результату даного етапу наведений в табл. 3.

Пошук вразливостей визначених активів

Пошук вразливостей визначених активів виконується у відповідності до спектру доступних перевірок:

1. Перевірка на проникнення (penetration test);
2. Визначення зловмисників серед співробітників цільової організації (insiders);
3. Аналіз налаштувань (конфігурації);
4. Аналіз фізичного доступу до об'єктів комп'ютерної мережі;
5. Інші перевірки ІБ.

Визначення загроз, що походять від знайдених вразливостей

Одна вразливість може бути джерелом декількох загроз (наприклад, фізичний доступ до сервера може бути причиною як знищення так і захоплення устаткування). Тому слід визначити загрози для кожної знайденої вразливості на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft).

Наприкінці цього етапу має бути складений перелік загроз.

Визначення ступеня небезпеки знайдених загроз за словесною шкалою

Визначення рівня небезпеки загроз відбувається за словесною шкалою.

Дані первинного опитування клієнта рецензуються на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft).

Наприкінці цього етапу кожна загроза повинна мати словесну оцінку рівня небезпеки. *Рекомендовані міри важливості*: Критичний, Важливий, Середній, Низький, Малоймовірний

Приклад результату даного етапу наведений в табл. 4.

Перевод важливості активів та ступеня небезпеки загроз у кількісні оцінки

Для автоматизованої оцінки ризиків слід перевести попередньо отримані словесні оцінки активів і загроз в кількісні. Рекомендовані шкали оцінок, що приведені в табл. 1 та 2, розроблені на основі методик [5, 9]. Приклад результату даного етапу наведений в таблицях 3 та 4.

Таблиця 1.

Рекомендована шкала оцінок важливості активів

Важливість активу	**Збиток при реалізації загроз (умовна оцінка)**
Критичний	5
Важливий	4
Рядовий	3
Маловажливий	2
Неважливий	1

Таблиця 2

Рекомендована шкала оцінок ступеня небезпеки загроз

Рівень небезпеки загрози	**Вірогідність реалізації (умовна оцінка)**
Критичний	5
Важливий	4
Середній	3
Низький	2
Малоймовірний	1

Приклад оцінок важливості активів Таблиця 3

Актив	**Важливість**	**Збиток**
Сервер доступу до Інтернет	Критичний	5
Сервер 1С:Підприємство, термінал.сервер	Критичний	5
Головний контролер домену	Критичний	5
Поштовий сервер	Важливий	4
Запасний контролер домену, сервер БД	Важливий	4

Приклад оцінок рівня небезпеки загроз Таблиця 4

Загроза	**Рівень небезпеки**	**Частота**
Переповнення буфера	Критичний	5
Несанкціоноване отримання прав	Важливий	4
Виток інформації	Важливий	4
Віддалене виконання коду	Середній	3
Відмова в обслуговуванні	Низький	2

Підрахування оцінок ризиків

Для автоматизованого підрахування оцінок ризиків в СУІБ «Матриця», слід виконати наступні дії у пункті головного меню «Списки елементів»:

1. Ввести в СУІБ виявлені активи у вигляді списку, що містить назви активів і значення збитку, згідно з вибраною шкалою оцінок;
2. Ввести в СУІБ виявлені загрози у вигляді списку, що містить назви загроз і їх частоти (вірогідність реалізації), згідно з вибраною шкалою оцінок;
3. Сформувати список ризиків шляхом призначення загроз активам. Автоматичне перехресне об'єднання активів з загрозами недоступне, оскільки можуть бути утворені неіснуючі, незначні, або навіть неможливі ризики (наприклад, фізичне пошкодження цифрових підписів).

Оцінки ризиків розраховуються автоматично шляхом множення значення збитку активу на значення частоти загрози:

$$R = W \times n,$$

де R – ризик, W – збиток, n – частота.

У пункті головного меню «Оцінка ризиків» зведена діаграма надає огляд ризиків, а зведена таблиця – розподіл загроз за активами і навпаки, з сумарними оцінками по кожному активу і кожній загрозі.

Сумарна оцінка ризику (у зведеній таблиці ризиків) потрібна для періодичного оцінювання. Вона дає можливість відстежити зміни загального рівня ризику з плином часу. Приклади зведеної таблиці та зведеної діаграми ризиків наведені відповідно на рис. 1 та рис 2.

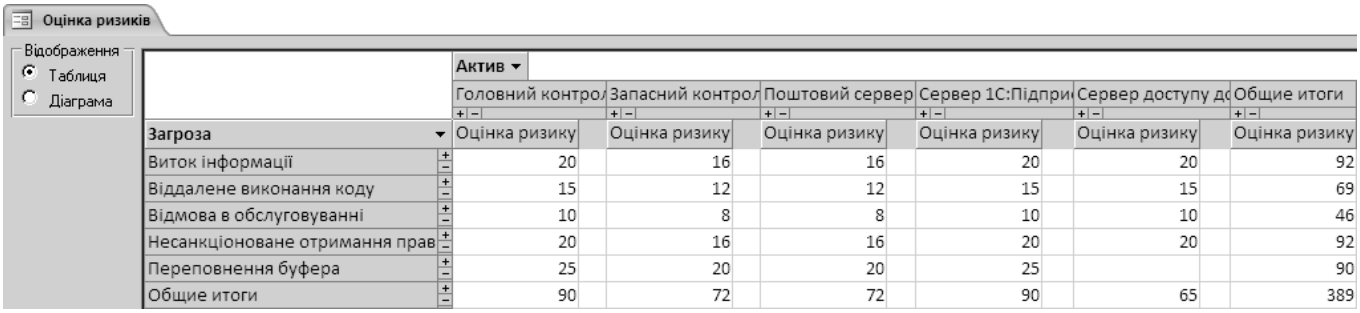

Рис. 1. Приклад зведеної таблиці ризиків

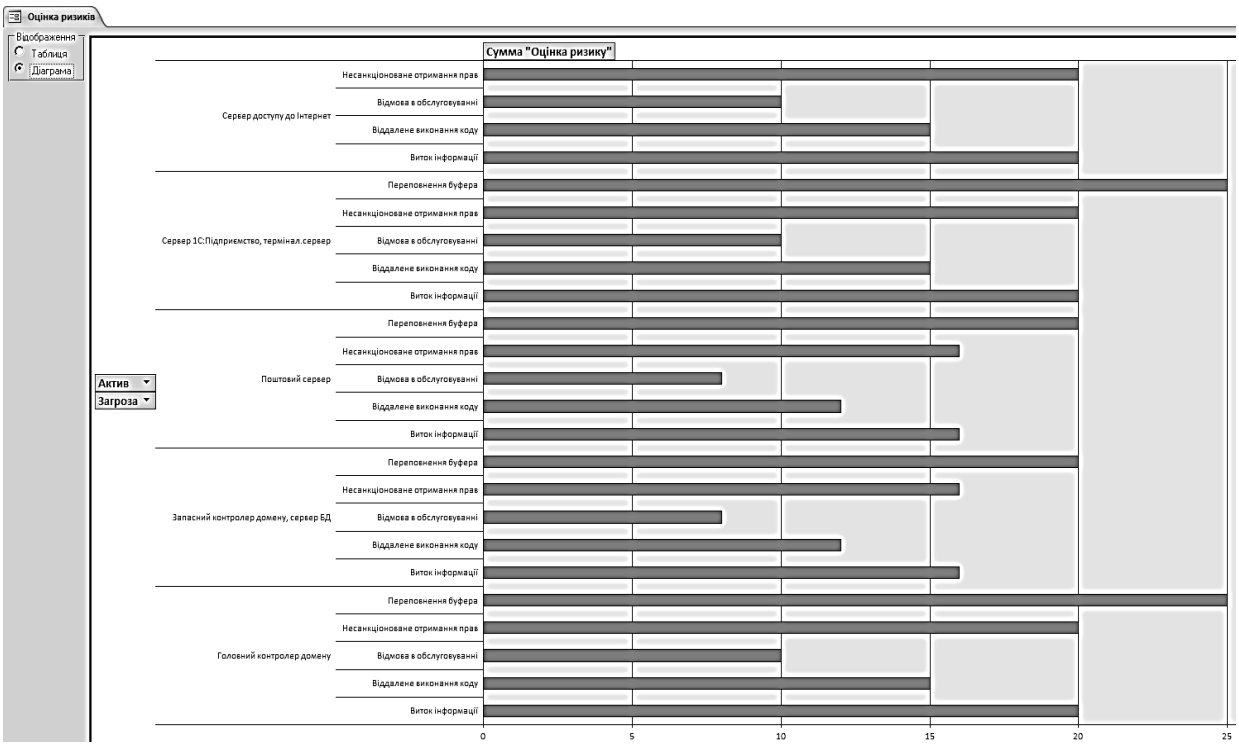

Рис. 2. Приклад зведеної діаграми ризиків

Визначення найбільш вразливих активів та найбільш небезпечних загроз

У зведеній діаграмі «Оцінка ризиків», прибираючи по черзі поля з області даних, отримати спочатку графік сумарних оцінок за активами, потім за загрозами. Приклади графіків сумарних оцінок за активами та за загрозами наведені відповідно на рис. 3 та рис. 4.

Зробити висновки про найвразливіші активи та найбільш небезпечні загрози (вони матимуть найвищі сумарні оцінки ризику).

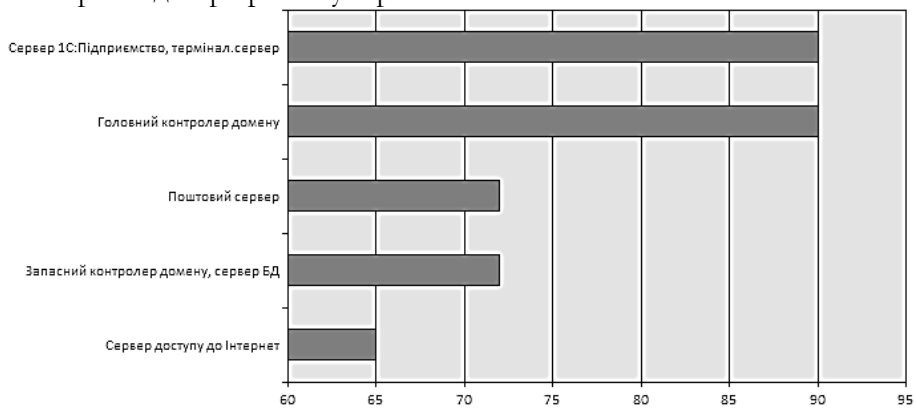

Рис. 3. Приклад графіку сумарних оцінок за активами

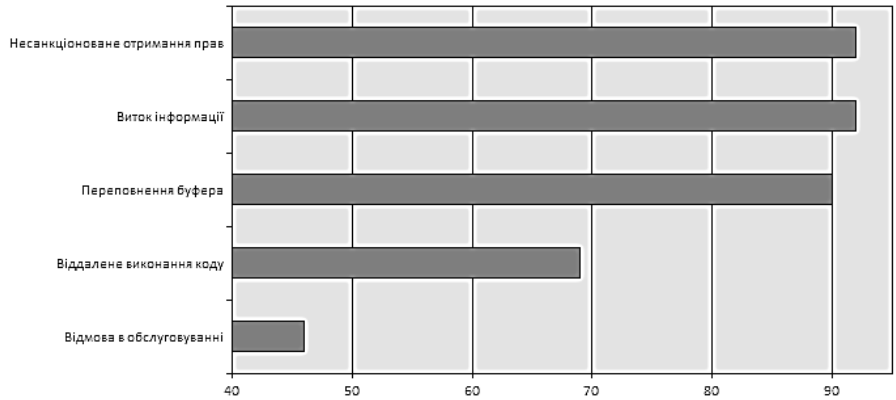

Рис. 4. Приклад графіку сумарних оцінок за загрозами

Ранжування вразливостей кожного активу

Слід згрупувати вразливості по активах і вирахувати сумарні оцінки ризику для кожної вразливості кожного активу. Слід мати на увазі, що кожна вразливість може бути джерелом однієї або декількох загроз.

Сумарна оцінка ризику для вразливості вираховується для кожного активу, оскільки для однакових загроз активи мають різну цінність.

Числова сумарна оцінка ризику для вразливості конкретного активу обчислюється як сума оцінок ризиків від кожної загрози, джерелом якої є ця вразливість для цього активу:

$$V_a = \sum R_a = W_a \times \sum n_a,$$

де V_a – вразливість активу, R_a – ризик активу, W_a – збиток активу, n_a – частота загрози.

Приклад розрахунку числової сумарної оцінки ризику для однієї вразливості наведений в табл. 5. Отримавши кількісні сумарні оцінки ризику для усіх вразливостей, відсортувати їх за спаданням, а потім перевести в словесні за рекомендованою шкалою оцінок, що представлена в табл. 6.

Приклад розрахунку числової сумарної оцінки ризику від вразливості активу «Головний контролер домену» Таблиця 5

Вразливість	**Загроза для даного активу**	**Оцінка ризику загрози для даного активу**	**Числова сумарна оцінка ризику вразливості**
Не встановлені критичні оновлення Windows: MS04-012, MS08-061, MS08-063, MS08-064.	Несанкціоноване отримання прав	20	70
	Віддалене виконання коду	15	
	Відмова в обслуговуванні	10	
	Переповнення буфера	25	

Рекомендована шкала сумарних оцінок ризику вразливості Таблиця 6

Числова сумарна оцінка ризику вразливості	**Словесна оцінка**	**Опис для клієнта**
>100	Критична	Несе найбільшу кількість загроз для даного активу; найбільший збиток у разі використання зловмисниками.
51-100	Важлива	Несе серйозні загрози і, ймовірно, буде використана зловмисниками.
25-50	Середня	Представляє небезпеку, проте її використання зловмисниками малоймовірно.
<25	Низька	Малоймовірні загрози, або мінімальний збиток.

Складання рекомендацій щодо усунення вразливостей та оформлення звіту

Скласти типові рекомендації по усуненню виявлених вразливостей на підставі офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft). Потім, доповнити рекомендації на підставі думок і досвіду експертів перевіряючої сторони.

Скласти таблиці вразливостей для кожного активу з колонками: Вразливість, Загрози, Важливість (словесна оцінка сумарного ризику вразливості), Рекомендації.

Скласти звіт з наступних розділів, що відображатимуть основні етапи оцінювання ризиків інформаційної безпеки за даною методикою:

1. Терміни, визначення і скорочення, використані в звіті;
2. Цілі та сфера дослідження;
3. Дослідження вразливостей: виявлені уразливості та зведені дані щодо оцінок ризиків;
4. Рекомендації щодо усунення вразливостей;
5. Додаткові розділи (за потреби);
6. Загальні висновки.

Висновки

Запропонована методика оцінювання захищеності ІС за допомогою СУІБ «Матриця» забезпечує отримання кількісних оцінок стану ІБ. В свою чергу, завдяки кількісним оцінкам забезпечується точний вибір пріоритетів в усуненні вразливостей ІБ.

Запропонована методика є універсальною з точки зору розміру та профілю організації.

ЛІТЕРАТУРА

[1]. Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992 с. ISBN 966-7992-36-5

[2]. Домарєв, В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) [Текст] / В.В. Домарєв, Д.В. Домарєв. – Донецьк: «Велстар», 2012. – 146 с. ISBN 978-966-2759-00-6

[3]. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Текст]: ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К.: Національний банк України, 2010. – 163 с. – Код УКНД 35.040.

[4]. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) [Текст]: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с. – Код УКНД 35.040.

[5]. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Текст]: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: Національний банк України, 2011.

[6]. Domarev, D.V. Information security management system "Matrix" based on system approach [Текст] / D.V. Domarev // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2011. – Вип. 2(34). – С. 36 – 39. ISSN 2073-4751

[7]. Information Security Management Systems (ISMS) [Текст]: BSI Standard 100-1, Version 2.0. – Bonn: BSI, 2008. – 38 p.

[8]. Information technology. Security techniques. Information security management systems. Overview and vocabulary [Текст]: international standard ISO/IEC 27000:2009(E). – Switzerland: ISO/IEC, 2009. – 26 p.

[9]. IT-Grundschutz Methodology [Текст]: BSI Standard 100-2, Version 2.0. – Bonn: BSI, 2008. – 93 p.

REFERENCES

[1]. Domarev V.V. Bezopasnost ynformatsyonnykh tekhnologyy. Systemnyy podkhod [IT security. The system approach]. Kyyiv: OOO "TID SD", 2004. 992 p.

[2]. Domarev V.V. Upravlinnya informatsiynoyu bezpekoyu v bankivskykh ustanovakh (Teoriya i praktyka vprovadzhennya standartiv seriyi ISO 27k) [Information security management in banking institutions (Theory and practice of ISO 27k standards implementation)]. Donetsk: «Welstar», 2012. 146 p.

[3]. Informatsiyni tekhnologiyi. Metody zakhystu. Zvid pravyl dlya upravlinnya informatsiynoyu bezpekoyu (ISO/IEC 27002:2005, MOD): GSTU SUIB 2.0/ISO/IEC 27002:2010 [Information technology – Security techniques – Code of practice for information security management (ISO/IEC 27002:2005, MOD): Branch standard of Ukraine ISMS 2.0/ISO/IEC 27002:2010]. Kyyiv: National bank of Ukraine, 2010. 163 p.

[4]. Informatsiyni tekhnologiyi. Metody zakhystu. Systema upravlinnya informatsiynoyu bezpekoyu (ISO/IEC 27001:2005, MOD): GSTU SUIB 1.0/ISO/IEC 27001:2010 [Information technology – Security techniques – Information security management system (ISO/IEC 27001:2005, MOD): Branch standard of Ukraine ISMS 1.0/ISO/IEC 27002:2010]. Kyyiv: National bank of Ukraine, 2010. 49 p.

[5]. Metodychni rekomendatsiyi schodo vprovadzhennya systemy upravlinnya informatsiynoyu bezpekoyu ta metodyky otsinky ryzykiv vidpovidno do standartiv Natsionalnogo banku Ukrayiny: lyst departamentu informatyzatsiyi Natsionalnogo banku Ukrayiny bankam Ukrayiny vid 03 bereznya 2011. № 24-112/365 [Methodical recommendations concerning implementation of information security management system and risks estimation method in compliance with the standards of the National bank of Ukraine: a letter from the National bank of Ukraine to all the Ukrainian banks]. Kyyiv: National bank of Ukraine, 2011.

[6]. Domarev D.V. Information security management system "Matrix" based on system approach. Problemy informatyzatsiyi ta upravlinnya [Problems of informatization and management]. 2011; 2(34): p. 36-39.

[7]. BSI-Standard 100-1: Information Security Management Systems (ISMS), Version 2.0. Bonn: BSI, 2008. 38 p.

[8]. Information technology. Security techniques. Information security management systems. Overview and vocabulary: international standard ISO/IEC 27000:2009(E). Geneva: ISO/IEC, 2009. 26 p.

[9]. BSI Standard 100-2: IT-Grundschutz Methodology, Version 2.0. Bonn: BSI, 2008. 93 p.

МЕТОДИКА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ПОМОЩЬЮ СУИБ «МАТРИЦА»

Обоснована актуальность вопросов оценивания защищенности информационных систем. Приведены область применения, назначение и процедура предлагаемой методики. Собственно процедура предлагаемой методики состоит из первичного опроса клиента, определения активов, определения важности активов по словесной шкале, поиска уязвимостей определенных активов, определения угроз, исходящих от найденных уязвимостей, определения степени опасности найденных угроз по словесной шкале, перевода важности активов и степени опасности угроз в количественные оценки, подсчета оценок рисков, ранжирования по суммарным оценкам рисков, определения наиболее уязвимых активов и наиболее опасных угроз, ранжирования уязвимостей каждого актива, составления рекомендаций относительно устранения уязвимостей, оформления отчета. Для практической реализации предлагаемой методики применена система управления информационной безопасностью «Матрица». Сделаны выводы о преимуществах предлагаемой методики.

Ключевые слова: оценка защищенности информационных систем, аудит информационной безопасности, оценка рисков ИБ, оценка риска ИБ, управление информационной безопасностью, СУИБ «Матрица».

METHOD OF INFORMATION SYSTEM'S SECURITY LEVEL ESTIMATION USING ISMS "MATRIX"

Actuality of information system's security level estimation is proved. For the offered method, the range of application, purpose and procedure are described. The procedure of the offered method consists of primary questioning of the client, determination of assets, determination of assets' importance using verbal estimations, search for vulnerabilities of the determined assets, determination of threats resulting from found vulnerabilities, determination the found threats' danger using verbal estimations, translation of assets' importance and threats' danger into quantitative estimations, risk assessment and ranking, determination of the most vulnerable assets and the most dangerous threats, ranking of vulnerabilities for every asset, production of recommendations concerning the vulnerabilities' remediation, compilation of report. For the practical realization of the offered method, the information security management system "Matrix" is applied. Conclusion is made about the advantages of the offered method.

Index Terms*:* information system's security level estimation, information security audit, risk evaluation, risk estimation, information security management, ISMS "Matrix".

Домарєв Дмитро Валерійович, аспірант, Національний авіаційний університет
E-mail: dimavsesvit@yahoo.com.
Домарев Дмитрий Валериевич, аспирант, Национальный авиационный университет.
Domarev Dmitry, postgraduate student of the National aviation university.

Домарєв Валерій Валентинович, к.т.н., доц., незалежний експерт з питань інформаційної безпеки
E-mail: domarev@ukr.net.
Домарев Валерий Валентинович, к.т.н., доц., независимый эксперт по вопросам информационной безопасности
Domarev Valerii, PhD, associate prof., independent expert in information security

Прокопенко Сергій Дмитрович, начальник Лабораторії комп'ютерної криміналістики та інформаційної безпеки, ТОВ «ЕПОС»
E-mail: sprokopenko@epos.ua.
Прокопенко Сергей Дмитриевич, начальник Лаборатории компьютерной криминалистики и информационной безопасности, ООО «ЕПОС»
Prokopenko Sergey, head of Computer forensics and information security lab., EPOS LLC