УДК 004.056

В.Б. Дудикевич, доктор технічних наук, професор
Г.В. Микитин, кандидат технічних наук
О.Я. Рудник

ФУНКЦІОНАЛЬНА БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ЗАСАДИ, МЕТОДОЛОГІЯ, РЕАЛІЗАЦІЯ

У рамках розгляду проблеми стратегічної безпеки об'єктів та життєвого циклу функціональної безпеки систем і програмного забезпечення у статті запропоновано методологію захисту структури інформаційних технологій: ресурсів, систем, процесів, мереж, управління, відповідно до якої реалізовано систему виявлення атак в інформаційних мережах.

Ключові слова: *стратегічна і функціональна безпека, інформаційна технологія, система, атака, алгоритмічно-програмне забезпечення.*

В рамках рассмотрения проблемы стратегической безопасности объектов и жизненного цикла функциональной безопасности систем и программного обеспечения в статье предложена методология защиты структуры информационных технологий: ресурсов, систем, процессов, сетей, управления, в соответствии с которой реализована система обнаружения атак в информационных сетях.

Ключевые слова: *стратегическая и функциональная безопасность, информационная технология, система, атака, алгоритмически-программное обеспечение.*

As a part of the strategic problems of security objects and life cycle of functional security systems and software several proposals for the methodology of protection structure of information technologies: resources, systems, processes, networks, management, whereby implemented system attack detection in information networks are given.

Keywords*: strategic and functional safety, information technology, system, attack, algorithmic-based software.*

Стратегічна безпека критичних об'єктів: безпека експлуатації, комплексна ІТ-безпека

Безпека об'єктів – енергетичного обладнання атомних і теплових станцій, аерокосмічного обладнання, нафтогазопроводів, конструкцій мостів і т. ін., які працюють в гранично допустимих умовах, перебувають у системі факторів впливу, сьогодні вимагає системного підходу щодо її оцінювання та забезпечення.

Одним із напрямів дослідження стану безпеки техногенних об'єктів є технічна діагностика, контроль параметрів, прогнозування залишкового ресурсу. Безпека експлуатації технологічного обладнання промислової інфраструктури передбачає розроблення підходів до забезпечення міцності матеріалів і довговічності конструкцій.

Проблема вирішується методами і засобами інформаційних технологій дослідження механічних властивостей конструкційних матеріалів, які, зокрема, працюють в агресивному середовищі. У літературі [1] представлений комплекс підходів щодо проблеми ресурсу конструкцій, споруд, машин у контексті

застосування методів і засобів відбору даних про стан об'єкта, методик оцінювання залишкового ресурсу елементів конструкцій.

Для точності відбору інформації від різнорідних об'єктів, оцінювання та прийняття рішення на управління інформаційні технології самі повинні відповідати вимогам безпеки. Гарантоздатність систем і програмного забезпечення, які обумовлюють рівень функціональної безпеки автоматизованих систем управління, достовірність даних, є основою інформаційної безпеки.

Аналогічна ситуація сьогодні склалася з проблемою безпеки природних об'єктів у рамках системи моніторингу екосистем – програми, інформаційних технологій, методичного забезпечення.

Актуальною є *стратегічна безпека об'єктів* – синтез безпеки експлуатації техногенних об'єктів, безпеки використання природних об'єктів та комплексної безпеки ІТ, направлених на забезпечення довготривалого ресурсу й, відповідно, якості параметрів і прийняття рішення для управління проблемно-об'єктною ситуацією в рамках системи моделей.

Засади функціональної безпеки інформаційних технологій

Проблема безпеки об'єктів у контексті інформаційних технологій (ІТ) сьогодні розвивається ученими на міжнародному рівні [2]. Методи підтримки ІТ-безпеки на рівні програмного забезпечення представлені у працях [3, 4]. Актуальними залишаються питання розроблення методів та засобів функціональної безпеки технологій, які, власне, забезпечують безпеку експлуатації критичних об'єктів. Такі дослідження проводяться в рамках міжнародного нормативного забезпечення [5] на рівні систем та програмного забезпечення [6–10].

З метою розроблення комплексної методології захисту інформаційних технологій та практичної реалізації на одному з рівнів ієрархічної структури ІТ розглянемо засади нормативного забезпечення з функціональної безпеки.

Система стандартів [11] регламентує вимоги до функціональної безпеки для всього життєвого циклу систем, що складаються з електричних і/або електронних та і/або програмованих електронних компонентів (Е/Е/РЕ), які використовують для виконання функцій безпеки; програмного забезпечення; застосування методів визначення рівнів повноти безпеки; управління (рис. 1).

Для досягнення необхідного рівня повноти безпеки Е/Е/РЕ-систем, пов'язаних із безпекою інформаційних технологій, а відповідно, і природно-техногенною безпекою об'єктів у системі стандартів ГОСТ Р МЭК 61508-1-2007 – ГОСТ Р МЭК 61508-7-2007 прийнята технічна модель повного життєвого циклу безпеки (рис. 2). Основою моделі повного життєвого циклу безпеки є: Е/Е/РЕ-системи; системи безпеки на інших технологіях; зовнішні засоби зменшення ризику.

Побудова концепції функціональної безпеки на повному життєвому циклі інформаційних технологій, призначених для відбору різнорідних даних від критичних об'єктів, оцінювання їх стану та прийняття рішення на стратегічне управління вимагає проведення відповідних процедур.

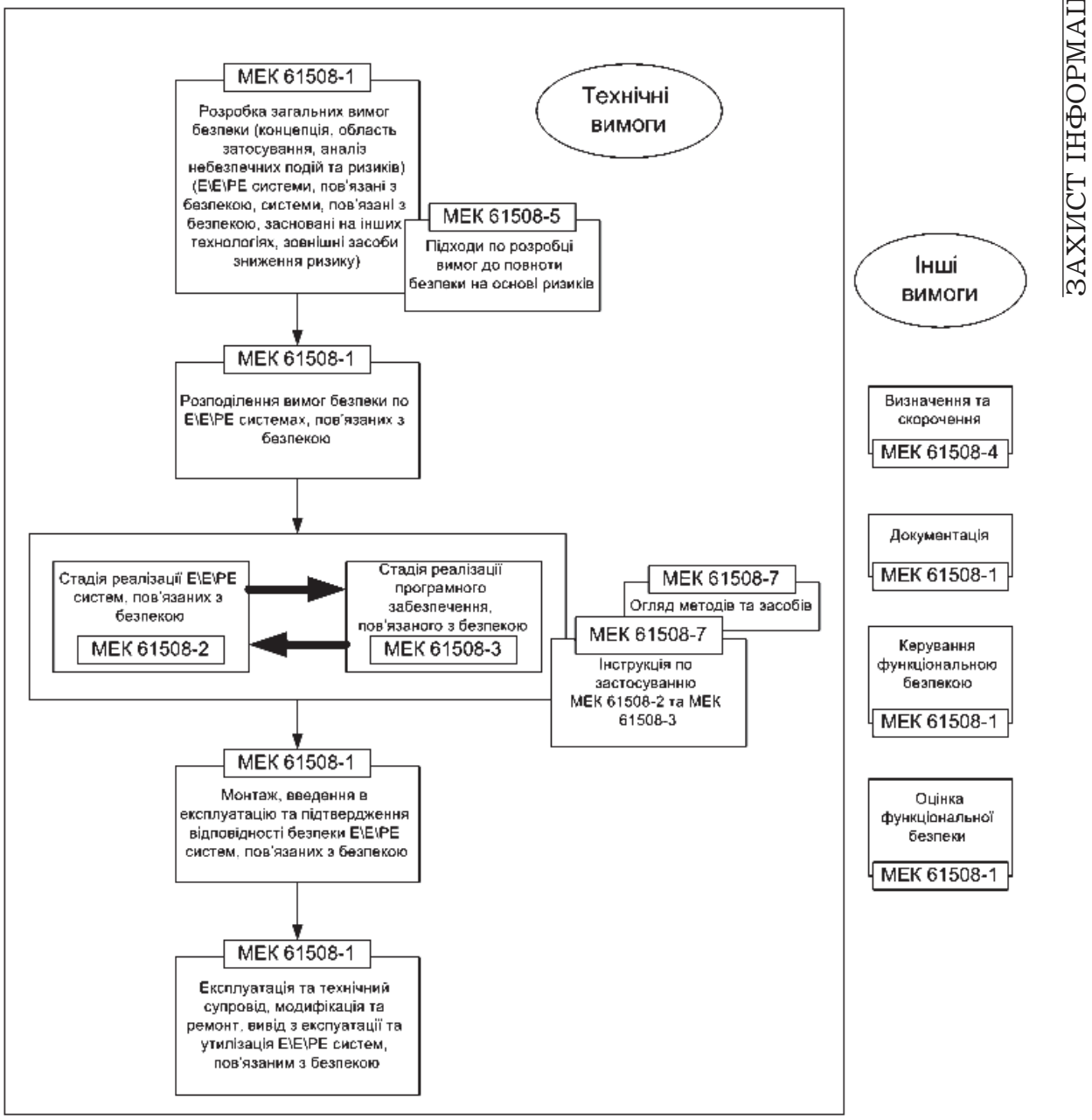

Рис. 1. Структура функціональної безпеки ІТ: системи, програмне забезпечення

До таких процедур відносяться: збір інформації про об'єкт дослідження, функції управління, навколишнє середовище; визначення потенційних джерел небезпеки та критичних ситуацій; отримання інформації про встановлені види небезпеки – руйнування, корозійність, реакційна здатність, токсичність тощо; отримання інформації про поточний стан регулювання у сфері безпеки на національному та міжнародному рівнях; встановлення видів небезпеки, які виникають внаслідок взаємодії досліджуваного об'єкта з об'єктами ближнього розташування.

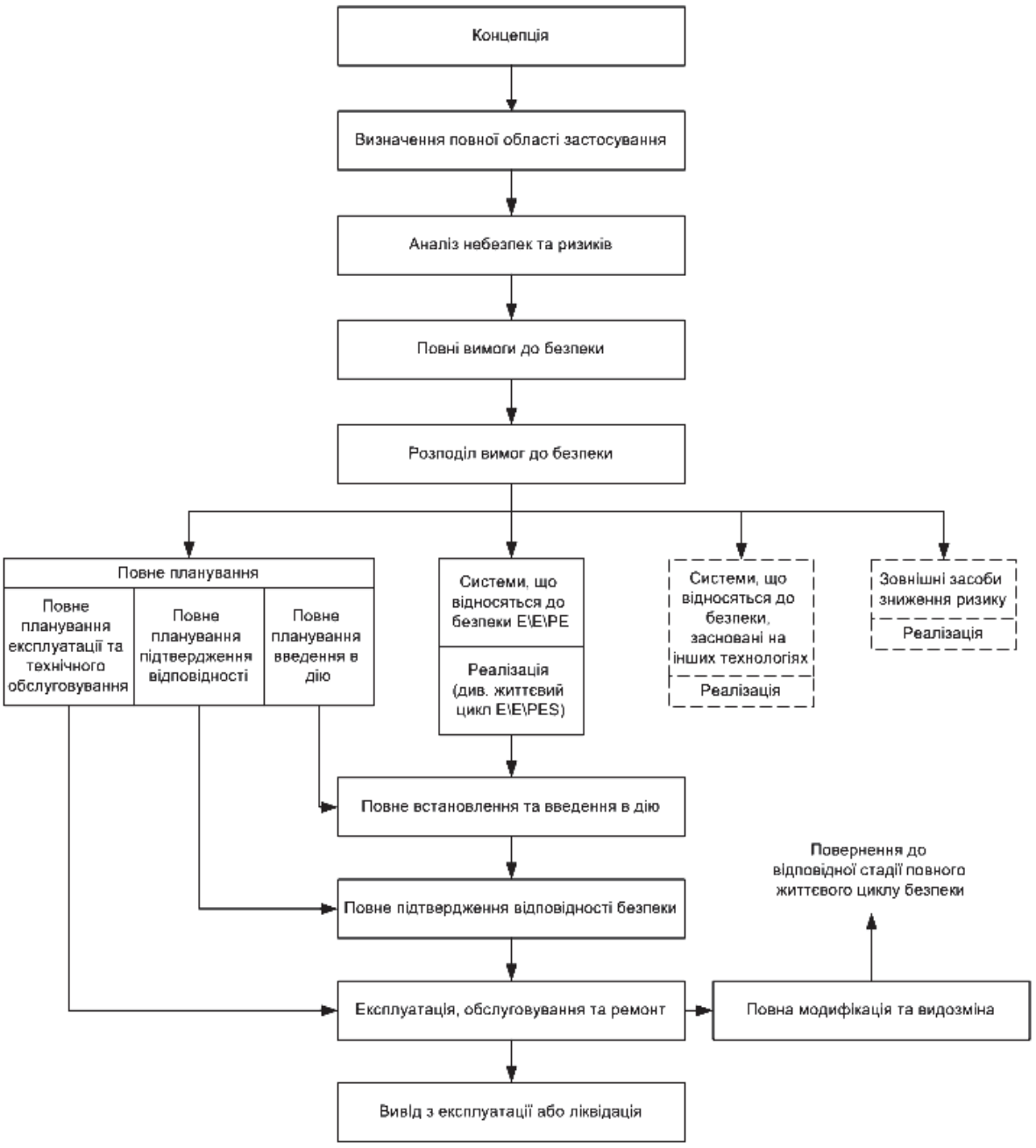

Рис. 2. Модель повного життєвого циклу функціональної безпеки ІТ

Модель життєвого циклу систем E/E/PES показано на рис. 3. Модель життєвого циклу безпеки програмного забезпечення показано на рис. 4. Структура взаємозв'язку моделей: повного життєвого циклу безпеки, життєвого циклу безпеки E/E/PES та життєвого циклу безпеки програмного забезпечення показано на рис. 5. Модель повного життєвого циклу функціональної безпеки інформаційних технологій розкривається на рівні концепції гарантоздатності систем та програмного забезпечення.

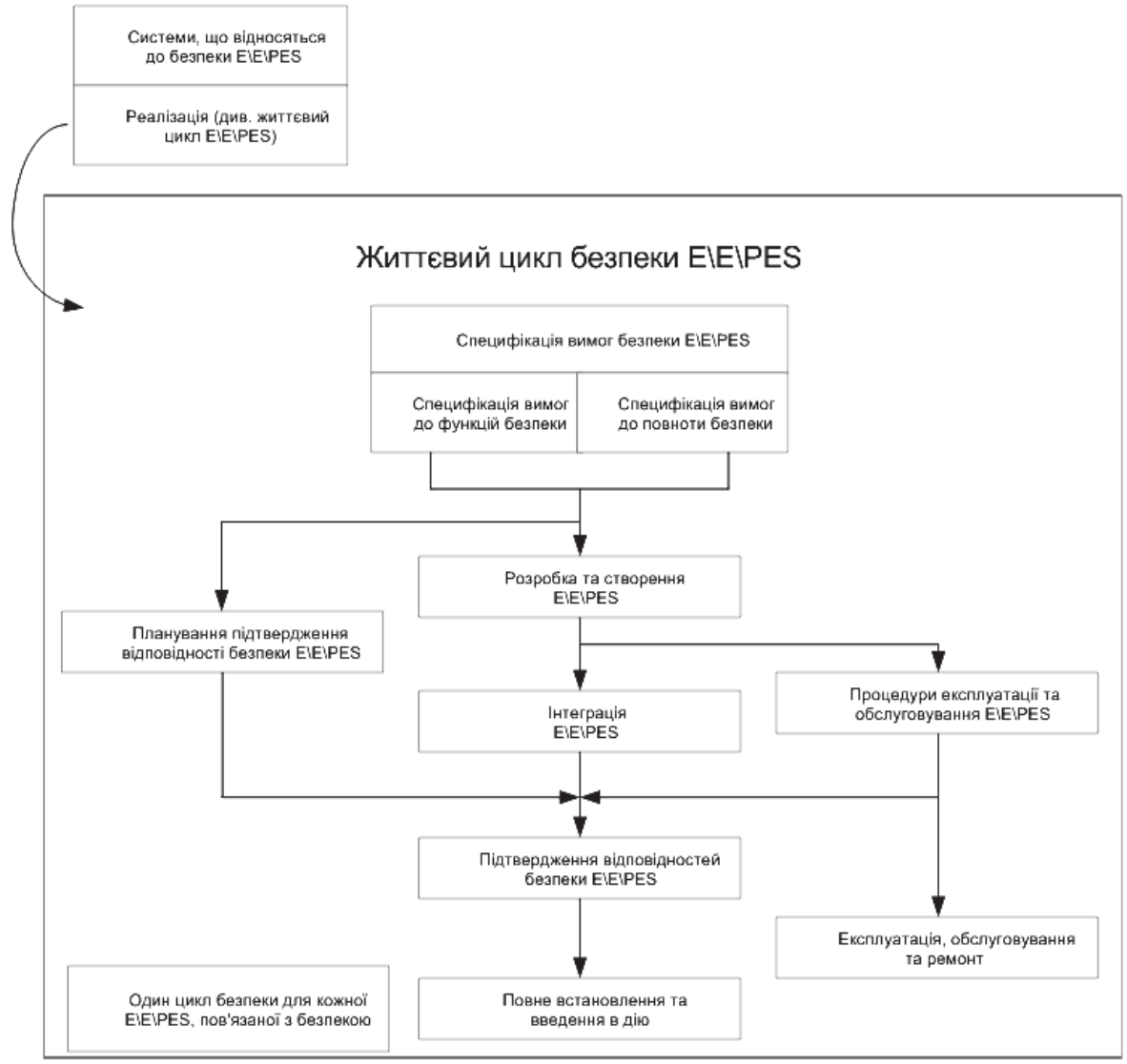

Рис. 3. Життєвий цикл безпеки E/E/PES на етапі реалізації

Гарантоздатність систем і програмного забезпечення становить основу для підвищення надійності на апаратно-програмному рівні функціональної безпеки; відповідно, забезпечення достовірності даних є основою інформаційної безпеки ІТ.

Концепція гарантоздатності дозволяє реалізувати модель повного життєвого циклу функціональної безпеки ІТ, ядром якої є інформаційна. Підтвердженням цьому є характеристики гарантоздатності: доступність – готовність до використання; надійність – здатність забезпечити неперервність обслуговування під час використання; безпечність – відсутність небезпечного впливу на оточення; захищеність – здатність зберегти конфіденційність; ремонтопридатність [12, 13, 14].

Сьогодні набуває актуальності тенденція системного представлення гарантоздатності на рівні апаратно-програмного забезпечення. Наприклад, у роботі [15] досліджується метод оцінювання гарантоздатності криптографічних комп'ютерних систем цифрового підпису на основі використання еліптичних кривих.

Рис. 4. Життєвий цикл безпеки програмного забезпечення на етапі реалізації

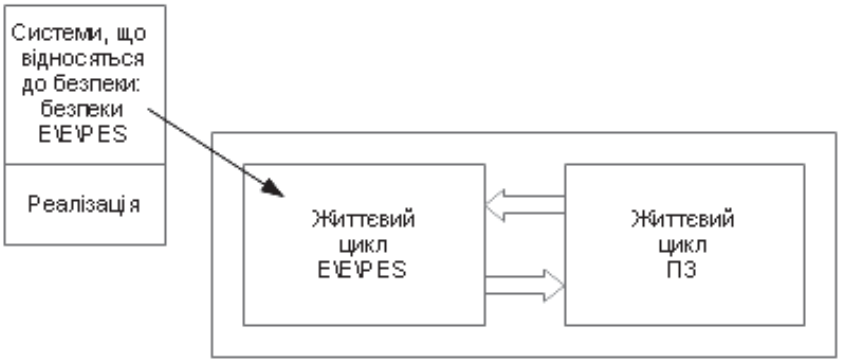

Рис 5. Взаємозв'язок між моделями циклів безпеки – повного, системи, програмного забезпечення

Розглянемо деякі елементи гарантоздатності – базового сегмента функціональної безпеки ІТ на рівні реалізації системи виявлення атак в інформаційних мережах.

Методологія захисту інформаційних технологій

Актуальною є комплексна безпека ІТ в контексті гарантоздатності автоматизованих систем, яка охоплює: функціональну безпеку ІТ – методи і засоби забезпечення надійності систем, та інформаційну безпеку – методи і засоби підвищення достовірності інформації, і становить основу стратегічної безпеки техногенних і природних об'єктів.

Запропонована методологія комплексної системи безпеки інформаційних технологій (ІТ) ґрунтується на моделі об'єкт (1–5) – загроза (а–е) – захист (А–Е) (рис. 6) [16].

Інформаційні технології обробки даних (ОД), управління, підтримки прийняття рішень, експертних систем як об'єкт захисту представлені системою взаємозв'язку та взаємодії рівнів:

– інформаційних ресурсів (1) – баз даних (БД), сховищ даних (СД), баз знань (БЗ), баз моделей (БМ), масивів інформації (МІ);

– інформаційних систем (2) – інформаційно-аналітичних систем (ІАС), вимірювальних інформаційних систем (ВІС), автоматизованих систем управління (АСУ), систем автоматизації офісу (САО), систем підтримки прийняття рішень (СППР), експертних систем (ЕС);

– інформаційних процесів (3);

– інформаційних мереж (каналів) (4);

– комплексне управління (5) – життєвим циклом інформації, системою безпеки ІТ.

П'ятирівневий захист формує комплексну систему безпеки ІТ обробки даних, управління, автоматизації офісу, підтримки прийняття рішень, експертних.

На першому рівні захисту підлягають інформаційні ресурси: масиви інформації у різних предметних сферах, бази моделей, бази і банки даних у відповідних інформаційних системах.

На другому рівні – передбачається захист функціональних апаратних (фізичних, технічних) та програмних елементів конкретної інформаційної системи (ІС) для завдань управління у предметних сферах.

Третій рівень – передбачає захист інформаційних процесів, які протікають в інформаційній системі: сприйняття / збір / відбір, обробка, зберігання, представлення, передавання інформації, які формують інформаційний зміст фаз, операцій та обробки даних.

Четвертий рівень – передбачає захист інформаційних мереж (каналів) (ІМ) відповідно до їх класифікації та топології.

На п'ятому рівні – передбачається управління об'єктом – життєвим циклом інформації, яка функціонує в ІС, та управління комплексною системою безпеки інформаційних технологій.

Оскільки інформаційні мережі є основною ланкою взаємодії системи об'єкт – ІТ, то, відповідно, пропонується реалізація системи виявлення атак в ІМ на рівні алгоритмічно-програмного забезпечення.

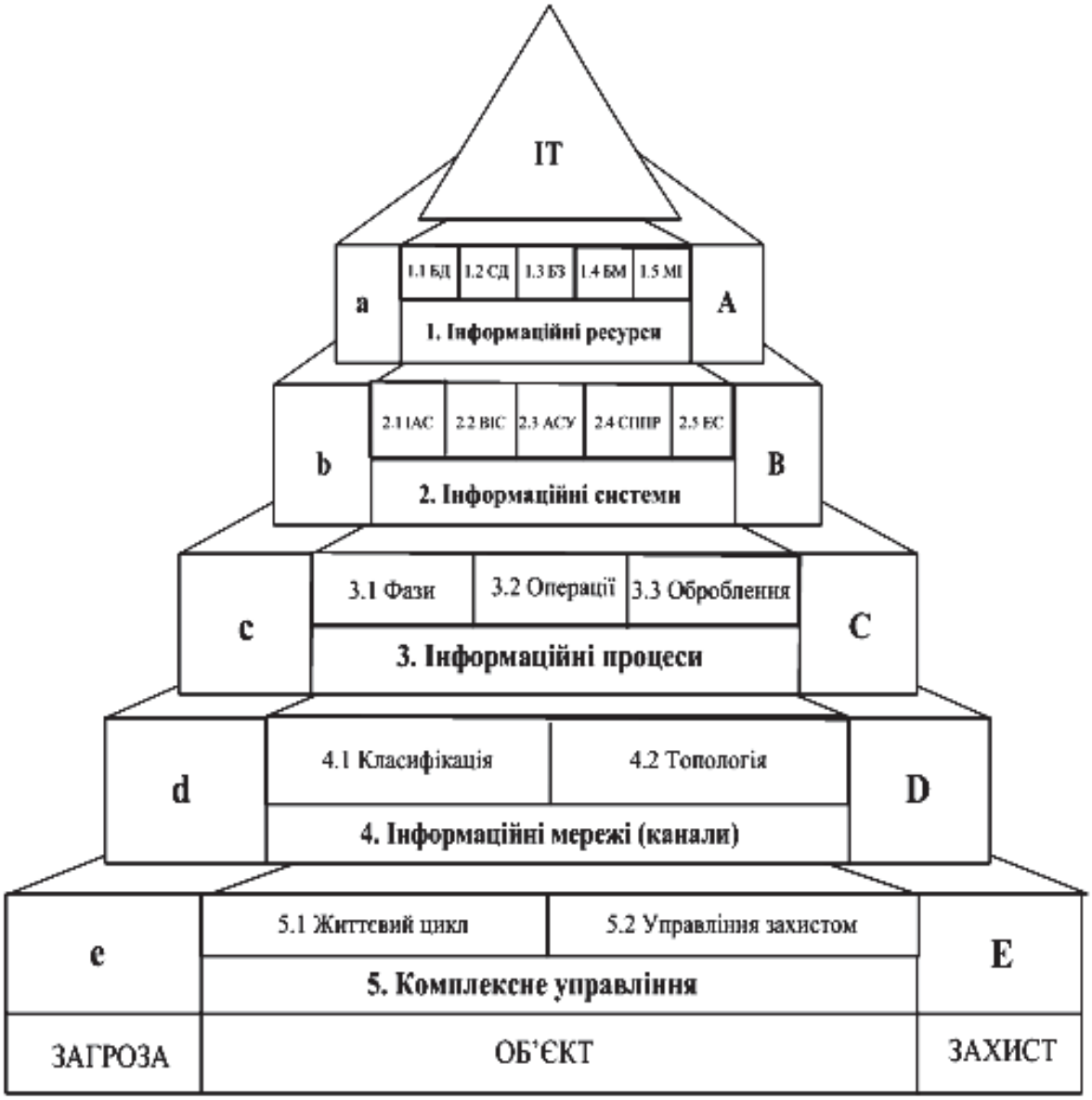

Рис. 6. Методологія захисту інформаційних технологій

Реалізація системи виявлення атак на рівні інформаційних мереж

Підхід до реалізації системи виявлення атак в інформаційних мережах.

Пропонується підхід до реалізації системи виявлення атак (СВА) як додатку до міжмережевого екрану (МЕ). Міжмережевий екран виконує функції частини елементів СВА, а решту виконує розроблене програмне забезпечення (ПЗ). Загальноприйнята структура системи виявлення атак охоплює: сенсор, аналізатор (детектор), засоби управління та реагування (менеджер) [17].

Розроблену СВА представлено дворівневою структурою на рис. 7. Задачі сенсора та первинного детектора виконує міжмережевий екран. Скрипт налаштувань міжмережевого екрану містить набори правил (сигнатур), за якими обслуговується вхідний/вихідний трафік, та дії, які необхідно виконати у випадку виявлення порушення (атаки, збою системи т.і.). Розроблене ПЗ інтегрується з МЕ, виконує задачі вторинного детектора та менеджера системи виявлення атак.

Сенсор у структурі СВА – призначений для зв'язку з обчислювальним середовищем, він відбирає необхідну для виявлення втручань інформацію, фільтрує її та надсилає до детектора. Первинний детектор – на основі відповідних критеріїв безпосередньо виявляє втручання та передає інформацію в log-файл. Вторинний детектор – здійснює аналіз отриманої первинним детектором інформації та здійснює уточнення: підтверджує факт виявлення або відкидає його. Менеджер – контролює решту компонентів СВА, приймає рішення щодо ініціювання тривоги та реалізації відповідних контрзаходів.

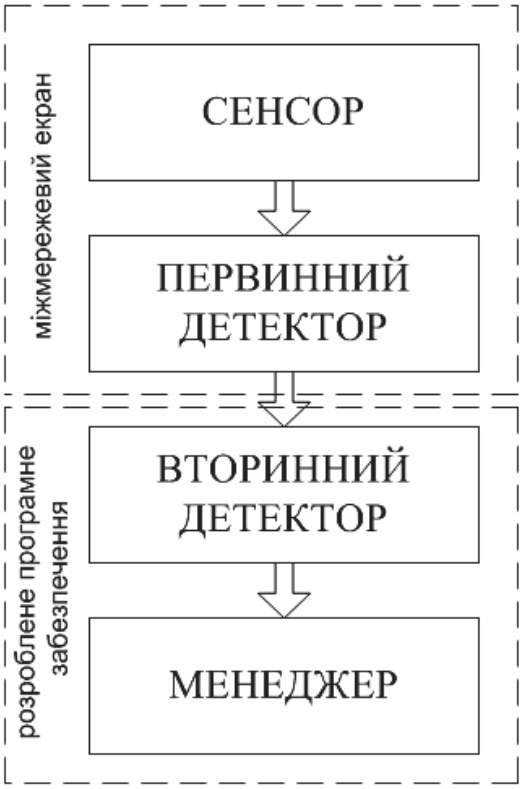

Рис. 7. Загальний підхід до реалізації системи виявлення атак в ІМ

Відмінність запропонованої СВА від структури загальноприйнятої: за рахунок того, що частина операцій детектування виконується міжмережевим екраном, а частина – відповідно розробленим програмним забезпеченням – етап детектування розділюється на два підетапи, що уможливлює підвищення точності виявлення загроз в інформаційній мережі та зменшення коефіцієнту помилкових спрацьовувань.

Алгоритм роботи системи виявлення атак. Алгоритм роботи запропонованої системи виявлення атак в інформаційній мережі представлений на рис. 8. При запуску програми за допомогою відповідної команди з консолі операційної системи запускається демон графічного інтерфейсу, який працює поки не отримає команду на вимкнення.

Демон графічного інтерфейсу запускає в окремому потоці модуль аналізу та детектування, який працює паралельно з графічним інтерфейсом до отримання другим команди на вимкнення.

Модуль аналізу та детектування зчитує інформацію з log-файлів міжмережевого екрану і здійснює її обробку. При виявленні атаки модуль передає сигнал демону графічного інтерфейсу, який виводить вікно з попереджувальним повідомленням та продовжує аналіз. Зчитування інформації здійснюється через задані інтервали часу, починаючи з моменту попереднього зчитування.

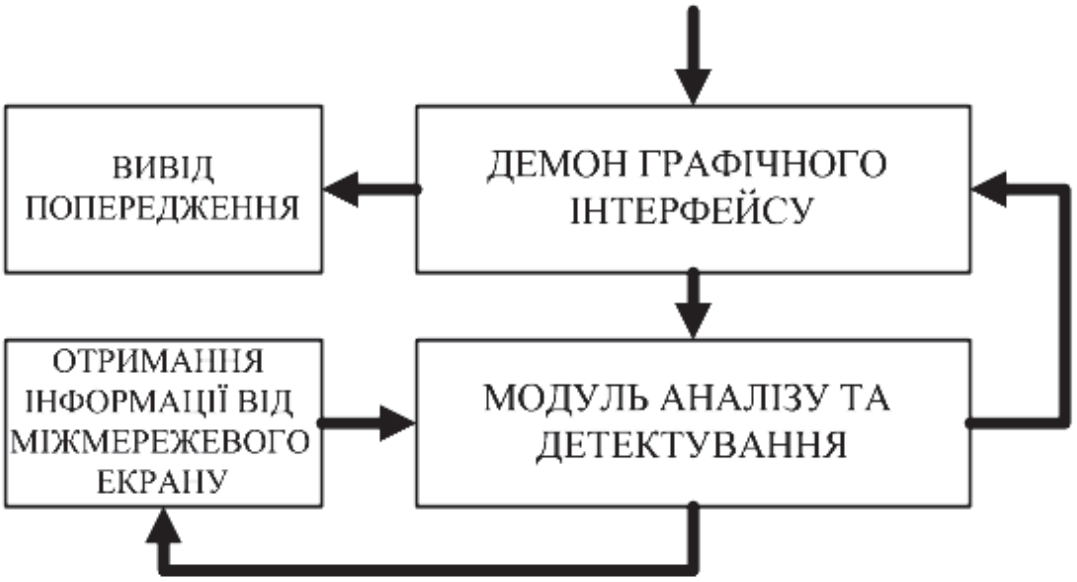

Рис. 8. Алгоритм роботи розробленої системи виявлення атак в ІМ

Зчитування та аналіз виконується паралельно з роботою модуля графічного інтерфейсу незалежно одне від одного. Також реалізований механізм доповнення інформації у вікні попереджень, якщо адміністратор/відповідальна особа з якоїсь причини не закрили вікно з попереднім повідомленням, для уникнення ситуації з втратою інформації про атаку та уникнення захаращування екрану вікнами попереджень. При виклику нового вікна попередження, якщо старе вікно не було закрите, воно закривається, інформація доповнюється та виводиться в новому вікні.

Проаналізовано актуальність стратегічної безпеки критичних об'єктів. Розглянуто засади функціональної безпеки ІТ на рівні систем та програмного забезпечення. Розроблено методологію захисту структури ІТ: ресурсів, систем, процесів, мереж, управління. Запропоновано підхід до створення системи виявлення атак в інформаційних мережах у контексті алгоритмічно-програмного забезпечення ІТ-безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Проблеми ресурсу і безпеки експлуатації конструкцій, споруд і машин. Цільова комплексна програма НАН України // Збірник наукових праць за результатами, отриманими у 2007–2009 рр. – К. : Інститут електрозварювання ім. О.Є. Патона НАН України, 2009. – 709 с.

2. *Харченко В.С.* Аналіз проблем ІТ-інженерії безпеки : проект TEMPUS-SAFEGUARD / В.С. Харченко // Радіоелектронні і комп'терні системи. – 2010. – № 7 (48). – С. 297–300.

3. *Скляр В.В.* Оцінка програмного забезпечення інформаційних та управляючих систем АЕС при експертизі ядерної й радіаційної безпеки / В.В. Скляр, М.Я. Ястребенець-

кий, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2008. – № 6 (33). – С. 180–184.

4. *Єфімова Т.І.* Відмовостійкість програмного забезпечення гарантоздатних комп'ютерних систем / Т.І. Єфімова , М.Г. Мудла, О.М. Шалейко // Математичні машини і системи. – 2009. – № 4. – С. 200–209.

5. *Дэвид Дж. Смит.* Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов / Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон. – М. : Издательский Дом "Технологии", 2004. – 208 с.

6. *Ястребенецкий М.А.* Оценка уровня безопасности информационных и управляющих систем АЭС / М.А. Ястребенецкий, В.В. Инюшев, О.Н. Бутова // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 96–103.

7. *Шубинский И.Б.* Безопасность критически важных информационных систем / И.Б. Шубинский, А.А. Тарасов // Транспортная безопасность и технологии. – 2005. – № 4. – С. 20–21.

8. *Похил В.С.* Методы оценивания и обеспечения функциональной безоспасности бортовых информационно-управляющих систем летательных аппаратов / В.С. Похил, А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2010. – № 7. – С. 278–282.

9. *Бахмач Е.С.* Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС / Е.С. Бахмач, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 7. – С. 75–82.

10. *Липаев В.В.* Функциональная безопасность программных средств / В.В. Липаев. – М. : СИНТЕГ. – 2004. – 384 с.

11. ГОСТ Р МЭК 61508-1-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования (IEC 61508-1:1998, IDT). – М. : Стандартинформ. – 2008. – 96 с.

12. СОУ-Н НКАУ 0060:2010. Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення. Настанова Національного космічного агентства України. – К., 2011. – 60 с.

13. *Харченко В.С.* Гарантоздатність комп'ютерних систем : межа універсальності в контексті інформаційно-технічних станів / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 7–14.

14. *Мудла Б.Г.* Гарантоздатність як фундаментальний узагальнюючий та інтегруючий підхід / Б.Г. Мудла, Т.І. Єфімова, Р.М. Рудько // Математичні машини і системи. – 2010. – № 2. – С. 148–165.

15. *Глухов В.* Оцінювання гарантоздатності криптографічних комп'ютерних систем / В.Глухов // Комп'ютерні науки та інформаційні технології. – № 616. – 2008. – С. 66–72.

16. *Дудикевич В.* Методологічні засади захисту інформаційних технологій / В. Дудикевич, Л. Сікора, Г. Микитин, О. Рудник // Захист інформації і безпека інформаційних технологій : Матеріали І-ої Міжнародної наук.-тех. конф. (31 травня – 1 червня 2012 р.), Львів. – С. 8–9.

17. *Биячуев Т.А.* Безопасность корпоративных сетей / Т.А. Биячуев ; под ред. Л.Г. Осовецкого. – СПб. : ГУ ИТМО, 2004. – 161 с.

Отримано 29.03.2013