УДК 004.056:004.75
DOI https://doi.org/10.32782/IT/2024-4-28

Максим ШАБАН
кандидат технічних наук, викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0003-2706-8235*

Наталія ДЯЧЕНКО
кандидат наук з державного управління, доцент кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-4306-7665*
***Scopus Author ID:** 57216565101*

Бібліографічний опис статті: Шабан, М., Дяченко, Н. (2024). Організація правил перевірки функціонального профілю захисту. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 230–234, doi: https://doi.org/10.32782/IT/2024-4-28

ОРГАНІЗАЦІЯ ПРАВИЛ ПЕРЕВІРКИ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ

У статті розглянуто процес формалізації правил перевірки функціонального профілю захисту (ФПЗ), який є основою для проведення державних експертиз комплексних систем захисту інформації (КСЗІ). ***Науковою новизною*** *роботи є використання функціонального профілю захисту, що використовується для оцінки повноти та несуперечності реалізації функціональних послуг безпеки (ФПБ) у грід-системах, а також для ідентифікації загроз інформаційній безпеці. Особлива увага приділяється формалізації правил, визначених нормативним документом НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», які дозволяють автоматизувати процес перевірки ФПЗ.*

Метою статті *є розгляд та вдосконалення трьох основних завдань, пов'язаних з ФПЗ: визначення рівнів реалізації ФПБ, оцінка їхньої повноти та несуперечності, а також ідентифікація опису функціональних послуг у вхідній документації. Описано математичну модель ФПЗ, яка враховує рівні ФПБ, набір критеріїв (конфіденційність, цілісність, доступність тощо) та умови реалізації послуг. Формалізація правил дозволяє ефективно перевіряти відповідність профілю нормативним вимогам та автоматизувати цей процес.*

Методологія *статті полягає в формулюванні умов виконання функціональних послуг безпеки, таких як «Довірча конфіденційність», із використанням матриць та рівнянь. Аналіз таких послуг демонструє, що їхня взаємозалежність і винятковість можуть бути враховані в автоматизованих системах перевірки ФПЗ.*

Висновки. *Запропоновані підходи є основою для створення систем підтримки прийняття рішень, що підвищують точність та швидкість проведення державної експертизи КСЗІ. Результати дослідження спрямовані на вдосконалення методологій забезпечення інформаційної безпеки у грід-системах.*

Ключові слова: *функціональний профіль захисту, функціональні послуги безпеки, автоматизація перевірки, грід-системи, державна експертиза.*

Maksym SHABAN
Candidate of Technical Sciences, Lecturer at the Department of Cybersecurity, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, sabanmaxim@gmail.com
***ORCID:** 0000-0003-2706-8235*

Natalia DIACHENKO
Candidate of Sciences in Public Administration, Associate Professor at the Department of Cybersecurity, IT and Economics, Kyiv University of Intellectual Property and Law, National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, n.diachenko@ukr.net
***ORCID:** 0000-0002-4306-7665*
***Scopus Author ID:** 57216565101*

To cite this article: Shaban, M., Diachenko, N. (2024). Orhanizatsiia pravyl perevirky funktsionalnoho profiliu zakhystu [Organization of rules for verification of the functional profile of protection]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 230–234, doi: https://doi.org/10.32782/IT/2024-4-28

ORGANIZATION OF RULES FOR VERIFICATION OF THE FUNCTIONAL PROFILE OF PROTECTION

The article considers the process of formalizing the rules for verifying the functional security profile (FS), which is the basis for conducting state examinations of integrated information security systems (IISS). The scientific novelty of the work is the use of a functional security profile used to assess the completeness and consistency of the implementation of functional security services (FSS) in grid systems, as well as to identify threats to information security. Particular attention is paid to the formalization of the rules defined by the normative document ND TZI 2.5.004-99 «Criteria for assessing the security of information in computer systems against unauthorized access», which allow automating the process of checking the FSIs.

***The purpose** of the article is to consider and improve three main tasks related to the FSI: determining the levels of implementation of the FSI, assessing their completeness and consistency, and identifying the description of functional services in the incoming documentation. The article describes a mathematical model of the FSF that takes into account the levels of FSF, a set of criteria (confidentiality, integrity, availability, etc.) and the conditions for the implementation of services. The formalization of rules allows to effectively check the compliance of the profile with regulatory requirements and automate this process.*

***The methodology** of the article is to formulate the conditions for the implementation of functional security services, such as «Trust Confidentiality», using matrices and equations. The analysis of such services demonstrates that their interdependence and exclusivity can be taken into account in automated systems for verifying FSS.*

***Conclusions.** The proposed approaches are the basis for the creation of decision support systems that increase the accuracy and speed of the state examination of IPSS. The results of the study are aimed at improving the methodologies for ensuring information security in grid systems.*

***Key words:** functional protection profile, functional security services, automation of verification, grid systems, state expertise.*

Одним з ключових завдань при проведенні державної експертизи є ідентифікація функціонального профілю захисту (ФПЗ). Основною метою створення ФПЗ є нейтралізація загроз несанкціонованого доступу до інформації (Давиденко і Шабан, 2014, с. 114), яка забезпечується реалізацією комплексів засобів захисту (КЗЗ) політики функціональних послуг (Новіков і Тимошенко, 2002, с. 40). У завдання ідентифікації (Зегжда і Калінін, 2002, с. 7) входять такі підзадачі: визначення рівнів функціональних послуг безпеки (ФПБ) реалізованих в комплексній системі захисту інформації (КСЗІ) об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікація опису (Лукацький, 2016) ФПБ у вхідних документах. При проведенні другої підзадачі необхідно враховувати правила побудови функціонального профілю захисту визначених НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Формалізація цих правил повинна створити сприятливі умови для автоматизації перевірки повноти та несуперечності ФПЗ.

Отже, перед нами стоять три завдання: визначення рівнів ФПБ реалізованих КСЗІ об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікація опису ФПБ у вхідних документах.

Визначення рівнів ФПБ реалізованих КСЗІ об'єкта експертизи включає попередній аналіз об'єкта експертизи в ході якого, шляхом пошагового опрацювання кожної ФПБ, формується ФПЗ.

На етапі визначення повноти та несуперечності ФПЗ експерт повинен перевірити відповідність отриманого на попередньому етапі ФПЗ вимогам НД ТЗІ 2.5.004-99 (Яловець, 2011, с. 25).

Останнє завдання, яке повинен вирішити експерт – опрацювати вхідні документи на предмет пошуку опису реалізації умов, що пред'являються до кожної ФПБ.

Розглянемо друге завдання більш детально. Вимоги до ФУБ задані у вигляді таблиць показують відповідність рівня реалізованої послуги переліком необхідних вимог для її коректної роботи (Гільгурт, Дурняк і Коростиль, 2014, с. 3).

Для автоматизації перевірки повноти та несуперечності профілю формалізуємо правила, які визначені у НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Перше правило: будь-який профіль зобов'язаний включати в себе контроль цілісності

КСЗІ. Позначимо профіль через множіство Fp тоді: $F_p = \{ФПБ0, ФПБ1, ..., ФПБN\} \cap НЦ_i \neq \varnothing$,

де ФПБ*N* N – функціональна послуга безпеки, а

$НЦ_i$ – «Цілісність комплексу засобів захист» і-ого рівня.

Більш детально розберемо необхідність цієї умови. Розберемо ФПБ «Цілісність комплексу засобів захисту» більш детально. В умовах виконання НЦ рівня 1 сказано: «Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ»; «В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора та автоматично відновити відповідність компонента еталону, або перевести КС до стану з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження»; «Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ». Тобто, невиконання цих правил автоматично робить неможливим гарантування безпеки експлуатації об'єкта експертизи і унеможливлює проведення державної експертизи.

Друге правило: відповідно до НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» деякі з ФПБ є умовно пов'язаними з іншими ФПБ. Іншими словами в НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» при наявності послуг потрібна наявність інших ФПБ, наприклад: для виконання умов ФПБ КД рівня 1 необхідною умовою є виконання умов ФПБ НИ рівня 1. Формалізуємо дану умову:

ФПБ $КД1 = \{УКД1, УКД2, ..., УКДN\} \cap УКД7.1 \neq \varnothing$.

Третє правило: якщо послуга має усі 4-ри рівня, то в функціональному профілі захисту може бути тільки одна. Третє правило говорить про поглинання старшим ФПБ молодших. Тобто, в одному профілі не можуть бути ФПБ однієї спрямованості різного рівня. Наприклад, якщо в ФПБ присутня послуга КД рівня 3 – це автоматично означає, що в даному ФПБ не можуть бути послуги КД рівня 1 або 2. Функціональні послуги одного типу мають властивості винятковості, причому пріоритет віддається послугам вищого рівня.

У подальшому постало питання необхідності якось формалізувати, з математичної точки зору, функціональний профіль послуг безпеки (ФППБ). Функціональний профіль послуг безпеки Fu – це функціональний профіль, що включає в себе множину актуальних послуг безпеки реалізованої КСЗІ об'єкта експертизи. ФППБ залежить від 3 параметрів: Кр – група критеріїв; Ri – рівень реалізованої послуги безпеки; Ui – кон'юнкція умов реалізації виконання і-тої ФПБ.

$$Fu(K_p R_i U_i);$$

Kp = {C, I, A, O, G};

де C – критерій конфіденційності; I – критерій цілісності; A – критерій доступності; O – критерій спостережності; G = критерій гарантій. Ri – це кількість рівнів кожної ФПБ, яка персоніфіковано залежить від виду послуги. Максимальний рівень, згідно з нормативним документом НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», четвертий, але в залежності від ФПБ зустрічаються ФПБ з одним рівнем тощо.

Ri = {1, 2, 3, 4};

де i = 1-23 – це кількість ФПБ згідно з даним ФПЗ, де 23 – це максимальна кількість ФПБ отриманих з нормативного документу НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Кон'юнкція умов реалізації виконання і-тої ФПБ (Ui) – це сума усіх включених ФПБ до профілю захисту, де Ni – кількість умов до і-послуги; $Y_{i,j}$ – це j умова реалізації і-ої послуги.

$$Ui, R_i = \cup_{j=1}^{Ni} Y_j \underline{F} (i, R_i, j) \quad (1.1);$$

Розглянемо приклад аналізу КД.

$$КД1 = \{УКД1.1, УКД2.1, УКД3.1, УКД4.1, УКД6.1, УКД7.1\} \quad (1.2)$$

$$КД2 = \{УКД1.1, УКД2.2, УКД3.1, УКД4.2, УКД5.2, УКД6.1, УКД7.1\}$$

$$КД3 = \{УКД1.2, УКД2.2, УКД3.1, УКД4.3, УКД5.2, УКД6.1, УКД7.2\}$$

$$КД4 = \{УКД1.2, УКД2.3, УКД3.1, УКД4.4, УКД5.2, УКД6.1, УКД7.2\},$$

де УКД – умова виконання ФПБ «Довірча конфіденційність».

На основі цього побудуємо матрицю значень для кожного рівня ФПБ КД використовуючи рівняння:

$$Ui, R_i = \cup_{j=1}^{Ni} Y_j \underline{F} (i, R_i, j) \quad (1.1),$$

де U = КД, Y = УКД, $\underline{КД} = \underline{УКД}$;

$$КД = \{КД1\, КД2\, КД3\, КД4\} \quad (1.3);$$

Виходячи з цього представимо вектор УКД у вигляді добутку матриць:

$$\overline{УКД} = \{УКД1 УКД2 УКД3 УКД4 УКД5 УКД6 УКД7\} \begin{Bmatrix} 1122 \\ 1223 \\ 1111 \\ 1224 \\ 0112 \\ 1111 \\ 1113 \end{Bmatrix} (1.4);$$

Для КД 1 це буде мати такий вигляд:

$$\overline{УКД} = \{1234567\} \begin{Bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{Bmatrix} (1.5);$$

Для КД 2:

$$\overline{УКД} = \{1234567\} \begin{Bmatrix} 1 \\ 2 \\ 1 \\ 2 \\ 1 \\ 1 \\ 1 \end{Bmatrix} (1.6);$$

Для КД 3:

$$\overline{УКД} = \{1234567\} \begin{Bmatrix} 2 \\ 2 \\ 1 \\ 3 \\ 2 \\ 1 \\ 2 \end{Bmatrix} (1.7);$$

Для КД 4:

$$\overline{УКД} = \{1234567\} \begin{Bmatrix} 2 \\ 3 \\ 1 \\ 4 \\ 2 \\ 1 \\ 2 \end{Bmatrix} (1.8);$$

Опис 1.5 – 1.8 є окремими випадками формули 1.1 за умови і = 1. Проведемо обчислення за формулою 1.3. Порахуємо добуток матриць згідно з правилом множення матриць: перший елемент першої матриці множимо на перший елемент другої матриці. Далі множимо другий елемент першої матриці на другий елемент другої матриці тощо. Коли число стовпців в першому співмножнику рівне числу рядків у другому, то в цьому випадку говорять, що форма матриць узгоджена. Як наслідок, отримаємо КД 1:

$$КД1 = \{УКД1.1, УКД2.1, УКД3.1, УКД4.1, УКД6.1, УКД7.1\}$$

Підводячи підсумок слід зазначити, що ми розглянули окремий випадок кон'юнкції умов реалізації виконання ФПБ КД. Розглянутий випадок підтверджує відповідність 1.2 до рівняння 1.1. Рівняння 1.1 дозволяє формалізувати процедуру перевірки повноти та несуперечності функціонального профілю захисту.

Висновки. Таким чином, завдання визначення повноти та несуперечності ФПЗ може бути зведена до перевірки запропонованих вище правил, а саме: правило контролю цілісності КСЗІ; правило контролю взаємозв'язку одних ФПБ по відношенню до інших; правило контролю рівнів ФПБ, що дозволяє автоматизувати цей процес шляхом побудови відповідної комп'ютерної системи підтримки прийняття рішень під час проведення державної експертизи на відповідність інформації циркулюючої в грід-системі. Проведена робота дає теоретичну основу для практичної реалізації системи автоматизації перевірки повноти та несуперечності ФПЗ.

ЛІТЕРАТУРА:

1. Зегжда Д. П., Калінін М. О. Методика аналізу захищеності інформаційних систем. *Проблеми інформаційної безпеки. Комп'ютерні системи*, 2002. (3), 7–12.

2. Лукацький А. Упевненість фахівців з безпеки у своїх силах похитнулась. 2016. URL: http://gblogs.cisco.com/ru/asr2016-2/.

3. Давиденко А. Н., Шабан М. Р. Розробка методики проведення експертиз комплексних систем захисту інформації. *Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г. Є. Пухова НАН України*, 2014. (73), 114–121.

4. Новіков О. М., Тимошенко А. О. (2002). Логіко-функціональні моделі безпеки інформації в інформаційно-обчислювальних системах з відкритою архітектурою. *Наукові вісті НТУУ «КПІ»*, (2), 40–46.

5. Гільгурт Я., Дурняк Б. В., Коростиль Ю. М. Протидія атакам алгоритмічної складності на системи виявлення вторгнень. *Моделювання та інформаційні технології*, 2014. (71), 3–12.

6. Яловець А. Л. Представлення та обробка знань з точки зору математичного моделювання. Київ: Наукова думка. 2011.

REFERENCES:

1. Zegzhda, D. P., & Kalinin, M. O. (2002). Methodology for analyzing the security of information systems. *Problems of Information Security. Computer Systems*, (3), 7–12.

2. Lukatskyi, A. (2016). Confidence of security specialists has been shaken [Electronic resource]. Retrieved from: http://gblogs.cisco.com/ru/asr2016-2/.

3. Davidenko, A. N., & Shaban, M. R. (2014). Development of a methodology for conducting expertise of comprehensive information protection systems. *Collection of scientific works of the Institute of Modeling Problems in Power Engineering of the NAS of Ukraine*, (73), 114–121.

4. Novikov, O. M., & Tymoshenko, A. O. (2002). Logical-functional models of information security in information-computing systems with open architecture. *Scientific News of NTUU "KPI"*, (2), 40–46.

5. Hilhurt, Y., Durniak, B. V., & Korostyl, Y. M. (2014). Counteracting algorithmic complexity attacks on intrusion detection systems. *Modeling and Information Technologies*, (71), 3–12.

6. Yalovets, A. L. (2011). Representation and processing of knowledge from the perspective of mathematical modeling. Kyiv: Naukova Dumka.