МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

V МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (PCSITS)

27-28 жовтня 2022 року

Збірник матеріалів доповідей та тез

Київ – 2022

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. – К.: ВПЦ "Київський університет", 2022. – 159 с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

ВСТУП

Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно- телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері. У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах. Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

У збірнику матеріалів науково-практичної конференції опубліковано тези доповідей вчених, науково-педагогічних працівників, аспірантів, студентів Київського національного університету імені Тараса Шевченка, інших вищих навчальних закладів та організацій України, в яких розглядаються науково- технічні та практичні аспекти створення й використання засобів безпеки інформаційно-телекомунікаційних систем та методи управління їх інформаційною безпекою.

В роботі конференції взяли участь представники: Київського національного університету імені Тараса Шевченка, Національного транспортного університету, Харківського коледжу Державного університету телекомунікацій, Харківського національного університету радіоелектроніки, Одеського національного політехнічного університету,

Харківського університету Повітряних Сил імені І. Кожедуба, Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Державного університету телекомунікацій, Національного авіаційного університету, Державного науково- дослідного інституту спеціального зв'язку та захисту інформації України, Харківського Національного Університету ім. В.Н. Каразіна, ООО "ІТЦ "Хай-Тек Бюро", Інституту програмних систем НАН України, Наукового центру зв'язку та автоматизації Військового інституту телекомунікацій та інформатизації, АТ "Інститут інформаційних технологій", Європейського університету, Військової частини А1906, Східноєвропейського національного університету імені Лесі Українки, Національного університету кораблебудування імені адмірала Макарова, Національного університету біоресурсів і природокористування України, Київського національного університету будівництва і архітектури, НТУУ "Київський політехнічний інститут ім. Ігоря Сікорського", Науково- дослідного інституту Міністерства оборони України, Житомирського військового інституту ім. С. П. Корольова, Київського державного університету культури і мистецтв, Центральноукраїнського національного технічного університету, Державної наукової установи Інститут модернізації змісту освіти, Університету економіки та права "КРОК", Національного інституту стратегічних досліджень, Державної установи "Інститут геохімії навколишнього середовища НАН України" та інші.

Характеристики функційної придатності архітектури систем управління інформаційною безпекою

Володимир Мохор[1], Ярослав Дорогий[2], Олександр Бакалинський[1], Василь Цуркан[3]

1. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, УКРАЇНА, м. Київ, вул. Генерала Наумова, 15, E-mail: v.mokhor@gmail.com, baov@meta.ua

2. Кафедра інформаційних систем і технологій, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", УКРАЇНА, м. Київ, вул. Політехнічна, 41, E-mail: argusyk@gmail.com

3. Кафедра кібербезпеки і застосування інформаційних систем і технологій, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", УКРАЇНА, м. Київ, вул. Верхньоключова, 4, E-mail: v.v.tsurkan@gmail.com

4.

Abstract – ***The process of information security management systems designing is considered. It is shown the need to take into account the requirements, expectations, and limitations of interested parties. For this purpose, the quality of the information security management system is singled out as a key factor in guaranteeing the safety of activities and the provision of services by organizations with an acceptable risk. This choice is due to the fact that on their basis requirements, functions are analyzed, the architecture and behavior of information security management systems are synthesized. Therefore, one of the most significant characteristics of their quality was chosen to be the functional suitability of the architecture. It is characterized in terms of functional completeness, functional correctness and expediency. For them, the conditions for accepting the minimum and maximum values are determined depending on the number of functions that are not correctly or not implemented by the architecture of the information security management system and, as a result, its best option.***

Ключові слова – якість системи управління інформаційною безпекою, характеристика функційної придатності, функційна повнота, функційна коректність, функційна доцільність.

Вступ

Запорукою успішності діяльності організацій є збереженість властивостей конфіденційності, цілісності та доступності інформації [1]. Це досягається завдяки побудові систем управління інформаційною безпекою [2, 3]. Їх наявністю гарантується зацікавленим сторонам безпечність діяльності та надання послуг організаціями з прийнятним ризиком [4]. Ключовим чинником такого гарантування є якість систем управління інформаційною безпекою [5–7]. Нею відображається задоволеність потреб, очікувань, обмежень зацікавлених сторін. Оскільки власне на їх основі аналізуються вимоги, функції і, як наслідок, синтезуються архітектури систем управління інформаційною безпекою [7, 8]. Їхня відповідність потребам, очікуванням, обмеженням зацікавлених сторін встановлюється за поведінкою даних систем у конкретному навколишньому середовищі (організації) і водночас ступенем якої визначається якість синтезованих архітектур [7].

Функційна придатність архітектури систем управління інформаційною безпекою

Якість систем управління інформаційною безпекою визначається як ступінь задоволення потреб, очікувань, обмежень зацікавлених сторін у конкретному навколишньому середовищі (організації) [5, 7]. Вона представляється трьома категоріями характектеристик, а саме: під час застосування, продукту, даних. Кожна з них додатково деталізується підхарактеристиками. Загалом ними утворюється структура характеристик якості систем управління інформаційною безпекою [5, 6]. Вони обираються залежно від значущості для зацікавлених сторін, яка визначається перш за все з огляду на задоволеність їх потреб, очікувань, обмежень у конкретному навколишньому середовищі (організації). Тому однією з найбільш значущих характеристик якості систем управління інформаційною безпекою є функційна придатність архітектури.

Функційною придатністю визначається ступінь реалізованості архітектурою системи управління інформаційною безпекою функцій відповідно до потреб, очікувань, обмежень зацікавлених сторін у конкретному навколишньому середовищі (організації). Цим обумовлюється гарантування безпечності діяльності та надання послуг організаціями з прийнятним ризиком. Виокремлена характеристика якості деталізується такими підхарактеристиками як функційна повнота, функційна коректність і функційна доцільність [5–7, 9]. Вони оцінюються на основі даних про реалізованість функцій системи управління інформаційною безпекою відповідно до синтезованих варіантів їх архітектури та поведінки [7].

Функційною повнотою визначається ступінь, в якому множина функцій охоплює усі потреби, очікування, обмеження зацікавлених сторін. Оцінюється показником функційного покриття (1)

$$F_{покр.}=1-\frac{F_{нр}}{F_{N_{UC}}}, \quad (1)$$

де $F_{покр.}$ – частина реалізованих функцій;

$F_{нр}$ – кількість не реалізованих функцій;

$F_{N_{UC}}$ – кількість специфікованих функцій (варіантів використання, use case, UC).

Функційною коректністю визначається ступінь, у якому архітектурою системи управління інформаційною безпекою надаються коректні результати з необхідним рівнем точності. Оцінюється показником функційної коректності (2)

$$F_{кор.}=1-\frac{F_{нк}}{F_{розгл.}}, \quad (2)$$

де $F_{кор.}$ – частина коректно реалізованих функцій;

$F_{нк}$ – кількість не коректно реалізованих функцій;

$F_{розгл.}$ – кількість розглянутих функцій.

Функційною доцільністю визначається ступінь, у якому реалізовані архітектурою системи управління інформаційною безпекою функції задовольняють потреби, очікування, обмеження зацікавлених сторін. Оцінюється показником функційної доцільності конкретної цілі використання (3)

$$F_{доц.цілі}=1-\frac{F_{нр/нк}}{F_{необх.}}, \quad (3)$$

де $F_{доц.цілі}$ – частина функцій, яка необхідна зацікавленим сторонам для досягнення конкретної цілі реалізування архітектури системи управління інформаційною безпекою, наприклад, оцінювання ризиків;

$F_{нр/нк}$ – кількість не коректно або не реалізованих функцій, яка необхідна зацікавленим сторонам для досягнення конкретної цілі реалізування архітектури системи управління інформаційною безпекою;

$F_{необх.}$ – кількість розглянутих функцій, яка необхідна зацікавленим сторонам для досягнення конкретної цілі реалізування архітектури системи управління інформаційною безпекою

або функційної доцільності системи (4)

$$F_{доц.,\ сист.}=\sum_{i=1}^{n}\frac{F_{доц.цілі,i}}{n}, \quad (4)$$

де $F_{доц.сист.}$ – частина функцій, яка необхідна зацікавленим сторонам для досягнення мети реалізування архітектури системи, наприклад, управління інформаційною безпекою;

$F_{доц.цілі,\ i}$ – частина функцій, яка необхідна зацікавленим сторонам для досягнення i цілі реалізування архітектури системи, наприклад, оцінювання ризиків інформаційної безпеки;

n – кількість цілей реалізування архітектури системи управління інформаційною безпекою.

З огляду на (1)–(3), показники функційної придатності архітектури систем управління інформаційною безпекою приймають

1) мінімальне значення при однаковій кількості:

– не реалізованих і специфікованих функцій, $F_{нр}=F_{N_{UC}}\to F_{покр.}=0$;

– не коректно реалізованих і розглянутих функцій, $F_{нк}=F_{розгл.}\to F_{кор.}=0$;

– не коректно або не реалізованих і необхідних функцій, $F_{нк/нр}=F_{необх.}\to F_{доц.цілі}=0$;

2) максимальне значення за відсутності не коректно або не реалізованих функцій:

– $F_{нр}=0\to F_{покр.}=1$;

– $F_{нк}=0\to F_{кор.}=1$;

– $F_{нк/нр}=0\to F_{доц.цілі}=1$;

Приклад графічного зображення залежності функційної придатності архітектури від кількості специфікованих функцій показано на рис. 1 [7].

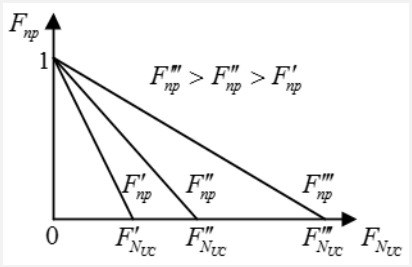

Рисунок 1 – Оцінки функційної придатності архітектури системи управління інформаційною безпекою

За рис. 1 серед трьох варіантів архітектури системи управління інформаційною безпекою обирається з найбільшою кількістю реалізованих функцій, $F'''_{пр}(F'''_{N_{UC}})$.

Висновок

Отже, ключовим чинником гарантування безпечності діяльності та надання послуг організаціями з прийнятним ризиком є якість системи управління інформаційною безпекою. Серед її характеристик обрано як найбільш значущу функційну придатність архітектури. Такий вибір обумовлено необхідністю задоволення потреб, очікувань, обмежень зацікавлених сторін при побудові систем управління інформаційною безпекою в організаціях.

Література

[1] ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07]. URL: https://www.iso.org/standard/73906.html (accessed on: 25.09.2022).

[2] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. [Valid from 2013-09-25; revised 2018-12-04]. URL: https://www.iso.org/standard/54534.html (accessed on: 25.09.2022).

[3] ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance. [Valid from 2017-04-12]. URL: https://www.iso.org/standard/63417.html (accessed on: 25.09.2022).

[4] ISO/IEC/IEEE 15026-1:2019. Systems and software engineering. Systems and software assurance. Part1: Concepts and vocabulary. [Valid from 2019-03-08]. URL: https://www.iso.org/standard/73567.html (accessed on: 25.09.2022).

[5] ISO/IEC 25010:2011. Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models. [Valid from 2011-03-01; revised 2017-08-16]. URL: https://www.iso.org/standard/35733.html (accessed on: 25.09.2022).

[6] ISO/IEC 25012:2011. Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Data quality model. [Valid from 2008-12-03; revised 2019-01-15]. URL: https://www.iso.org/ standard/35736.html (accessed on: 25.09.2022).

[7] Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. *Захист інформації*. Липень – Вересень 2021. Том 23, № 4. С. 200–211. DOI: http://dx.doi.org/10.18372/2410-7840.23.16766.

[8] ISO/IEC 15288:2015. Systems and software engineering. System life cycle processes. [Valid from 2015-05-21; revised 2020-09-03]. URL: https://www.iso.org/ standard/63711.html (accessed on: 25.09.2022).