Микитин Г. Засади стратегічної безпеки системи “об’єкт – інформаційна технологія” / Г. Микитин // Вісник ТНТУ — Тернопіль : ТНТУ, 2014. — Том 74. — № 2. — С. 189-198. — (приладобудування та інформаційно-вимірювальні технології).

УДК 004:056

Г. Микитин, докт. техн. наук

Національний університет “Львівська політехніка”

ЗАСАДИ СТРАТЕГІЧНОЇ БЕЗПЕКИ СИСТЕМИ “ОБ’ЄКТ – ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ”

***Резюме**. Проаналізовано аспекти безпеки техногенних об’єктів та безпеки інформаційних технологій (ІТ). Уведено поняття “стратегічна безпека об’єктів” та розроблено комплексну модель стратегічної безпеки структури “об’єкт – ІТ”. Запропоновано парадигму побудови ІТ для задач контролю фактичного стану промислових об’єктів на основі структури стратегічна безпека “об’єкт – ІТ” – інфраструктура інформатизації – концепція створення ІТ, що дає підстави для цілісного вирішення проблеми ресурсу і безпечної експлуатації об’єктів відповідно до методології розроблення ІТ, методології безпеки ІТ, стандартизації.*

***Ключові слова**: об’єкт, інформаційна технологія, відбір даних, роботоздатність, гарантоздатність, система ”об’єкт – інформаційна технологія”, стратегічна безпека, комплексна модель, парадигма побудови інформаційних технологій.*

G. Mykytyn

PRINCIPLES OF STRATEGIC SYSTEM SECURITY “OBJECT – INFORMATION TECHNOLOGY”

***Summary.** Security aspects of anthropogenic objects and IT security aspects were analyzed. A concept of ‘strategic security of objects’ was introduced and a complex model of strategic security of the system ‘object – IT’ was developed on the level ‘working capacity and dependability’. There was proposed a paradigm to build IT selection of mixed data for controlling tasks of actual conditions on the basis of the strategic security structure ‘object – IT’ – infrastructure of informational support – concept of IT development.*

System conception as a paradigm core which is orinted on the development of: methodologies for creation of IT data selection on the complex approach level to determine the parameters under workability structure: object - IT - metrological tools; IT-security methodology, as the main instrument of industrial infrastructure according to the standartization system with the purpose of making effective management decisions at the level of "defect - damage - destruction: detection - assessment - classification"

Metodology of IT-security based on clasification of possible threats for information resources, systems, processes, networks, management forms a set of methods and tools of securit according to the system, regulatory and complex models and is inseparately directed to the providing of information security on "leakage - modification - destruction" level, under critical for informational, technological, structural threats. Standartizatizational of information tool in terminology context and formation of the concept of information resources is a basis for the standardizing methods of IT-creation for the tasks of problems station managing.

Paradigm of IT-selection construction and heterogeneous data processing is the basis for providing: workability of man-made objects in emergence control and defects evolution of construction level, assessment of hydrogen degradaion level of metals, materials sress-strain state determination; automation control systems protection that comprehensively describes the approaches to the resource solution and safe equipment operation in the areas in question.

***Key words:** object, information technology, data selection, workability, dependability, system “object – information technology”, strategic security, complex model, paradigm of information technology creation.*

Постановка проблеми. Безпека об’єктів промислової інфраструктури є однією з провідних проблем у комплексних програмах наукових досліджень. Інформаційні технології – головний інструментарій забезпечення безпеки техногенних об'єктів на рівні процесів відбору даних про їх фактичний стан, які дають підстави вирішувати науково-прикладні завдання контролю і розвитку дефектів у матеріалах, їх деградації, тріщиностійкості. Для відбору даних, оцінювання параметрів технічного стану агрегатів, елементів трубопроводів, металевих конструкцій обладнання, апаратних комплексів та інших об’єктів з метою прийняття управлінського рішення на рівні

“міцність – ресурс” автоматизовані системи контролю мають задовольняти критеріям безпеки на інформаційному та функціональному рівнях.

Два наукові сегменти – безпека об’єктів у контексті інформаційних технологій та ІТ-інженерія безпеки представлені науковими школами Києва, Харкова, Львова, фундаментальними розробками університетів, інститутів, наукових центрів щодо застосування ІТ у галузі неруйнівного контролю (НК) і технічної діагностики (ТД) та забезпечення функціональної безпеки (ФБ) інформаційних технологій. Тому питання створення методологічних засад безпеки системи “об’єкт – ІТ” є фундаментом для реалізації стратегічної безпеки об’єктів промислової інфраструктури України.

Аналіз останніх досліджень і публікацій. *Аспекти ресурсу та безпеки експлуатації техногенних об’єктів.* Проблемі ресурсу й безпеки експлуатації техногенних об’єктів приділено багато фундаментальних та прикладних наукових досліджень, зокрема в рамках Концепції цільової комплексної програми “Проблеми ресурсу і безпеки експлуатації конструкцій, споруд та машин” [1, 2, 3, 4, 5, 6, 7, 8, 9].

Безпека (населення, матеріальних об'єктів, навколишнього середовища) – відсутність неприпустимого ризику, пов'язаного з можливістю завдавання будь-якої шкоди (ДСТУ 2156-93). Техногенний об’єкт – обладнання, агрегати, машини, конструкції, апарати, створені технікою, промисловістю [10]. Одним з найактуальніших питань у галузі промислової безпеки є визначення роботоздатності потенційно небезпечних об’єктів. Потенційно небезпечний об’єкт – будь-яке джерело потенційної шкоди життєво важливим інтересам людини (ДСТУ 2156-93). Роботоздатність об’єкта – технічний стан, за якого об'єкт виконує всі свої функції, зберігаючи при цьому допустимий рівень ризику (ДБН В.1.2-14-2009).

Загалом ресурс об’єктів атомної, теплової енергетики, авіаційної та космічної техніки; нафтогазопроводів; мостобудування і суднобудування повинен відповідати вимогам призначеного терміну експлуатації, що зумовлює рівень забезпечення промислової безпеки. Призначений термін експлуатації – гарантований період безаварійної експлуатації конструкції, що визначається на етапі проектування і регламентується технічними умовами або правилами експлуатації (ДСТУ-Н Б В.2.3-21:2008).

Для забезпечення безпеки промислових об’єктів у контексті ІТ відбору даних на рівні “міцність – ресурс” актуальними й перспективними є:

– теоретико-експериментальні методи визначення властивостей матеріалів (механічних, фізико-механічних, технологічних та інших) на основі застосуванням методів і засобів ІТ відбору даних у галузі НК і ТД матеріалів техногенних об’єктів;

– експериментальні підходи до визначення впливу комплексу факторів: механічного навантаження, температури, тиску і концентрації водню, води, як технологічного ресурсу обладнання атомної і теплової енергетики, на експлуатаційні параметри промислових об’єктів;

– встановлення (підтвердження) аналітичних залежностей “параметр сигналу – параметр руйнування матеріалу” на основі використання: фізичного явища та ефекту, критеріїв механіки руйнування (МР), ефективних методів і засобів відбору даних про технічний стан об’єктів;

– застосування стандартизованих методик (або розроблення і стандартизація нових) прогнозування залишкового ресурсу техногенних об’єктів;

– створення методичних рекомендацій щодо застосування металів, сталей, сплавів у робочих середовищах водню, технологічної води за зміни факторів впливу, наприклад температури, механічного навантаження та інших;

– упровадження рекомендацій щодо технологічних процесів виготовлення, сталей, сплавів, конструкційних матеріалів, елементів енергетичного обладнання з високоякісними параметрами роботоздатності.

Такі дослідження сприятимуть мінімізації ризиків на промислових об’єктах,

уникненню відмов та аварійних ситуацій, відповідно забезпеченню ресурсу їх безпечної експлуатації. Аварійна ситуація – стан потенційно небезпечного об'єкта, що характеризується порушенням меж та (або) умов безпечної експлуатації, але не перейшов в аварію, при якому всі несприятливі впливи джерел небезпеки на персонал, населення та навколишнє середовище утримуються у прийнятних межах за допомогою відповідних технічних засобів, передбачених проектом (ДСТУ 2156-93).

Вплив водню, технологічної води, температури, механічного навантаження на матеріали промислових об’єктів призводить до виникнення напружено-деформованого стану відповідно до: зниження фізико-механічних властивостей, водневої деградації і корозії, передчасного руйнування елементів конструкцій, зношування обладнання у процесі експлуатації.

Проблема оцінювання технічного стану об’єктів на рівні “міцність – ресурс”, що зумовлює рівень безпечності їх експлуатації, є системною і потребує аналізу: елементів обладнання ядерної і теплової енергетики з позиції матеріалознавства; умов експлуатації, системи факторів впливу, класів дефектів; ІТ відбору даних як засобів дослідження зміни властивостей матеріалів і стану; методики визначення параметрів роботоздатності на основі методології вимірювання відповідних фізичних величин; прогнозування залишкового ресурсу; методології ФБ та інформаційної безпеки автоматизованих систем контролю.

В літературі [11] синтезовані тенденції розвитку засобів ІТ відбору й опрацювання даних про технічний стан об’єктів методами НК і ТД згідно з критеріями МР і методиками механічних випробувань і на цій основі прогнозування залишкового ресурсу елементів конструкцій та обладнання. В праці [12] обговорюються наукові результати проектування, виготовлення та експлуатації машинобудівних конструкцій, зокрема у контексті методів та засобів контролю й діагностування технічного стану об’єктів, методів оцінювання ресурсу енергетичного обладнання в робочих умовах експлуатації. Відомі підходи до створення ІТ відбору й опрацювання даних характеризують рівень забезпечення безпечної експлуатації промислових об’єктів на відповідному інтервалі часу, які працюють в умовах граничного навантаження та взаємодіють із системою факторів впливу, зокрема з агресивними середовищами.

У контексті безпечної експлуатації промислових об’єктів актуальною залишається безпека користування природними об’єктами, зокрема водою, як технологічною, так і питною, оскільки техногенна система і водна екосистема взаємодіють між собою. Екологічна безпека – відсутність дій, станів та процесів, які призводять до суттєвих збитків для навколишнього природного середовища, населення та матеріальних об’єктів (ДСТУ 2156-93).

Структура моніторингу водної екосистеми навколишнього середовища передбачає: програму; ІТ відбору і обробки параметрів води; методику виконання вимірювань, оцінювання екологічних ризиків щодо стану якості води, відповідно прийняття рішення на управління водною системою на основі прийнятої моделі. Рівень безпеки водокористування питною водою оцінюється станом якості екологічних параметрів (наприклад, фізико-хімічних, радіаційних мікробіологічних та інших) за дії комплексу природно-антропогенних факторів [13].

Оцінювання стану якості екосистем на основі комплексного екологічного моніторингу є одним із головних напрямів програми досліджень з проблем раціонального природокористування та збереження навколишнього середовища [14]. Ефективність відбору та оцінювання екологічних параметрів води як технологічної, так і питної зумовлюється точністю методів і автоматизованих систем контролю та відповідно їх гарантоздатністю.

Безпека інформаційних технологій. Інформаційні технології, які є основними засобами забезпечення безпечної експлуатації потенційно небезпечних об’єктів та моніторингу екосистем і застосовуються для відбору даних, оцінювання та прийняття

рішення на управління проблемною ситуацією з метою мінімізації ризику у промисловій та екологічній інфраструктурах, повинні самі бути безпечними у своєму функціонуванні. Питання забезпечення безпеки ІТ сьогодні прогресивно розвиваються згідно з Концепцією технічного захисту інформації в Україні та на рівні міжнародних проектів [15].

Проблематика ФБ інформаційних технологій фундаментально представлена в системі міждержавних стандартів (IEC 61508-1:1998, IDT): ГОСТ Р МЭК 61508-1-2007; IEC 61508-2:2000, IDT): ГОСТ Р МЭК 61508-2-2007; IEC 61508-3:1998, IDT): ГОСТ Р МЭК 61508-3-2007; IEC 61508-4:1998, IDT): ГОСТ Р МЭК 61508-4-2007), які гармонізовані з міжнародними на рівні безпеки повного життєвого циклу, життєвого циклу безпеки систем і життєвого циклу безпеки програмного забезпечення. Розроблено засади та критерії: ФБ експлуатації систем ядерних реакторів атомних електростанцій [16] та бортової авіаційної техніки [17]; ієрархічного управління експлуатацією складних систем [18]; створення бази знань для оцінювання безпеки ІТ управління обладнанням теплових і атомних електростанцій [19], захисту інформації у сфері надзвичайних ситуацій [20].

У контексті забезпечення безпеки ІТ для завдань управління проблемними ситуаціям актуальними є питання діагностування та прогнозування технічного стану комп'ютерних систем в умовах невизначеності інформації: концепція, методологія, системи моніторингу [21].

Методологічною основою безпеки ІТ, які використовуються в завданнях управління потенційно небезпечними об'єктами, є гарантоздатність – це комплексна властивість інформаційних та управляючих систем забезпечувати безперервність функціонування техногенних і природних об'єктів у діапазоні безпечних параметрів їх експлуатації з метою мінімізації ризиків аварій та збитків (СОУ-Н НКАУ 0060:2010).

Серед характеристик гарантоздатності: доступність – готовність до використання; надійність – здатність забезпечити неперервність обслуговування під час використання; безпечність – відсутність небезпечного впливу на оточення; захищеність – здатність зберегти конфіденційність; ремонтопридатність. Забезпечення гарантоздатності полягає у створенні (використанні) методів та засобів: запобігання помилок, терпимості до помилок, виправлення помилок, передбачення помилок.

Функціональна безпека – частина загальної безпеки, яка відноситься до об'єкта управління і залежить від правильності функціонування E/E/PE систем (електричних / електронних / програмованих електронних), пов'язаних з безпекою, систем забезпечення безпеки, які ґрунтуються на інших технологіях, і зовнішніх засобів зменшення ризику (IEC 61508-4:1998, IDT): ГОСТ Р МЭК 61508-4-2007).

Ядром функціональної безпеки ІТ є інформаційна, яка функціонально спрямована на захист даних. Інформаційна безпека – такий стан інформаційних потоків і технологій, інформаційних ресурсів, баз і банків даних, що із визначеною ймовірністю виключає можливість випадкового чи навмисного доступу до них осіб, що не мають на це права [22]. Захист даних – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації (ДСТУ 5034:2008).

З цієї позиції на практиці впроваджуються наукові розроблення на рівні концептуального, нормативного, технічного, апаратно-програмного забезпечення гарантоздатності (СОУ-Н НКАУ 0060:2010) [23, 24, 25, 26]. Невідповідність систем вимогам гарантоздатності призводить до виникнення дефектів, помилок, аварій на програмно-технічному рівні, що зумовлює дефіцит безпеки об'єктів. Функціональна безпека автоматизованих систем у завданнях управління промисловими об'єктами є головним критерієм недопущення ризику аварійних ситуацій [27, 28]. Достовірність даних у життєвому циклі автоматизованих систем є індикатором їх інформаційної безпеки.

Мета роботи. Для цілісного вирішення проблеми безпеки як об’єктів, так і ІТ необхідно: розробити комплексну модель стратегічної безпеки системи “об’єкт – ІТ”; створити парадигму побудови ІТ відбору різнорідних даних від природно-техногенних об’єктів, які інтегрально спрямовані на визначення фактичного стану техногенних систем для мінімізації ресурсного ризику “дефект – руйнування – загроза – збитки” та інформаційного ризику “витік – модифікація – втрата” у структурі функціонального ризику “невизначеність – відмова – аварія”.

Комплексна модель стратегічної безпеки системи “об’єкт – ІТ”. Ефективність забезпечення безпеки об’єктів в експлуатаційних умовах, зокрема за дії граничного навантаження та комплексу факторів впливу зумовлюється безпекою ІТ відбору даних. Це дає підстави для уведення поняття стратегічної безпеки системи “об’єкт – ІТ”.

Стратегічна безпека об’єктів – комплекс підходів, методів і засобів забезпечення безпеки експлуатації техногенних об'єктів / безпеки використання природних об’єктів та безпеки ІТ, спрямованих на визначення міцності й довговічності конструкційних матеріалів; параметрів якості води як технологічного ресурсу, захищеності автоматизованих систем контролю і, на цій основі, прийняття рішення на управління проблемною ситуацією в рамках системи моделей за умов дії комплексу факторів впливу. Комплексна модель стратегічної безпеки системи “об’єкт – ІТ” зображенаа на рис.1.

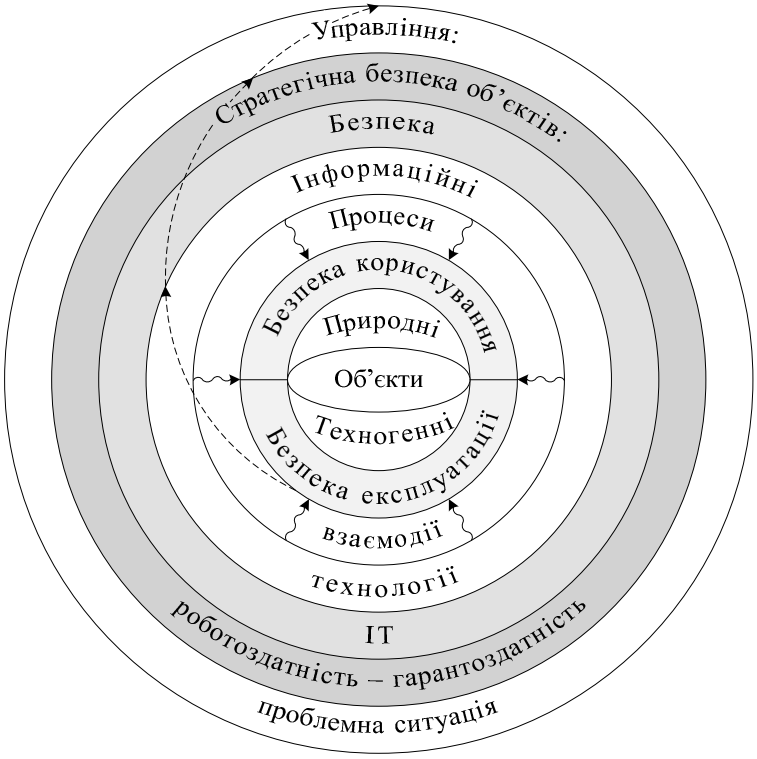

Рисунок 1. Комплексна модель стратегічної безпеки системи “об’єкт – ІТ”

Figure 1. Complex model of strategic system security “object - IT”

Комплексна модель безпеки системи “об’єкт – ІТ” є підставою для розроблення методологічних засад побудови ІТ для завдань управління проблемними ситуаціями у галузі контролю (діагностування) техногенних об’єктів у контексті оцінювання їх роботоздатності та прогнозування ресурсу, а також методології захисту даних в автоматизованих системах контролю.

Парадигма побудови ІТ відбору даних від об’єктів для забезпечення їх

стратегічної безпеки. На сьогодні прогресивно розвиваються напрямки створення ІТ відбору даних у контексті визначення параметрів роботоздатності об'єктів, прогнозування їх безпечного ресурсу, а також розроблення підходів до забезпечення безпеки автоматизованих систем у прикладних задач контролю та управління промисловою безпекою. Оскільки ІТ є ефективним засобом оцінювання технічного стану техногенних об'єктів за комплексом інформативних параметрів на рівні "міцність – ресурс", то відповідно повинні відповідати вимогам функціональної та інформаційної безпеки.

Розвиток методологічних засад створення ІТ відбору й опрацювання різнорідних даних від техногенних об'єктів у рамках безпечного функціонування системи "об'єкт – ІТ" зумовлює необхідність: забезпечення процесів ефективного відбору інформативних параметрів на рівні "дефект – руйнування – загроза – збитки"; забезпечення інформаційної безпеки життєвого циклу даних на рівні загроз "витік – модифікація – знищення" в рамках функціональної "невизначеність – відмова – аварія", що дозволяє забезпечити необхідну точність на рівні "міцність – ресурс" і дає підстави для формування стратегії управління системою "роботоздатність – гарантоздатність".

Єдиний підхід до побудови ІТ відбору різнорідних даних від об'єктів обґрунтовує системні критерії безпечного функціонування як техногенних/ природних об'єктів, так функціональної та інформаційної безпеки ІТ. Це дозволяє сформувати цілісність безпеки структури "об'єкт – ІТ" на рівні узгодження методів і засобів НК (ТД) та вимірювання, методик механічних випробувань, методології та методик виконання вимірювань, системних моделей метрологічного забезпечення (МЗ) згідно з концептуальною структурою; методів і засобів захисту автоматизованих систем контролю технічного стану техногенних об'єктів промислової інфраструктури.

Проблемна ситуація "техногенний / природний об'єкт – ІТ – стратегічна безпека" та інфраструктура інформатизації як засіб подолання надзвичайних ситуацій техногенного / природного характеру, є підставою для обґрунтування нової парадигми побудови ІТ відбору й опрацювання різнорідних даних від об'єктів, яка трансформується у різні предметні сфери відповідно до проблемних завдань. Вертикальна декомпозиція науково-прикладної проблеми побудови ІТ для забезпечення стратегічної безпеки системи "об'єкт – ІТ" представлена на рис.2.

Парадигма побудови ІТ відбору різнорідних даних враховує основні положення: Концепції цільової комплексної програми "Проблеми ресурсу і безпеки експлуатації конструкцій, споруд та машин", Концепції комплексної програми з проблем сталого розвитку, раціонального природокористування та збереження навколишнього середовища, Концепції Національної програми інформатизації, Концепції технічного захисту інформації в Україні [6, 14, 15, 29].

Системні підходи до створення парадигми побудови ІТ відбору й опрацювання даних уможливлюють розбиття її структури на компоненти – завдання, вирішення яких відображають особливості методологій створення ІТ у кожному окремому випадку.

Складовими структури парадигми побудови ІТ відбору різнорідних даних від об'єктів у контексті забезпечення їх стратегічної безпеки є:

– стратегічна безпека системи "об'єкт – ІТ" на рівні – ресурс/ норматив для техногенних / природних об'єктів, захищеність автоматизованих систем (інформаційно-аналітичних систем (ІАС), вимірювальних інформаційних систем (ВІС), автоматизованих систем управління (АСУ), систем підтримки прийняття рішення (СППР), експертних систем (ЕС)) для завдань управління;

– інфраструктура інформатизації (інформаційні ресурси, інформаційні технології, стандартизація, інформаційна безпека);

– системна концепція створення ІТ відбору різнорідних даних на рівні підходів (методологічного, системного, комплексного та інших) до вирішення проблеми роботоздатності об'єктів на рівні "міцність – ресурс": контроль виникнення й розвитку

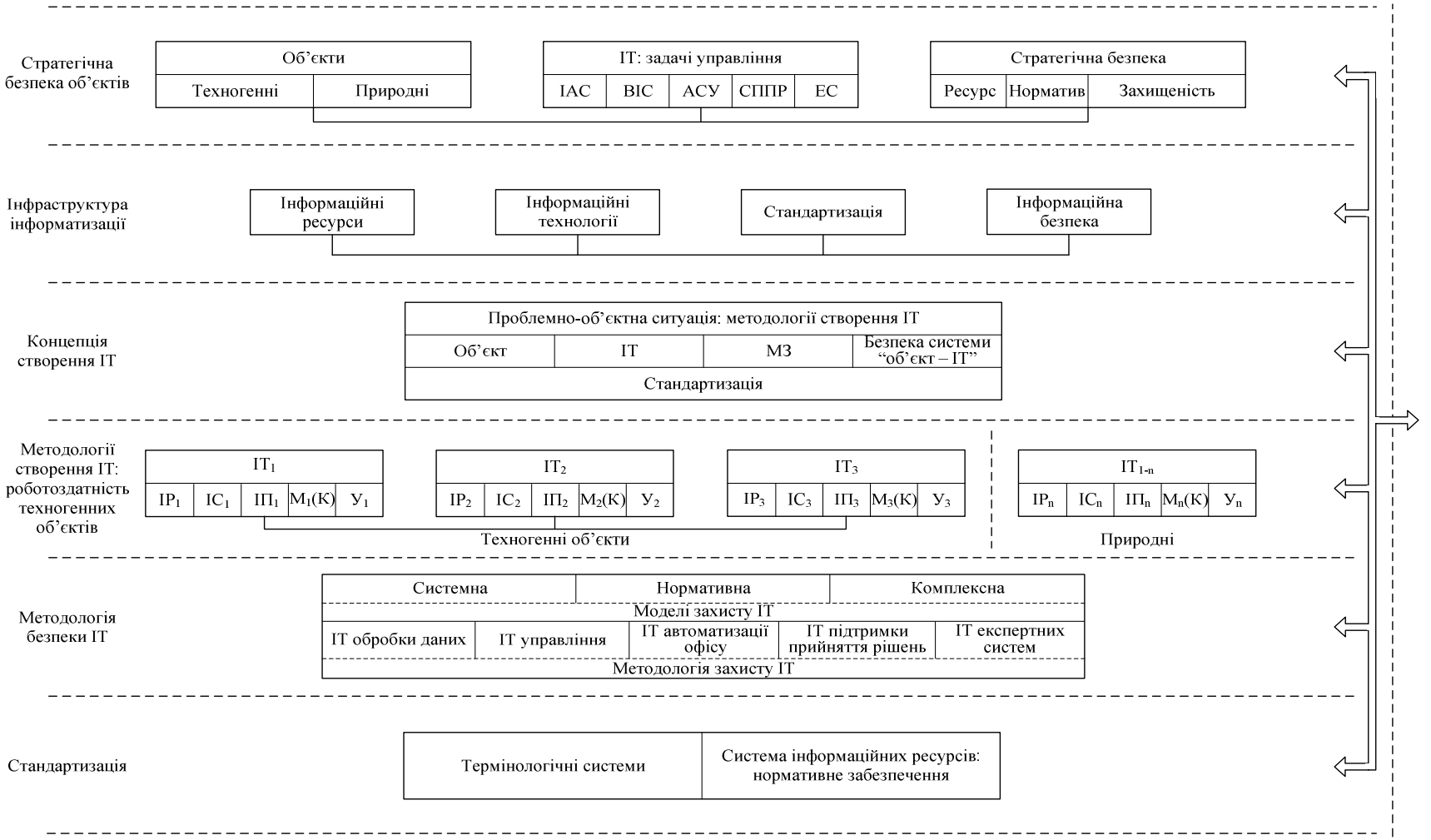

Рисунок. 2. Парадигма побудови ІТ відбору різнорідних даних від об'єктів

Figure 2. Paradigm of creation IT selection heterogeneous data from objects

дефектів елементів конструкцій, оцінювання ступеня деградації металів за умов впливу системи факторів (водню, температури, навантаження, технологічної води), оцінювання статичної тріщиностійкості матеріалів;

– методології створення інформаційних технологій (ІТ1-n) відбору даних про фактичний стан техногенних / природних об'єктів на рівні інформаційних ресурсів (IPn), інформаційних систем (ICn), інформаційних процесів (IПn), інформаційних мереж (каналів) (IMn (К)), управління (Уn);

– безпека ІТ на основі системної, нормативної і комплексної моделей та методології комплексного захисту в рамках структури гарантоздатності автоматизованих систем;

– стандартизація як комплекс нормативного забезпечення для уніфікації терміносистем, методів та засобів відбору й опрацювання різнорідних даних від об'єктів з метою забезпечення їх стратегічної безпеки.

Концепція створення ІТ відбору різнорідних даних як система представлена підсистемами: методологіями розроблення ІТ відповідно до мети та завдань дослідження предметної сфери, функціональної та інформаційною безпекою, стандартизацією, які у взаємозв'язку та взаємодії становлять єдину структуру у контексті проблеми забезпечення безпеки на рівні структури "об'єкт – ІТ". Кожна підсистема розглядається на рівні взаємозв'язку та взаємодії, що зумовлює фактори впливу на систему в цілому і наповнює її відповідним змістом. Аналіз і синтез компонент (підсистем) концепції є підґрунтям для уніфікації методів створення ІТ відбору різнорідних даних та методів захисту автоматизованих систем у контексті забезпечення безпеки структури "об'єкт – ІТ".

Висновки. Проаналізовано аспекти безпеки експлуатації техногенних об'єктів у контексті ІТ та елементи безпеки ІТ. Уведено поняття "стратегічна безпека об'єктів" та розроблено комплексну модель стратегічної безпеки системи "об'єкт – ІТ". Запропоновано парадигму побудови ІТ відбору різнорідних даних на основі стратегічної безпеки системи "об'єкт – ІТ", інфраструктури інформатизації, концепції створення ІТ, методології побудови ІТ, методології безпеки ІТ, стандартизації, що уможливлює її трансформацію у різні предметні сфери з метою забезпечення як безпеки експлуатації об'єктів, так і безпеки самих ІТ, як засобів оцінювання параметрів роботоздатності та прийняття управлінського рішення.

Conclusions. Security aspects of anthropogenic objects operation were analyzed in IT context as well as IT security elements. A concept of 'strategic security of objects' was introduced and a complex model of strategic security of a system 'object – IT' was developed. There was proposed a paradigm to build IT selection of mixed data on the basis of: strategic security of a system 'object – IT', infrastructure of informational support, concept of IT development, methodology of IT elaboration, methodology of IT security, and standardization, which makes it possible to transform into various subject areas with the aim of providing both security of objects operation and security of IT itself in the context of structure parameters evaluation 'working capacity to dependability' and in making administrative decisions.

Список використаної літератури

1. Механика разрушения и прочность материалов: справ. пособие в 4 т. [Текст] / В.В. Панасюк / В.В. Панасюк, А.Е. Андрейкив, В.З. Партон; ред. В. В. Панасюк. – К.: Наук. думка, 1988–1990. – 2219 с.
2. Патон, Б.Е. О новых подходах в оценке состояния сварных конструкций и определения их остаточного ресурса [Текст] / Б.Е. Патон, А.Я. Недосека // Техническая диагностика и неразрушающий контроль. – 2000. – № 1. – С. 3–8.
3. Механіка руйнування і міцність матеріалів: довідниковий посібник [Текст]; За заг. ред. В.В. Панасюка. Т.5: Неруйнівний контроль і технічна діагностика; за ред. З.Т. Назарчука. – Львів: ФМІ, 2001. – 1134 с.

4. Назарчук, З.Т. Акустико-емісійне діагностування елементів конструкцій: науково-технічний посібник: у 3-х томах. – Т.1: Теоретичні основи методу акустичної емісії [Текст] / З.Т. Назарчук, В.Р. Скальський. – К.: Наук. думка, 2009. – 287 с.
5. Муравський, Л.І. Методи спекл-кореляції для дослідження механічних властивостей конструкційних матеріалів [Текст] / Л.І. Муравський. – К.: Наукова думка, 2010. – 208 с.
6. Постанова Президії Національної академії наук України "Про виконання цільової комплексної програми наукових досліджень "Проблеми ресурсу і безпеки експлуатації конструкцій, споруд та машин"" від 24.02.2010 № 54 [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?uid=1041.43322.0
7. Технология диагностирования и оценка остаточного ресурса паропроводов высокого давления тепловых электростанций по уровню микроповрежденности металла [Текст] / Е.Я. Векслер, И.В. Замекула, В.Ю. Толстов, Е.В. Семешко // Техн. диагностика и неразрушающий контроль. – 2010. – № 1. – С. 23–31.
8. Дубов, А.А. Проблемы оценки остаточного ресурса стареющего оборудования / А.А. Дубов // Техническая диагностика и неразрушающий контроль. – 2010. – № 2. – С. 49–54.
9. Ясній, В. Вплив наводнювання на сповільнене деформування і руйнування теплостійкої сталі [Текст] / В. Ясній // Вісник ТНТУ. – 2013. – Т. 71, №3. – С. 264 – 271.
10. Великий тлумачний словник сучасної української мови [Текст] / Уклад. і голов. ред. В. Т. Бусел. – К.: Ірпінь, ВТФ "Перун", 2005. – 1728 с.
11. Проблеми ресурсу і безпеки експлуатації конструкцій, споруд і машин // Збірник наукових праць за результатами, отриманими у 2007 – 2009 рр. [Текст] – Київ: Інститут електрозварювання ім. О.Є. Патона НАН України, 2009. – 709 с.
12. Теорія і практика раціонального проектування, виготовлення і експлуатації машинобудівних конструкцій [Текст] // Тези доповідей 3-ої Міжнародної науково-технічної конференції. – Львів: КІНПАТРІ ЛТД. – 2012. – 180 с.
13. Микитин, Г.В. Методологія оцінювання якості води [Текст] / Г.В. Микитин, Л.С. Сікора, В.Б. Дудикевич // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України. – 2011. – № 60. – С. 150–161.
14. Розпорядження Президії Національної академії наук України "Про затвердження концепції Цільової комплексної міждисциплінарної програми наукових досліджень НАН України з проблем сталого розвитку, раціонального природокористування та збереження навколишнього середовища" від 03.02.2010 № 31 [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/
link1/MUS13748.html
15. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 № 1126. Остання редакція від 13.10.2011 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1126-97-%D0%BF,415
16. Ястребенецький, В.В. 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.
17. Похил, В.С. Методы оценивания и обеспечения функциональной безоспасности бортовых информационно-управляющих систем летательных аппаратов [Текст] / В.С. Похил, А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2010. – № 7 – С. 278–282.
18. Зеленцов, В.А. Задачи иерархического управления эксплуатацией сложных систем [Текст] / В.А. Зеленцов, В.А. Заславский // Радіоелектронні і комп'ютерні системи. – 2010. – № 7(48). – С. 306–310.
19. Клевцов, А.Л. База знаний для оценки безопасности информационных и управляющих систем АЭС [Текст] / А.Л. Клевцов // Радіоелектронні і комп'ютерні системи. – 2007. – № 7 (26). – С. 114–120.
20. Грицюк, Ю.І. Проблеми захисту інформації у структурних підрозділах МНС України [Текст] / Ю.І. Грицюк, Т.Є. Рак // Науковий вісник НЛТУ України: зб. на-ук.-техн. праць. – Львів: РВВ НЛТУ України. – 2011. – Вип. 21.12. – С. 330–346.
21. Поморова, О.В. Теоретичні основи, методи та засоби інтелектуального діагностування комп'ютерних систем: монографія [Текст] / О.В. Поморова. – Хмельницький: Тріада-М, 2007. – 252 с.
22. Зеркалов, Д.В. Безпека життєдіяльності: начальний посібник [Текст] / Д.В. Закалов. – К.: Основа, 2011. – 168 с.
23. Глухов, В. Оцінювання гарантоздатності криптографічних комп'ютерних систем [Текст] / В. Глухов // Комп'ютерні науки та інформаційні технології. – 2008. – № 616. – С. 66–72.

24. Мудла, Б.Г. Гарантоздатність як фундаментальний узагальнюючий та інтегруючий підхід [Текст] / Б.Г. Мудла, Т.І. Єфімова, Р.М. Рудько // Математичні машини і системи. – 2010. – № 2. – С. 148–165.
25. Мудла, Б.Г. Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічних станів [Текст] / Б.Г. Мудла, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 7–14.
26. Теслер, Г.С. Концепция построения гарантоспособных вычислительных систем [Текст] / Г.С. Теслер // Математичні машини і системи. – 2006. – № 1. – С. 134–145.
27. Отказобезопасные информационно-управляющие системы на программируемой логике [Текст] / Е.С. Бахмач, А.Д. Герасименко, В.А. Головир и др.; под ред. В.С. Харченко, В.В. Скляра // Национальный аэрокосмический университет "ХАИ". – Кировоград: НПО "Радий", 2008. – 380 с.
28. Теслер, Г.С. Решение проблемы гарантоспособности компьютерных систем в аспекте базисов компьютерной науки [Текст] / Г.С. Теслер // Математичні машини і системи. – 2008. – № 4. – С. 171–188.
29. Закон України "Про Національну програму інформатизації" від 4 лютого 1998 року №74/98-ВР. Остання редакція від 02.12.2012 – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

Отримано 15.04.2014