DOI 10.34185/1562-9945-6-155-2024-20
УДК 004.056.5

Д.О. Остапець, О.О. Сухомлин

# АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ

*Анотація. У роботі проведено аналіз існуючих підходів до формування функціональних профілів захищеності (ФПЗ) в процесі створення систем захисту інформації. Метою роботи є аналіз підходів до визначення функціональних профілів захищеності при проектуванні систем захисту інформації на основі їх порівняльної характеристики. Вирішувані задачі: формування вимог до характеристик підходів та методик визначення ФПЗ, аналіз існуючих підходів та методик визначення ФПЗ та їх порівняльна характеристика. Сформовано перелік ключових характеристик відомих методик визначення ФПЗ. Проведено порівняльний аналіз методик, визначено їх переваги та обмеження. Надані рекомендації щодо покращення ефективності процесу формування ФПЗ.*

*Ключові слова: функціональний профіль захищеності, інформаційна безпека, автоматизована система, інтелектуальні методи, експертна система.*

**Постановка проблеми.** Забезпечення інформаційної безпеки (ІБ) в сучасних умовах цифровізації та активного розвитку автоматизованих систем (АС) є однією з ключових задач будь-якої організації. Особливо важливою складовою цього процесу є формування функціональних профілів захищеності (ФПЗ), які визначають рівень захисту інформації від несанкціонованого доступу (НСД). На сьогодні існує багато різних підходів до розробки ФПЗ, кожен із яких має свої переваги та обмеження. У сучасних дослідженнях відзначається важлива роль кваліфікації експерта при виборі та формуванні ФПЗ, що зумовлює актуальність розробки більш універсальних методик, які мінімізують вплив людського фактора. Ця стаття спрямована на огляд існуючих підходів до формування ФПЗ, а також їх аналіз та порівняння.

**Аналіз останніх досліджень і публікацій.** В нормативній базі України містяться документи в галузі захисту АС від НСД, що стосуються ФПЗ: НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [1], НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні ФПЗ оброблюваної інформації від несанкціонованого доступу» [2] та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації ФПЗ в засобах захисту інформації від несанкціонованого доступу» [3].

В результаті аналізу цих документів та наявних публікацій [4], стає зрозуміло наступне:





ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

- існують суперечності у вимогах до функціональних профілів захисту ФПЗ та в політиках ІБ;

- надають нечітку методику щодо вибору відповідних ФПЗ, причому всі прийняті рішення ґрунтуються на експертних оцінках та висновках фахівців з ІБ та відповідних комісій.

Методики, що описані в роботах [5-11], мають велику залежність на професійність експерта, що виконує формування ФПЗ. Таким чином, ефективність кожного методу напряму залежить від кваліфікації та досвіду цього експерта. Отже, покращення експертної оцінки при формуванні ФПЗ є актуальною проблемою.

**Мета дослідження.** Метою роботи є аналіз підходів до визначення функціональних профілів захищеності при проектуванні систем захисту інформації на основі їх порівняльної характеристики. Результати роботи можуть бути використані при реалізації засобів автоматизації проектування відповідних систем. В роботі відповідно до мети поставлені такі задачі: формування вимог до характеристик підходів та методик визначення ФПЗ, аналіз існуючих підходів та методик визначення ФПЗ та їх порівняльна характеристика.

**Основний матеріал дослідження.** Для порівняння методик, щодо визначення ФПЗ, пропонується використовувати наступні характеристики: часові витрати, складність методики, вплив кваліфікація експерта, можливість вибору нестандартних ФПЗ:

- ***Часові витрати*** - показник, що відображає, скільки часу необхідно для побудови ФПЗ відповідно до обраної методики.
- ***Складність методики*** - відображає рівень складності опанування методики, тобто наскільки легко або важко її реалізувати на практиці.
- ***Вплив кваліфікація експерта*** - характеризує, якою мірою рішення експерта з ІБ впливають на результативність та правильність вибору ФПЗ.
- ***Можливість вибору нестандартних ФПЗ*** - визначає, чи дозволяє методика створювати та використовувати ФПЗ, які не є визначеними у нормативних документах як стандартні.

НД ТЗІ 2.5-005-99 [2] описує стандартні ФПЗ, які можуть застосовуватися в державному та банківському секторах, проте без детального визначення методів їх вибору. Таким чином, із змісту нормативних документів випливає, що після аналізу середовища експерт з ІБ повинен обирати ФПЗ зі стандартних, що перекладає відповідальність за остаточне рішення на досвід та компетентність самого експерта та експертної комісії.

Методику вибору зі стандартних ФПЗ експертом з ІБ, можна визначити наступні характеристики:

- ***Часові витрати*** - значні, експерт з ІБ має провести глибокий аналіз середовища циркуляції інформації, врахувати всі необхідні критерії безпеки та на основі цього вибрати найбільш підходящий стандартний ФПЗ або той, що найбільше відповідає вимогам.
- ***Складність методики*** - середня, через обмежену кількість стандартних ФПЗ процес вибору є спрощеним, що зменшує кількість можливих варіантів і полегшує процес прийняття рішення.

- ***Вплив кваліфікація експерта*** - значний, якість виконання методики повністю залежить від компетентності та досвіду експерта, оскільки саме він визначає релевантність і відповідність стандартного ФПЗ до конкретної системи.
- ***Можливість вибору нестандартних ФПЗ*** - ні, методика не передбачає можливості створення або вибору нестандартних ФПЗ, обмежуючи гнучкість і варіативність рішень стандартними профілями.

Авторами [5] аналізуються вимоги нормативних документів щодо формування ФПЗ інформаційних систем від НСД. Автори вказують на недоліки існуючого підходу до формування таких профілів і пропонують нові методи для їх розробки, а саме автори описують новий метод, який передбачає використання спеціальних таблиць для кожної функціональної послуги захищеності. Ці таблиці дозволяють експерту визначати, які послуги необхідні для конкретної системи, і як вони мають бути реалізовані.

Задля перевірки та верифікації збудованої ФПЗ, автори описують в роботі [6] метод, який дозволяє перевірити коректність та несуперечність збудованої ФПЗ. Верифікація виконується в 3 кроки: перевірка наявності усіх необхідних послуг, перевірка сумісності послуг, викриття помилок типу "неповнота".

Метод побудови ФПЗ опитувальними таблицями та верифікацією можна охарактеризувати наступним чином:

- ***Часові витрати*** - середні, незважаючи на використання спеціальних таблиць та алгоритмів, які зменшують час на побудову ФПЗ, усе одно експерту необхідно провести аналіз загроз та відповісти на питання щодо критеріїв безпеки та верифікувати результат. Але усе одно це буде швидше ніш перебор усіх можливих варіантів вручну.
- ***Складність методики*** - середня, через використання опитувальних таблиць та алгоритму верифікації, дозволяє спростити процес побудови ФПЗ.
- ***Вплив кваліфікація експерта*** - значний, метод найбільш ефективний для досвідчених фахівців. Висококваліфікований експерт, який знайомий з принципами побудови систем захисту інформації та вимогами нормативних документів, зможе використовувати метод ефективно і швидко. Водночас методика дозволяє дещо компенсувати недостатність кваліфікації завдяки інструментам самоперевірки та детальним таблицям питань і відповідей.
- ***Можливість вибору нестандартних ФПЗ*** - так, побудова ФПЗ "з нуля" здійснюється за допомогою цього методу завдяки гнучкості таблиць, які дозволяють додавати нові функції або змінювати рівні поточних послуг. Однак створення нестандартного профілю вимагатиме більше часу та глибоких знань експерта, оскільки потрібно враховувати всі взаємозалежності між послугами безпеки та верифікувати їх.

У статті [7], автори детально описано підхід до формалізації завдання вибору оптимального ФПЗ для систем захисту інформації (СЗІ). Підхід базується на кількох ключових етапах та використовує математичне моделювання для оцінки загроз і вибору відповідних заходів захисту. Кожна загроза має свою ймовірність появи, яка залежить від зовнішніх дестабілізуючих факторів, що впливають на об’єкт захисту. Експертним шляхом визначається ймовірність появи цих факторів та їх вплив на загрози. В основі



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

підходу лежить припущення, що загроза нейтралізується відповідними засобами захисту.

Для кожної загрози розраховується ймовірність її нейтралізації через функціональні послуги. Ці послуги групуються в ФПЗ, і завданням експертів є визначення необхідного набору послуг для досягнення оптимального рівня захищеності.

Метод оптимального вибору функціонального профілю захищеності, можна охарактеризувати наступним чином:

- ***Часові витрати*** - значні, модель передбачає детальну оцінку загроз і залежностей між ними, що може потребувати значного часу, особливо при створенні нестандартних профілів.
- ***Складність методики*** - значна, через використання математичних моделей і необхідність експертних оцінок методика є складною і вимагає від експертів глибоких знань в області інформаційної безпеки.
- ***Кваліфікація експертів*** - значна, успіх реалізації методу залежить від досвіду та компетентності експертів, які повинні визначати ймовірності загроз та рівні захисту.
- ***Можливість вибору нестандартних ФПЗ*** - так, метод дозволяє гнучко адаптувати профілі захисту для нестандартних об'єктів завдяки можливості додавання або зміни функцій та рівнів послуг.

Метод вибору ФПЗ, запропонований у роботі [8], можна назвати як ймовірнісно-вартісний метод вибору ФПЗ. Він базується на формалізованій математичній моделі та охоплює кілька ключових етапів, які сприяють оптимальному вибору профілю захисту для інформаційних систем. Основна мета цього підходу – мінімізація збитків від загроз при одночасному контролі витрат на систему захисту.

Цей метод вибору ФПЗ допомагає знайти найкращий набір заходів для захисту інформаційної системи, при цьому враховуючи, скільки це буде коштувати і як добре система захисту може запобігти загрозам

Ймовірнісно-вартісний метод вибору ФПЗ можна розбити на наступні ключові етапи:

3. залучення експертів;
4. збір інформації;
5. розрахунок ймовірностей - вираховуються, наскільки ймовірно, що загрози справді можуть трапитися, і наскільки ефективними будуть засоби захисту;
6. оцінка збитків - визначають, скільки збитків може нанести загроза, і скільки вдасться уникнути завдяки захисту;
7. пошук оптимального рішення - яке найкраще захищає від загроз та не перевищує допустиму вартість реалізації.

Цей підхід допомагає створити таку систему захисту, яка не тільки добре захищає інформацію, але й допомагає знайти оптимальне рішення щодо витрачений грошей. У результаті аналізу, можна оцінити наступні характеристики:

- ***Часові витрати*** - значні, метод є досить трудомістким і потребує значного часу, оскільки включає безліч необхідних етапів.

- ***Складність методики*** - значна, метод має високу складність, оскільки він базується на математичному моделюванні та розрахунках, що включають ймовірності, оцінку збитків і впровадження оптимального рішення.
- ***Кваліфікація експертів*** - значна, від рівня знань і досвіду експертів залежить точність оцінки загроз, правильний підбір засобів захисту та визначення їхньої ефективності. Низька кваліфікація може призвести до неточних оцінок і неефективного вибору ФПЗ.
- ***Можливість вибору нестандартних ФПЗ*** - так, це можливо завдяки його гнучкості методу. Експерти можуть створювати профілі з урахуванням специфічних вимог системи та додавати нові послуги або коригувати рівні існуючих.

У статті [9] автори запропонували свій підхід до визначення стандартних ФПЗ для АС від НСД. Цей підхід базується на нормативних документах технічного захисту інформації (ТЗІ), зокрема на НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99. Цьому методу можна дати назву як - логіко-матричним методом вибору ФПЗ. З цього методу, можна виділити наступні етапи:

4. визначення залежностей між послугами;
5. розбиття критеріїв інформаційної безпеки на вимоги;
6. побудова логічної рівняння для визначення критеріїв захисту та їх рівнів;
7. використання матриці знань, що містить опис кожного критерію.

Такий підхід дозволяє створити автоматизовану систему для визначення та обґрунтування вибору стандартного ФПЗ. Цей метод можна оцінити наступним чином:

- ***Часові витрати*** - середні, метод є досить трудомістким з точки зору реалізації, але під час експлуатації дасть процес ас на вибору стандартного ФПЗ.
- ***Складність методики*** - середня, хоч під час реалізації експертної системи і потребує багато зусиль та уваги на побудову матриці знань та логічного опису критеріїв захисту. Проте, фахівцям у сфері ІБ, які мають досвід у побудові ФПЗ, цей підхід буде зрозумілим.
- ***Кваліфікація експертів*** - значна, експерта відіграє вирішальну роль, оскільки він відповідає за коректну оцінку вимог по захисту інформації, побудову функціональних профілів та правильну інтерпретацію результатів.
- ***Можливість вибору нестандартних ФПЗ*** - так, у цій роботі автори досліджували використання методу для вибору функціонального профілю захищеності зі списку стандартних. Однак, метод є досить гнучким, що дозволяє його адаптувати для створення нестандартних ФПЗ, що забезпечує більш ефективний захист інформації.

Метод вибору парето-оптимальних ФПЗ описаний автором у роботі [10] ставе задачу оптимізувати процес вибору ФПЗ. Особливу увагу приділено створенню моделі, яка враховує ресурсні обмеження. Також запропоновано метод пошуку парето-оптимальних проектних альтернатив при побудові ФПЗ.

Можна виділити наступні етапи цього методу:



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

3. Формування множини припустимих ФПЗ (для кожної АС формується множина можливих варіантів ФПЗ, де кожен варіант має свої показники безпеки та витрат на його реалізацію).

4. Визначення критеріїв оптимальності (вводяться критерії, за якими буде проводитися оцінка ФПЗ).

5. Пошук Парето-оптимальних рішень.

6. Звуження множини до єдиного рішення.

Таким чином, метод дозволяє знайти баланс між рівнем захищеності інформації та ресурсними витратами на впровадження ФПЗ. У результаті аналізу, метод вибору парето-оптимальних ФПЗ, можна оцінити наступним чином:

- ***Часові витрати*** - значні, метод є часоємким, оскільки включає декілька етапів – від формування множини варіантів ФПЗ до пошуку Парето-оптимальних рішень.
- ***Складність методики*** - значна, метод вимагає глибокого розуміння в математичній моделі та знаннях у сфері ІБ та побудові ФПЗ.
- ***Кваліфікація експертів*** - значна, від кваліфікації спеціаліста залежить точність і надійність кінцевого рішення.
- ***Можливість вибору нестандартних ФПЗ*** - так, хоча основний акцент робиться на стандартні ФПЗ, підхід дозволяє створювати нестандартні ФПЗ.

Адаптивний метод визначення ФПЗ АС на основі оптимізації загроз описано автором у роботі [11]. Метод ґрунтується на математичному моделюванні та теорії ймовірностей. Основна мета методу – підвищити ефективність побудови систем захисту АС, адаптуючи ФПЗ до поточного рівня загроз. В зазначеному методі можна виділити наступні етапи:

1. Аналіз загроз та вибір критеріїв (обираються такі критерії як ризик безпеки, гарантія безпеки, вартість реалізації захисту та інші).

2. Обчислення цільової функції (на основі обраних критеріїв і математичних моделей (включаючи оптимізацію по Беллману) проводяться обчислення).

3. Оцінка витрат та ризиків (оцінюється витрати на впровадження ФПЗ та ймовірність успішного протистояння загрозам).

Адаптивний метод визначення ФПЗ АС на основі оптимізації загроз дозволяє ефективно генерувати ФПЗ та оптимізувати його відповідно до рівня загроз та вимог безпеки. У результаті аналізу, можна оцінити наступні характеристики:

- **Часові витрати** - середні, метод зменшує час на вибір ФПЗ завдяки автоматизації процесу та використанню математичного моделювання, особливо в частині обчислення цільової функції та перевірки збіжності.
- - ***Складність методики*** - значна, оскільки метод передбачає використання оптимізаційних моделей (зокрема, методу Беллмана) і застосування теорії ймовірностей, що вимагає не лише знань у галузі ІБ, але й розуміння математичних методів.
- - ***Кваліфікація експертів*** - значна, метод вимагає значну кваліфікацію експерта, особливо на етапі вибору початкових даних, таких як критерії оцінки загроз та ризиків.

- ***Можливість вибору нестандартних ФПЗ*** - так, метод передбачає можливість вибору нестандартних ФПЗ, оскільки він підтримує гнучке налаштування критеріїв і адаптацію до поточних загроз.

На основі проведеного аналізу методик визначення ФПЗ, виконано їх порівняльну характеристику, результати якої представлено в табл. 1.

Порівнюючи методики визначення ФПЗ від НСД, можна побачити, що всі з них вимагають значних часових ресурсів та більшість з них потребують необхідних знань та навичок. Окрема увага приділяється кваліфікації експерта, від якої залежить ефективність побудованої ФПЗ. Більшість методів підтримують можливість розробки нестандартних ФПЗ, що свідчить про їх здатність відповідати сучасним вимогам у сфері ІБ. Таким чином, можна запропонувати покращити ефективність процесу визначення ФПЗ шляхом побудови експертних систем із використанням інтелектуальних методів, які можуть також зменшити вплив кваліфікації експерта на результат сформованого ФПЗ.

Таблиця 1

Порівняльна характеристика методик визначення ФПЗ

| Методика побудови ФПЗ | Характеристики | | | |
|---|---|---|---|---|
| | Часові витрати | Складність методики | Вплив кваліфікації експерта | Побудова нестандартних ФПЗ |
| Вибір зі стандартних ФПЗ експертом | значні | середня | значний | ні |
| Метод побудови ФПЗ опитувальними таблицями та верифікацією | середні | середня | значний | так |
| Метод оптимального вибору ФПЗ | значні | значна | значний | так |
| Ймовірнісно-вартісний метод вибору ФПЗ | значні | значна | значний | так |
| Логіко-матричним методом вибору ФПЗ | середні | середня | значний | так |
| Метод вибору парето-оптимальних ФПЗ | значні | значна | значний | так |
| Адаптивний метод визначення ФПЗ АС на основі оптимізації загроз | середні | значна | значний | так |



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

**Висновки.** У роботі проведено огляд та аналіз існуючих методик до формування ФПЗ автоматизованих систем. Визначено ключові характеристики, що описують методики побудови ФПЗ, зокрема кваліфікацію експерта, складність методик, часові витрати та можливість створення нестандартних профілів. Порівняння існуючих методик дозволило визначити їх переваги та обмеження, що дає можливість для подальшого вдосконалення процесу визначення ФПЗ. Зазначено, що покращити ефективність процесу формування ФПЗ можна шляхом побудови експертних систем із використанням інтелектуальних методів.

**ЛІТЕРАТУРА**

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. – Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649
2. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. – Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/
3. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-010-09. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=103247
4. Паламарчук Н.А., Хлапонін Ю.І., Овсянніков В.В. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації // Збірник наукових праць ВІТІ НТУУ «КПІ» – К.: ВІТІ НТУУ «КПІ», 2011. №3. С. 78 – 82. Режим доступу: http://viti.edu.ua/files/zbk/2011/11_3_2011.pdf
5. Лєншин А.В., Буслов П.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу // Радіоелектронні і комп'ютерні системи : науч. тр. – Х.: Нац. аэрокосм. ун-т "ХАИ", 2010. – Вып. 7(48). – С. 77–81. – Режим доступу: http://nbuv.gov.ua/UJRN/recs_2010_7_15
6. Потій О.В., Лєншин А.В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу //Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2010. – Том 9. – №3. – С.479 – 488. – Режим доступу: http://openarchive.nure.ua/handle/document/410
7. Пискун С. Ж., Хорошко В.О. Оптимізація вибору функціонального профілю захищеності // Сучасна спеціальна техніка. - 2011. - № 3. - С. 36-40. - Режим доступу: http://nbuv.gov.ua/UJRN/sstt_2011_3_8
8. Ткач Ю. М. Метод вибору функціонального профілю захищеності // Інформатика та математичні методи в моделюванні.- 2020. Т. 10, № 1-2. С. 68-74.
9. Юдін О.К., Бучик С.С., Мельник С.В. Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу. Наукоємні технології. 2016. Вип. 2. С. 195-205.

10. Берестов Д.С. Методика вибору проектних альтернатив системи захисту інформації в автоматизованій системі відомчого призначення на основі ієрархічних моделей: автореф. дис. канд. техн. наук: 05.13.21. Київ, 2015. - 21 с.
11. Потенко О.С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз: автореф. дис. канд. техн. наук : 05.13.21. Київ, 2024. - 24 с.

**REFERENCES**

1. Criteria for Assessing Information Security in Computer Systems from Unauthorized Access: ND TZI 2.5-004-99. – Available at: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649
2. Classification of Automated Systems and Standard Functional Security Profiles of Processed Information from Unauthorized Access: ND TZI 2.5-005-99. – Available at: http://www.dstszi.gov.ua/dstszi/doccatalog/
3. Methodical Guidelines for Assessing the Level of Correctness Guarantees in Implementing Functional Security Services in Information Protection Tools from Unauthorized Access: ND TZI 2.7-010-09. – Available at:
http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=103247
4. Palamarchuk N.A., Khlaponin Yu.I., Ovsyannikov V.V. The Current State of the Regulatory Framework in the Field of Technical Information Protection // Collection of Scientific Papers of VITI NTUU "KPI" – K.: VITI NTUU "KPI", 2011. No. 3. P. 78-82. Available at: http://viti.edu.ua/files/zbk/2011/11_3_2011.pdf
5. Lenshin A.V., Buslov P.V. Method of Forming Functional Security Profiles from Unauthorized Access // Radio-electronic and Computer Systems: Scientific Journal – Kharkiv: National Aerospace University “KhAI”, 2010. – Issue 7(48). – P. 77–81. – Available at: http://nbuv.gov.ua/UJRN/recs_2010_7_15
6. Potii O.V., Lenshin A.V. Methods of Building and Verifying the Consistency and Completeness of Functional Security Profiles from Unauthorized Access // Scientific and Technical Journal "Applied Radio Electronics. Thematic Issue Devoted to Information Security Problems”. – Kharkiv, 2010. – Vol. 9. – No. 3. – P. 479–488. – Available at:
openarchive.nure.ua/handle/document/410.
7. Piskun S.G., Khoroshko V.O. Optimization of Functional Security Profile Selection // Modern Special Equipment. - 2011. - No. 3. - P. 36-40. - Available at:
http://nbuv.gov.ua/UJRN/sstt_2011_3_8
8. Tkach U. M. Method of Selecting a Functional Security Profile // Informatics and Mathematical Methods in Modeling. – 2020. – Vol. 10, No. 1-2. – P. 68-74.
9. Yudin O.K., Buchyk S.S., Melnyk S.V. Theoretical Foundations for Defining Standard Functional Security Profiles of Automated Systems from Unauthorized Access. High-Tech Technologies. 2016. Issue 2. P. 195-205.
10. Berestov D.S. Methodology for Selecting Design Alternatives for Information Protection Systems in Departmental Automated Systems Based on Hierarchical Models: PhD Thesis Abstract in Technical Sciences: 05.13.21. Kyiv, 2015. - 21 p.


ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

11. Potenko O.S. Methods for Defining the Functional Security Profile of an Automated System Considering the Current Threat Level: PhD Thesis Abstract in Technical Sciences: 05.13.21. Kyiv, 2024. - 24 p.

Received 12.11.2024.
Accepted 19.11.2024.

***Analysis of existing approaches to the formation of functional security profiles***

*The work examines existing methods for forming functional security profiles (FSP) for information protection systems. The purpose of the work is to analyze approaches to determining FSP when designing information protection systems based on their comparative characteristics. Solved tasks: formation of requirements for the characteristics of approaches and methods for determining the FSP, analysis of existing approaches and methods for determining the FSP and their comparative characteristics. The authors explore the key characteristics of various methodologies, such as time consumption, complexity, the influence of expert qualification, and the possibility of creating non-standard profiles. The work compares the advantages and limitations of existing methods. The research shows that all methodologies require significant time and are dependent on the qualifications of specialists. At the same time, most methods support the development of non-standard profiles, allowing them to be adapted to specific information security requirements. Based on the analysis, it is concluded that the use of automated systems based on intelligent methods is necessary to improve the efficiency and accuracy of FSP formation. Thus, the work makes a significant contribution to the field of information security research, providing practical recommendations for improving methodologies for forming FSP in the context of increasing threats in the information technology sphere.*

**Остапець Денис Олександрович** – к.т.н., доцент, доцент кафедри «Електронні обчислювальні машини» Українського державного університету науки і технологій, ORCID: 0000-0003-1778-7770

**Сухомлин Олексій Олександрович** – аспірант кафедри «Електронні обчислювальні машини» Українського державного університету науки і технологій, ORCID: 0009-0006-7928-4721

**Ostapets Denys** – candidate of technical sciences, associate professor, associate professor of «Electronic computers» department of Ukrainian State University of Science and Technologies, ORCID: 0000-0003-1778-7770

**Sukhomlyn Oleksii** – graduate student of «Electronic computers» department of Ukrainian State University of Science and Technologies, ORCID: 0009-0006-7928-4721