DOI 10.15276/imms.v11.no3.173
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 3, pp. 173-180

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло

Національний університет «Одеська політехніка»,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@op.edu.ua,

У роботі розглядається сучасний стан розробок в області оцінки захищеності. Проблема забезпечення безпеки інформаційних технологій займає все більш значне місце у реалізації комп'ютерних систем у міру того, як зростає їхня роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій є комплексною проблемою, що вирішується у напрямах удосконалення правового регулювання застосування інформаційних технологій, удосконалення методів та засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. У роботі розглядаються системні проблеми безпеки інформаційних систем, наводиться перелік загроз, які можуть спричинити один або кілька шкідливих впливів на системи. У роботі наводиться перелік стандартів та нормативних документів за допомогою яких можна оцінити якість інформаційної системи чи окремі показники. Наводяться актуальність роботи, її мета та задачі. Ключовим аспектом вирішення проблеми безпеки інформаційних технологій є вироблення системи вимог, критеріїв та показників рівня безпеки інформаційних технологій. У роботі детально описується структура стандарту ISO 15408, який був обраний за основу методики, що розробляється. Стандарт ISO 15408 складається з трьох частин. У роботі використовується друга частина стандарту, яка містить універсальний систематизований каталог функціональних вимог безпеки та передбачає можливість їх деталізації та розширення за певними правилами. Наводиться розроблена методика оцінки захищеності інформаційних систем. В роботі описані основні показники, за допомогою яких проводиться оцінка захищеності інформаційних систем у методики, що розроблялась. Було розроблено програмний продукт, який реалізує описану методику і в роботі наводиться інтерфейс програми у вигляді основних вікон програми.

Ключові слова: інформаційна система, захист інформаційної системи, стандартизація, стандарт ISO 15408, оцінка захищеності інформаційних систем.

Вступ

На сьогоднішній день інформаційна безпека підприємства – один з провідних факторів його ефективного розвитку. Інформація має реальну вартісну вагу, яка чітко визначається прибутком, що отримується при її використанні, або шкодою, яку може бути завдано підприємству у разі використання її іншими особами.

Постійно зростає частка витрат організацій на забезпечення цілісності інформації та захисту її від можливих зовнішніх загроз. У зв'язку з цим гостро постає питання оцінки ефективності засобів захисту та оцінки захищеності всієї інформаційної системи в цілому. Зробивши таку оцінку, можна вибрати найбільш ефективну систему захисту як із функціонального, так і з економічного погляду у кожному конкретному випадку. Тому дана робота є актуальною в житті суспільства.

Метою роботи є розробка методики оцінки захищеності інформаційної системи шляхом використання стандарту ISO 15408.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Проаналізувати стан сучасних розробок в області оцінки захищеності;
- Провести аналіз сучасних стандартів безпеки;
- Розробити методику оцінки захищеності інформаційної системи;

– Розробити програмний продукт, який реалізує розроблену методику оцінки захищеності інформаційної системи.

Основна частина

Проблема забезпечення безпеки інформаційних технологій займає все більш значне місце у реалізації комп'ютерних систем у міру того, як зростає їхня роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій є комплексною проблемою, що вирішується у напрямах удосконалення правового регулювання застосування інформаційних технологій, удосконалення методів та засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації.

Інформаційна система – інтегрований набір компонентів для збору, зберігання та обробки даних, а також для надання інформації, знань та цифрових продуктів. Бізнес-фірми та інші організації покладаються на інформаційні системи для здійснення та управління своїми операціями, взаємодії зі своїми клієнтами та постачальниками та конкуренції на ринку.

Уряди впроваджують інформаційні системи для економічного надання послуг громадянам. Цифрові товари, такі як електронні книги, відеопродукти та програмне забезпечення, та онлайн-послуги, такі як ігри та соціальні мережі, постачаються разом із інформаційними системами.

Інформаційні системи часто піддаються різним видам загроз, які можуть спричинити різні типи збитків, що може призвести до значних фінансових втрат. У різних дослідженнях називаються системні проблеми безпеки інформаційних систем:

– маніпулювання доступом у внутрішній інформаційний простір;
– крадіжка інформації з корпоративних мереж і баз даних;
– зміна інформації, фальсифікація документів в електронному вигляді;
– промислове стеження;
– крадіжка засобів з банківських рахунків;
– вірусні загрози.

Загроза безпеці може спричинити один або кілька шкідливих впливів на системи, на які вони поділяються. Їх є сім видів:

1) знищення інформації,
2) пошкодження інформації,
3) крадіжка або втрата інформації,
4) розкриття інформації,
5) відмова у використанні,
6) підвищення привілеїв,
7) незаконне використання.

Ключовим аспектом вирішення проблеми безпеки інформаційних технологій є вироблення системи вимог, критеріїв та показників рівня безпеки інформаційних технологій.

Стандартизація – це діяльність, що направлена на розробку та встановлення вимог, норм та правил, характеристик, що є обов’язковими до виконання або рекомендованими.

Самі стандарти – це нормативні документи, що розроблені на основі консенсусу, затвердженого признаним органом та направлені на досягнення оптимального ступеня упорядкованості у певній області. В стандарті встановлюють для загального та багатократного використання загальні принципи, правила і характеристики, що стосуються змісту різних видів діяльності або їх результатів.

Стандарти в галузі інформаційної безпеки покликані виробити чіткий набір критеріїв, за якими можна звести до мінімуму можливі загрози системі. При оцінці

безпеки інформаційних систем слід враховувати думку трьох груп фахівців: розробників інформаційних систем, замовників або користувачів інформаційних систем, спеціалістів – аналітиків з інформаційної безпеки.

Розглянемо, за допомогою яких стандартів та нормативних документів можна оцінити якість інформаційної системи чи окремі показники.

ISO/IEC 27001 – цей документ містить стандарти ISO щодо вимог щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Стандарт ISO/IEC 27001 є першим загальновизнаним міжнародним стандартом системи управління інформаційною безпекою. Від багатьох інших стандартів у галузі захисту інформації його відрізняє те, що він може застосовуватись у будь-якій організації незалежно від роду її діяльності. Особливістю ISO 27001 є те, що він висуває вимоги не так до технічних засобів захисту, як до системи управління інформаційною безпекою.

ISO/IEC 27002 – Цей документ вводить кодекс практики для контролю інформаційної безпеки.

ISO/IEC 27017 – цей документ містить рекомендації, що підтримують впровадження засобів контролю інформаційної безпеки для споживачів і постачальників хмарних послуг. Вибір відповідних засобів контролю та застосування рекомендацій щодо впровадження базуються на оцінці ризиків та інших вимогах до використання хмарних сервісів.

Стандарт ISO/IEC 13355 – це посібник з управління безпекою інформаційних та телекомунікаційних технологій, встановлює концепцію та моделі, що лежать в основі базового розуміння безпеки, і розкриває загальні питання управління, які важливі для успішного планування, реалізації та підтримки безпеки. Метою цього стандарту є формування загальних понять та моделей управління безпекою.

Загальні критерії, також відомі як ISO/IEC 15408 – це набір критеріїв оцінки розроблено та узгоджено з національними організаціями стандартів безпеки Австралії, Канади, Франції, Німеччини, Японії, Нідерландів, Нової Зеландії, Іспанії, Великобританії та США. У стандарті детально розглянуті загальні підходи, методи та функції забезпечення захисту в організаціях. Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації.

ISO/IEC 15408 складається з наступних частин під загальною назвою Інформаційні технології – Методи безпеки – Критерії оцінки IT-безпеки:

– Частина 1: Вступ і загальна модель;
– Частина 2: Функціональні вимоги безпеки;
– Частина 3: Вимоги до забезпечення безпеки.

Оцінка інформаційної безпеки ґрунтується на моделях системи безпеки, що складаються з перелічених у стандарті функцій. В ISO 15408 міститься ряд зумовлених моделей (так званих профілів), що описують стандартні модулі безпеки.

Особливості ISO 15408 в порівнянні з іншими стандартами безпеки:

– стандарт дозволяє визначити повний перелік вимог до засобів безпеки, а також критеріїв їхньої оцінки (показники захищеності інформації);

– стандарт визначає повний перелік об'єктів аналізу та вимог до них, не загострюючи уваги на методах створення, управління та оцінки системи безпеки;

– стандарт дозволяє оцінити повноту системи інформаційної безпеки з технічного погляду, не розглядаючи при цьому комплекс організаційних заходів із забезпечення захисту інформації.

Усі функції в стандарті ISO/IEC 15408 представлені у вигляді чотирьохрівневої ієрархічної структури: клас – сімейство – компонент – елемент. За аналогією представлені

вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки та зіставити створену модель із поточним станом справ.

У стандарті ISO/IEC 15408–2 виділено 11 класів функцій: аудит, ідентифікація та аутентифікація, криптографічний захист, конфіденційність, передача даних, захист даних, управління безпекою, захист функцій безпеки системи, використання ресурсів, доступу до системи, надійність коштів [1].

Кожен функціональний клас має унікальну назву. Категоріальна інформація складається з короткої назви з трьох символів. Коротка назва класу використовується в специфікації коротких імен сімейства цього класу.

Назва сім'ї надає категоріальну та описову інформацію, необхідну для ідентифікації та категоризації функціональної сім'ї. Кожна функціональна сім'я має унікальну назву. Інформація про категорію складається з короткої назви з семи символів, причому перші три ідентичні короткій назві класу, за якими слідує символ підкреслення та коротка назва сімейства (XXX_YYY). Унікальна коротка форма назви надає основне посилання для компонентів [1].

Функціональні сімейства містять один або більше компонентів, будь-який з яких можна вибрати. Метою цього розділу є надання інформації користувачам при виборі відповідного функціонального компонента після того, як сімейство було визначено як необхідну або корисну частину їхніх вимог безпеки. Цей розділ опису функціонального сімейства описує доступні компоненти та їх обґрунтування. Точні відомості про компоненти містяться в кожному компоненті. Відносини між компонентами всередині функціонального сімейства можуть бути ієрархічними, а можуть і не бути такими. Компонент є ієрархічним щодо іншого, якщо він забезпечує більшу безпеку [1].

Для кожного компонента надається набір елементів. Кожен елемент визначається окремо і є самостійним. Функціональний елемент – це функціональна вимога безпеки, подальше розділення якої не дасть значущого результату оцінки [1]. Це найменша функціональна вимога безпеки, визначена та визнана в ISO/IEC 15408.

Залежності між функціональними компонентами виникають, коли компонент не є самодостатнім і покладається на функціональність або взаємодію з іншим компонентом для свого належного функціонування.

Список залежностей визначає мінімальні функціональні або впевнені компоненти, необхідні для задоволення вимоги безпеки, пов'язані з ідентифікованим компонентом. Компоненти, які є ієрархічними щодо ідентифікованого компонента, також можуть використовуватися для задоволення залежності. Залежності, зазначені в ISO/IEC 15408-2, є нормативними [1].

Розроблена методика оцінки захищеності інформаційних систем має наступні кроки:

1. Визначення класів, що беруть участь в оцінці;
2. Ранжирування класів та розрахунок вагових коефіцієнтів класів;
3. Ранжирування сімейств кожного класу та розрахунок вагових коефіцієнтів сімейств;
4. Відмітка про виконання дій зазначених в компонентах кожного сімейства серед класів, що беруть участь в оцінці;
5. Формування матриці вагової функції по відміткам про виконання;
6. Розрахунок залежностей для кожної компоненти сімейства, якщо така залежність присутня у стандарті;
7. Розрахунок узагальнених показників по кожному класу;
8. Розрахунок підсумкової оцінки;

9. Розрахунок залежностей, узагальнених показників та підсумкової оцінки для класів, що беруть участь в оцінці в ситуації що стоять всі позитивні відмітки про виконання дій зазначених в компонентах кожного сімейства;

10. Порівняння результатів, отриманих на кроках 8 та 9 та формування рекомендацій по підвищенню захищеності інформаційної системи, що оцінюється.

Розглянемо детальніше перелічені кроки.

Обчислення вагових коефіцієнтів C_i для кожного і-го класу безпеки відбувається за формулою:

$$C_i = 1 - \frac{R_i - 1}{M}$$

де R – ранг, а M – число функціональних класів.

Нормування коефіцієнтів, виконується наступним чином:

$$C_k = \frac{C_i}{\sum_{i=1}^{M} C_i}.$$

Ранжування сімейств класів та обчислення вагового коефіцієнту сімейству відбувається за наступними формулами:

$$F_i = 1 - \frac{R_i - 1}{M}.$$

$$F_k = \frac{F_i}{\sum_{i=1}^{M} F_i}.$$

Вводиться вагова функція яка має 3 різні поведінки: «–1» – якщо компонент не виконано, «0» – якщо він не використовується та «1» – якщо компонент виконано. Ці значення заносяться у вагову функцію на етапі анкетування, коли експерт проставляє виконання компонентів кожного сімейства.

В результаті анкетування компонентів кожного сімейства обчислюється оцінка по сімейству:

$$W_{kj} = \sum_{k=1}^{n} F_k^j w_k ,$$

де F_k^j – ваговий коефіцієнт к-сімейству j-класу;

w_k – вагова функція к-сімейству.

Вагова функція сімейству складається з вагових функцій компонент цього сімейству з урахуванням залежностей для кожної компоненти сімейства.

Оцінка по кожному класу обчислюється за наступною формулою:

$$X_j = \sum_{k=1}^{n} C_j w_{kj} ,$$

де C_j – ваговий коефіцієнт важливості j-го класу;

w_{kj} – підсумковий показник по всім сімействам j-го класу

Підсумкова оцінка захищеності визначається за формулою:

$$Y = \sum_j X_j$$

Було розроблено програмний продукт, який реалізує описану методику оцінки захищеності інформаційних систем. Для ранжування класів та сімейств класів використовується вікно, яке представлено на рисунку 1.

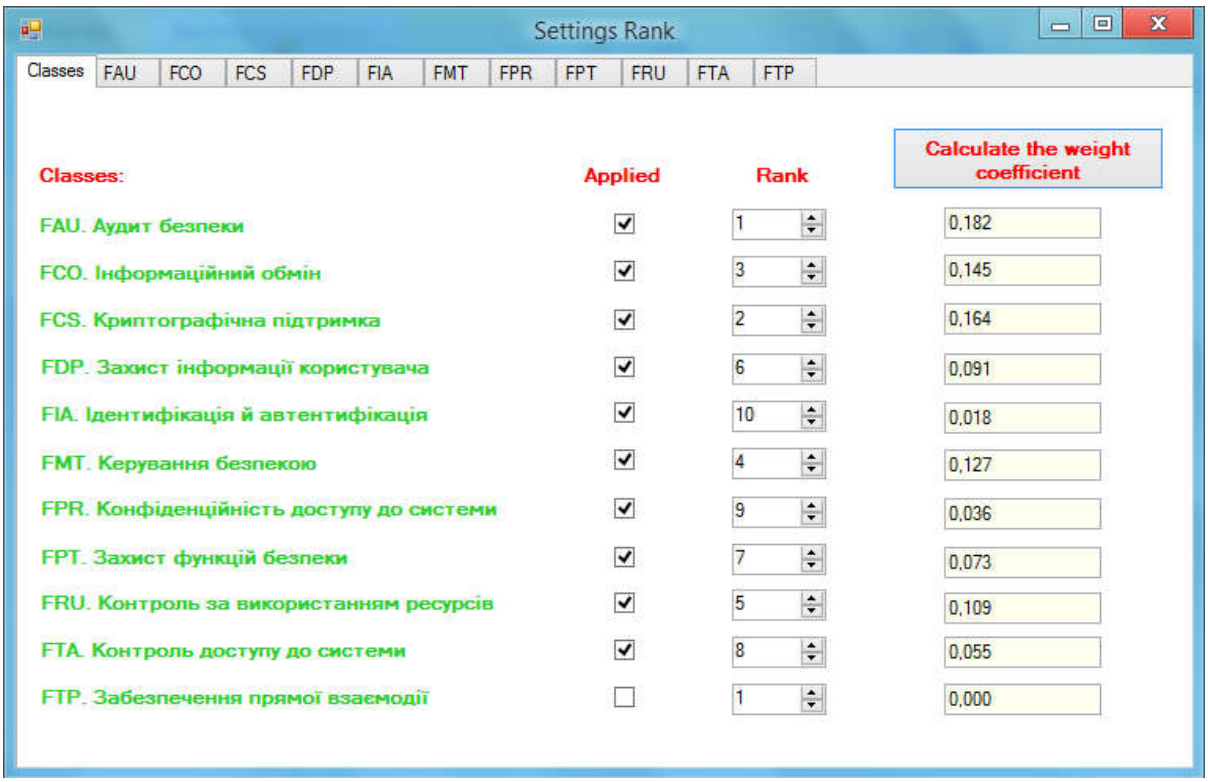

Рис. 1. Вікно для ранжування класів та сімейств класів

Для встановлення вагових коефіцієнтів компонентів кожного сімейства використовується вікно, , яке представлено на рисунку 2.

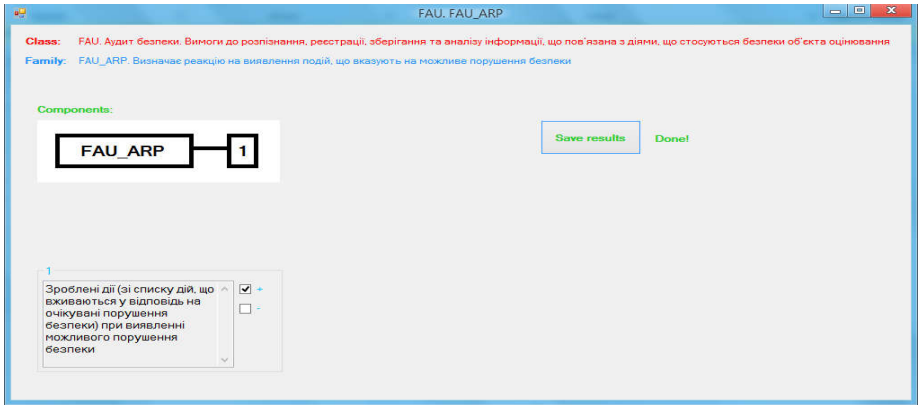

Рис. 2. Вікно для опитування

Після оцінки усіх класів можна отримати оцінку захищеності конкретної інформаційної системи згідно з результатами анкетування.

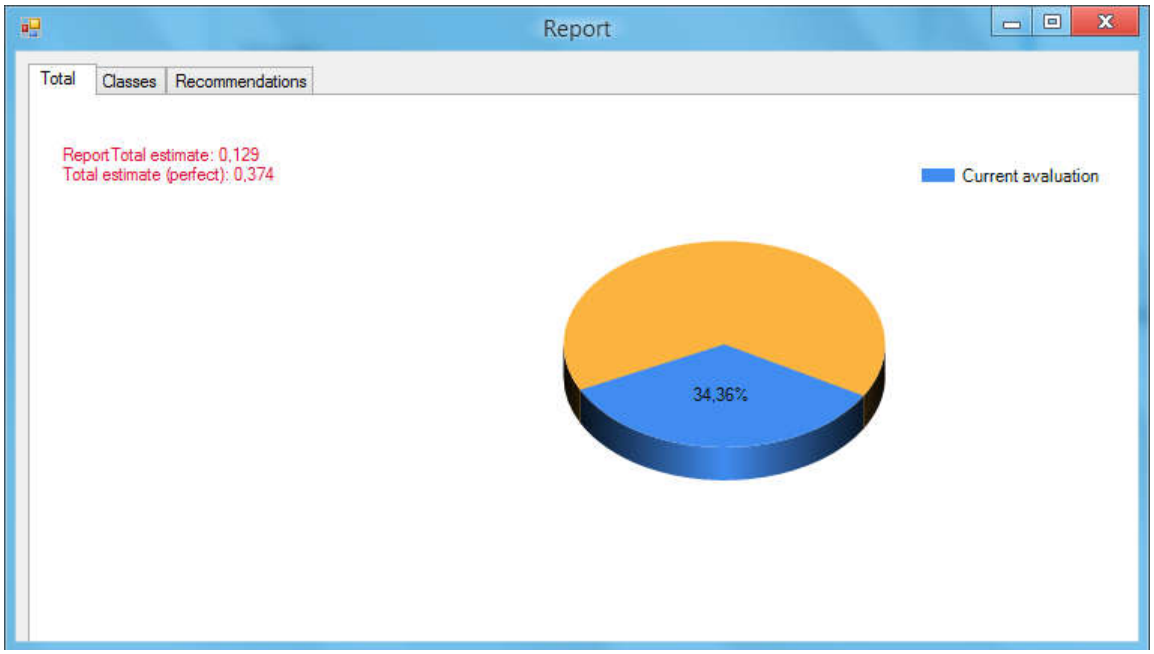

Рис. 3. Відображення результатів оцінювання

Висновки

Було проведено аналіз сучасного стану розробок в області оцінки захищеності. Для методики оцінки захищеності інформаційних систем були обрані функціональні вимоги стандарту ISO/IEC 15408. Було розроблено програмний продукт, який дозволяє оцінити захищеність інформаційної системи згідно з розробленої методики.

Список літератури

1. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-2:ed-3:v2:en

METHODOLOGY FOR ASSESSING THE SAFETY OF INFORMATION SYSTEMS

S.V. Batechko, O.Yu. Lebedova, V.V. Zorilo

National Odessa Polytechnic University
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: o.y.lebedieva@opu.ua,

The paper considers the current state of developments in the field of security assessment. The problem of information technology security is becoming increasingly important in the implementation of computer systems as their role in the informatization of society. Ensuring the security of information technology is a complex problem that is solved in the areas of improving the legal regulation of information technology, improving methods and means of their development, development of certification systems, ensuring appropriate organizational and technical conditions of operation. The paper considers systemic problems of information systems security, lists the threats that can cause one or more harmful effects on systems. The paper provides a list of standards and regulations that can be used to assess the quality of the information system or individual indicators. The urgency of the work, its purpose and objectives are given. A key aspect of solving the problem of information technology security is to develop a system of requirements, criteria and indicators of the level of information technology security. The paper describes in detail the structure of the ISO 15408 standard, which was chosen as the basis of the developed methodology. The ISO 15408 standard consists of three parts. The paper uses the second part of the standard, which contains a universal systematized catalog of functional safety requirements and provides for the possibility of detailing and expanding them according to certain rules. The developed method of assessing the security of information systems is given. The paper describes the main indicators used to assess the security of information systems in the developed methodology. A software product has been developed that implements the described technique and the program interface is presented in the form of the main program windows.

Keywords: information system, information system protection, standardization, ISO 15408 standard, information systems security assessment.