УДК 004.056

Г.В. Микитин

КОМПЛЕКСНА СИСТЕМА БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАДАЧ УПРАВЛІННЯ ПРОБЛЕМНИМИ СИТУАЦІЯМИ

Розглянуто інфраструктуру інформатизації як засіб подолання надзвичайних ситуацій техногенного характеру в галузі промислової безпеки. З метою ефективного забезпечення безпеки експлуатації об'єктів та безпеки автоматизованих систем інформаційні технології (ІТ) представлено рівневою структурою: інформаційні ресурси (ІР), інформаційні системи (ІС), інформаційні процеси (ІП), інформаційні мережі (канали) (ІМ (К)), управління (У). В рамках структури гарантоздатності створено комплексну систему безпеки інформаційних технологій (КСБІТ), яка дозволяє забезпечити інформаційну безпеку (ІБ) на рівні "витік – модифікація – знищення" в рамках функціональної безпеки (ФБ) на рівні "невизначеність – відмова – аварія".

Ключові слова: *об'єкт, інформатизація, інформаційна технологія, гарантоздатність, інформаційна та функціональна безпека, комплексна система безпеки.*

Рассмотрена інфраструктура информатизации как средство преодоления чрезвычайных ситуаций техногенного характера в сфере промышленной безопасности. С целью эффективного обеспечения безопасности эксплуатации объектов и безопасности автоматизированных систем информационные технологии (ИТ) представлены уровневой структурой: информационные ресурсы, информационные системы, информационные процессы, информационные сети (каналы), управление. В рамках структуры гарантоспособности создана комплексная система безопасности ИТ, позволяющая обеспечить информационную безопасность на уровне " утечка – модификация – уничтожение" в рамках функциональной безопасности на уровне "неопределенность – отказ – авария".

Ключевые слова: *объект, информатизация, информационная технология, гарантоспособность, информационная и функциональная безопасность, комплексная система безопасности.*

An informatization infrastructure, as means of man-made emergencies overcoming in industrial safety field was considered. In order to of effective security providing of objects exploitation and automated systems security, an information technologies (IT) is presented by the level structure: information resources, information systems, information processes, information networks (channels), management. Within dependability structure the comprehensive IT safety system was created, which allows to provide information security on "leak – modification – dectruction" level, within functionality safety on "uncertain-ty – failure – emergency" level.

Keywords: *object, informatization, information technology, dependability, information and functionality safety, combined security system.*

Сьогодні ІТ є головним інструментарієм вирішення прикладних задач у предметних сферах. Єдиний підхід до створення ІТ відбору даних від природно-техногенних об'єктів обґрунтовує системні критерії: безпечного функціонування технологічних та природних систем [1]; функціональної та інформаційної безпеки інформаційних технологій [2]. Наука і практика зацікавлені у такому підході, оскільки він – системний і об'єднує кілька наукових напрямів. Розвиток ІТ для прикладних задач управління проблемними ситуаціями передбачає синтез двох напрямів: 1) вдосконалення / створення нових методів та засобів відбору і обробки інформації про фактичний стан техногенних систем на рівні процесів відбору параметрів сигналів для мінімізації ресурсного ризику "дефект – руйнування – загроза – збитки"; 2) вдосконалення створення методів і засобів забезпечення безпеки автоматизованих систем для мінімізації інформаційного ризику "витік – модифікація – втрата" у структурі функціонального ризику "невизначеність – відмова – аварія".

Парадигма створення ІТ відбору різнорідних даних від технологічних і природних систем, які функціонують в умовах невизначеності, є підставою для: контролю та оцінювання стану техногенних об'єктів; моніторингу екосистем на предмет визначення їх параметрів; застосування методології безпеки ІТ як основного інструментарію забезпечення ресурсу тривалої експлуатації об'єктів промислової інфраструктури та нормативу якісного природокористування, що забезпечує безпеку системи "об'єкт – ІТ" за дії впливу комплексу факторів [3].

Мета роботи – розроблення КСБІТ на засадах гарантоздатності для забезпечення цілісної безпеки структури "роботоздатність об'єкта – захищеність автоматизованої системи".

Інформаційні технології для задач управління проблемними ситуаціями

Інформатизація як засіб подолання надзвичайних техногенних ситуацій. Серед основних завдань Концепції Національної програми інформатизації – застосування та розвиток сучасних ІТ у відповідних наукових галузях; підвищення ефективності виробництва на основі використання ІТ; формування системи національних ІР, інтегрованих у світовий інформаційний простір [4]. Основні напрями інформатизації відповідних науково-технічних галузей функціонально пов'язані із: системами стандартизації і сертифікації; ІР; інформаційно-комунікаційними мережами; ІТ; інформаційною безпекою. Інформаційні технології є засобом інформатизації, зокрема таких актуальних галузей, як неруйнівний контроль (НК) і технічна діагностика (ТД) стану техногенних об'єктів в робочих умовах експлуатації з метою прийняття рішення для управління проблемними ситуаціями. Засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, ІС або їх окремі елементи, ІМ і мережі зв'язку, що використовуються для реалізації інформаційних технологій.

Інформаційні ресурси, ІТ, стандартизація, безпека ІТ складають основу інфраструктури інформатизації, яка є засобом подолання надзвичайних ситуацій техногенного і природного характеру в умовах впливу системи факторів. Основою організаційно-правового, технічного, нормативного забезпечення інфраструктури інформатизації у галузі НК (ТД) параметрів техногенних об'єктів є:

– розвиток методології створення ІР: формування баз даних (БД), сховищ даних (СД), баз знань (БЗ), баз моделей (БМ), масивів інформації (МІ), які функціонально відображають відповідні предметні сфери та інтегруються в глобальні ІМ за єдиними принципами;

– забезпечення критеріїв ефективного функціонування ІР згідно з системами кодування інформації;

– розроблення методологічних засад створення ІТ відбору і обробки даних від об'єктів, як засобів інформатизації, для вирішення задач контролю параметрів працездатності та управління проблемними ситуаціями;

– створення національної системи стандартизації і сертифікації ІТ, як засобів інформатизації у галузі контролю (діагностування) технічного стану об'єктів;

– розроблення комплексного підходу до забезпечення безпеки ІТ для прикладних задач управління об'єктами в умовах невизначеності і ризику аварій.

Рівнева структура ІТ. Для обґрунтування вибору критеріїв забезпечення безпеки системи "об'єкт – ІТ" на основі системного аналізу запропоновано рівневу структуру ІТ (рис. 1.) [5].

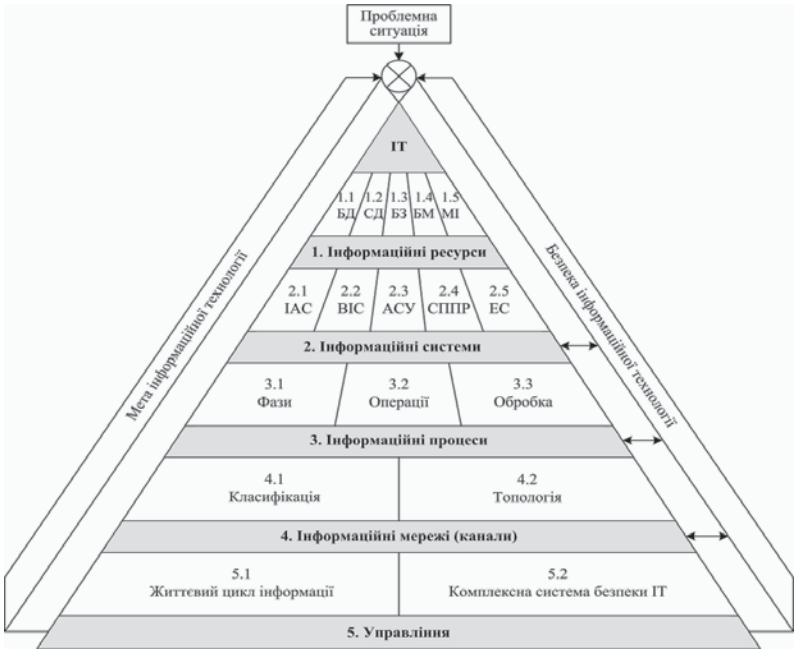

Рис. 1. Рівнева структура ІТ для задач управління проблемними ситуаціями

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

– інформаційних ресурсів (1) – БД, СД, БЗ, БМ, МІ;

– інформаційних систем (2) – інформаційно-аналітичних систем (ІАС), вимірювальних інформаційних систем (ВІС), автоматизованих систем управління (АСУ), систем підтримки прийняття рішення (СППР), ЕС;

– інформаційних процесів (3);

– інформаційних мереж (каналів) (4);

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

3. Гарантоздатність ІТ: надійність, функціональна та інформаційна безпека

Гарантоздатність. Гарантоздатність ІТ є однією зі складових стратегічної безпеки техногенних об'єктів. В нормативному документі СОУ-Н НКАУ 0060:2010 та наукових публікаціях наведено: інтерпретації поняття гарантоздатності, аналіз складу її властивостей, еволюцію, визначення основних показників [6, 7, 8]. В стандарті СОУ-Н НКАУ 0060:2010 гарантоздатність та її складові властивості розглянуто стосовно програмно-технічних комплексів різних типів і функціо-

нального призначення. Стандарт відображає, зокрема: методи забезпечення гарантоздатності та управління; принципи, показники та методи оцінювання гаорантоздатності; загальні вимоги до гарантоздатності. Гарантоздатність – це комплексна властивість системи надавати необхідні послуги, яким можна оправдано довіряти. Структура гарантоздатності включає такі складові: первинні властивості гарантоздатності; загрози, що призводять до порушення працездатності; відмовостійкість як ключовий механізм забезпечення гарантоздатності; вторинні властивості, які деталізують зміст первинних; взаємозв'язки між складовими (рис. 2).

До первинних властивостей гарантоздатності відносяться:

– безвідмовність – властивість надавати необхідні послуги впродовж заданого часу;

– готовність – властивість доступності ресурсів для надання необхідних послуг;

– обслуговуваність – властивість пристосовуватись до модифікацій, обслуговування та ремонту;

– живучість – властивість мінімізувати зниження працездатності та зберігати в прийнятних межах обсяг та якість надаваних послуг у разі відмов, обумовлених зовнішніми впливами різної природи;

– функціональна безпека – властивість виключати або мінімізувати шкідливі наслідки у разі відмов для користувачів, інших систем або навколишнього середовища;

– цілісність – властивість виключати непередбачені зміни даних, системи та надаваних послуг;

– конфіденційність – властивість перешкоджати неавторизованому доступу до інформації обмеженого доступу;

– вірогідність – властивість правильно оцінювати коректність наданих послуг.

Гарантоздатність та ІБ мають загальні властивості (цілісність і конфіденційність) та специфічні – автентичність, достовірність. Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації (НД ТЗІ-001-99, НД ТЗІ 1.1-002-99, НД ТЗІ 1.1-003-99).

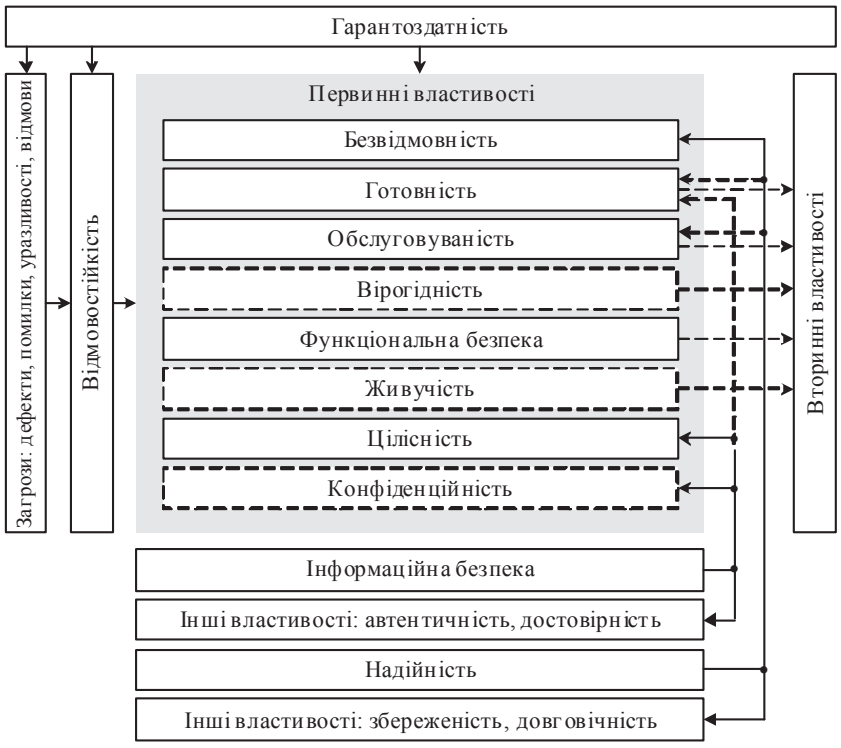

Рис. 2. Структура гарантоздатності ІТ

Надійність, функціональна та інформаційна безпека ІТ. Гарантоздатність ІТ поєднує аспекти надійності, функціональної та інформаційної безпеки. Надійність – властивість об'єкта зберігати в часі у встановлених межах значення всіх параметрів, які характеризують його здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування (ISO/IEC 14598-1:1999). Надійність програмного забезпечення – сукупність властивостей, що обумовлюють здатність програмного продукту зберігати зазначений рівень працездатності у заданих умовах (ECSS-Q-80B–2002). Актуальними є методи аналізу надійності технічних систем, які підтримуються системою державних стандартів [9]. Стандарт ДСТУ 2861-94 встановлює два основних підходи до аналізу надійності об'єктів: аналіз надійності за результатами заходів і способів її забезпечення на етапах проектування, виробництва та експлуатації відповідно до програми; кількісні методи аналізу надійності об'єкта, які ґрунтуються на аналізі умов експлуатації, причин і механізмів відмов, показників надійності елементів, стратегій технічного обслуговування та ремонту. Стандарт ДСТУ 2863-94 передбачає вимоги до змісту програми забезпечення надійності. Стандарт ДСТУ 2864-94 встановлює основні положення щодо експериментального оцінювання і контролю надійності техніки. Згідно зі стандартом ДСТУ 3004-95 для визначення показників надійності використовують два методи: непараметричний, параметричний. У стандарті ДСТУ 2634-94 представлені показники надійності електронної техніки: середній наробіток до відмови; інтенсивність відмов під час експлуатації; інтенсивність відмов під час випробувань; інтенсивність відмов під час зберігання; мінімальний наробіток; гамма-відсотковий ресурс; мінімальний термін збережуваності; гамма-відсотковий термін збережуваності та методи їх оцінювання. Гарантоздатність у контексті забезпечення надійності систем і програмного забезпечення досягається такими підходами: підвищенням надійності деталей і вузлів; побудовою надійних систем з менш надійних елементів за рахунок структурної надлишковості – дублювання елементів, пристроїв, підсистем; використанням методів і засобів функціонального контролю (ФК) з діагностикою відмов [10]. До задач ФК автоматизованих систем відносяться: своєчасне виявлення збоїв, несправностей, програмних помилок; виключення їх впливу на подальший процес обробки інформації; виявлення місця елементу або блоку програми, які відмовили для подальшого швидкого відновлення системи. Серед методів ФК систем: програмні, апаратні і комбіновані (апаратно-програмні). Якість ФК обумовлюється параметром щільності розподілу засобів виявлення помилок по всій "площі" контрольованої системи. Показниками якості ФК є: час виявлення і локалізації відмов апаратури з точністю до елемента; повнота контролю функціонування системи; достовірність контролю.

Функціональна безпека – це властивість системи виконувати задані функції без недопустимого ризику створення нею аварійних станів, які можуть призвести до загибелі, травмування, погіршення здоров'я людей, негативного впливу на довкілля, завдання матеріального чи іншого збитку [11]. Основою функціональної безпеки ІТ є – нормативне, наукове, технічне та програмне забезпечення. Система міждержавних та міжнародних стандартів: ГОСТ Р МЭК 61508, СТБ IEC 61508-1/ПР, IEC 61508 (IDT) встановлює загальний підхід до питань забезпечення безпеки для всього життєвого циклу систем, які складаються з електричних і/або електронних і/або програмованих електронних компонентів (E/E/PE), що використовуються для виконання функцій безпеки. Стандарт ГОСТ Р МЭК 61508-1-2007 регламентує вимоги до ФБ для всього життєвого циклу: систем; програмного забезпечення; застосування методів визначення рівнів повноти безпеки; управління в рамках узагальненої структури системи міжнародних стандартів МЭК 61508-1-1998 – ГОСТ МЭК-7-1998 (рис. 3).

З метою досягнення необхідного рівня повноти безпеки E/E/PE-систем прийнята технічна модель повного життєвого циклу безпеки (ГОСТ Р МЭК 61508-1-2007). Основою моделі повного життєвого циклу безпеки є: E/E/PE-системи; системи безпеки на інших технологіях; зовнішні засоби зменшення ризику. Побудова концепції ФБ на повному життєвому циклі ІТ, призначених для відбору різнорідних даних від промислових об'єктів, оцінювання їх технічного стану та прийняття рішення на управління вимагає: відбору/збору інформації про об'єкт дослідження (ОД), функції управління, навколишнє середовище; визначення потенційних джерел небезпеки, граничних та аварійних ситуацій; отримання інформації про встановлені види небезпеки – корозійність, руйнування, токсичність, радіаційність; отримання інформації про поточний стан регулювання у галузі промислової безпеки на державному та міжнародному рівнях; встановлення видів небезпеки, які виникають внаслідок взаємодії ОД з іншими об'єктами ближнього розташування. В стандарті ГОСТ Р МЭК 61508-1-2007 представлено моделі життєвого циклу безпеки E/E/PE-систем та життєвого циклу безпеки програмного забезпечення, які утворюють стадію реалізації повного життєвого циклу ФБ, що визначає системний рівень гарантоздатності. В нормативних документах IEC 61508-7: 2000 та СОУ-Н НКАУ 0058:2008 та в наукових працях [12, 13, 14, 15] проаналізовано рівні функціональної безпеки інформаційних та управляючих систем техногенних об'єктів та програмного забезпечення.

На рівні спільних властивостей – цілісності та конфіденційності інформаційна безпека є вбудованою в функціональну. Відповідно витік, модифікація, знищення даних може призвести до невизначеності, відмови та аварії. Технічні ризики функціонального та інформаційного рівнів обумовлюють технологічні (та природні) ризики, відповідно дефекти, руйнування, аварії для техногенних об'єктів та збитки навколишнього середовища, а також здоров'я людини. Методи і засоби ІБ постійно вдосконалюються на апаратно-програмному згідно системи стандартів: ГОСТ Р ИСО/МЭК 13335; ГОСТ Р ИСО/МЭК 15408; ДСТУ ISO/IEC TR 13335.

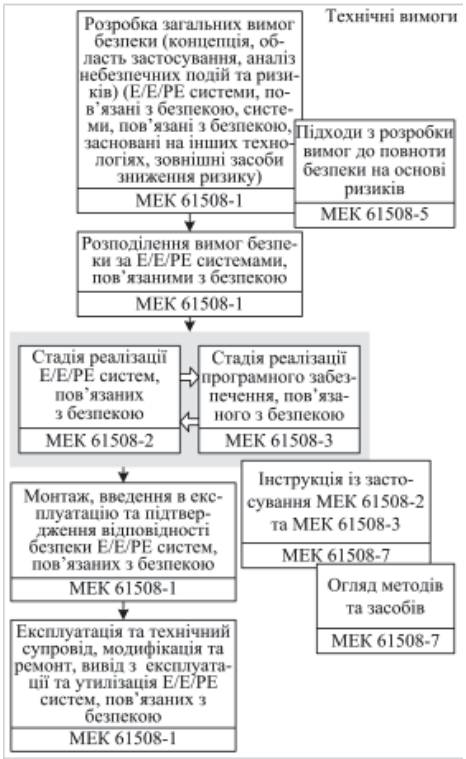

Рис. 3. Структура функціональної безпеки ІТ

4. Комплексна система безпеки ІТ: структура

Ефективність забезпечення безпеки ІТ для прикладних задач контролю (діагностування) технічного стану об'єктів визначається багаторівневою будовою системи безпеки. В цьому випадку реалізація будь-якої загрози зможе впливати на ІТ тільки у разі подолання усіх рівнів захисту. На основі системної, нормативної і комплексної моделей пропонується методологія КСБІТ для задач управління проблемними ситуаціями [16]. Комплексність припускає забезпечення захисту даних на усіх рівнях інформаційної технології. До складу комплексної системи безпеки даних входять заходи і засоби, які реалізують способи, методи і механізми захисту даних від:

– витоків технічними каналами;

– несанкціонованих дій і несанкціонованого доступу (НСД) до інформації, які можуть здійснюватися шляхом: під'єднання до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання даних або нав'язування помилкової інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів і т. і.;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності даних або руйнування системи безпеки.

Комплексна система безпеки передбачає захист даних відповідно до 5-ти рівнів структури ІТ на основі нормативного забезпечення (рис. 4).

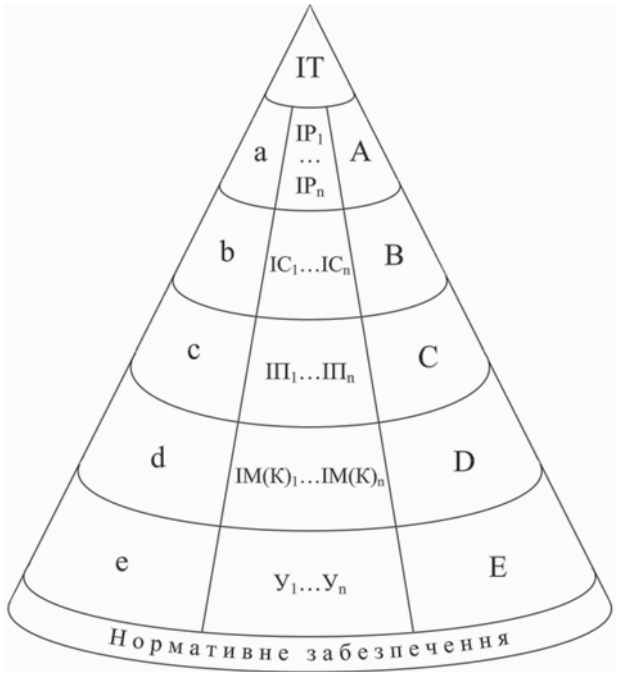

Рис. 4. Комплексна система безпеки ІТ для задач управління проблемними ситуаціями

Комплексна система безпеки ІТ представлена підсистемами безпеки – ІР, ІС, ІП, ІМ(К), У. Структура КСБІТ має властивості цілісності та емерджентності. Згідно нормативної моделі основою КСБІТ є система державних, міждержавних, міжнародних стандартів. Наприклад, в табл. 1 представлена КСБІТ на рівні ІС для задач управління проблемними ситуаціями згідно концепції "об'єкт – загроза – захист".

Таблиця 1

КСБІТ на рівні – інформаційні системи

Рівень захисту	Інформаційні технології для задач управління проблемними ситуаціями		
	Нормативне забезпечення: ДСТУ 4145-2002; ДСТУ ГОСТ 28147:2009; ДСТУ ISO 9160-2003; ДСТУ ISO/IEC 9798-1-2002; ДСТУ ISO/IEC 9798-2:2002; ДСТУ ISO/IEC 9798-3-2002; ДСТУ ISO/IEC 9798-4:2002; ДСТУ ISO/IEC 9798-5:2002; ДСТУ ISO/IEC 9798-6:2002; ДСТУ ISO/IEC 14888-1-2002; ДСТУ ISO/IEC 14888-2-2002; ДСТУ ISO/IEC 14888-3-2002; ДСТУ ISO/IEC 11770-2-2002; ДСТУ ISO/IEC 11770-3-2002; ДСТУ ISO/IEC 10118-1:2003; ДСТУ ISO/IEC 10118-2:2003; ДСТУ ISO/IEC 2382-14:2005; ДСТУ ISO/IEC 15946-3:2006; ДСТУ ISO/IEC 9797-1: 2009; ДСТУ ISO/IEC 19790:2009		
ІС	2.b.1. Відключення або виведення з ладу підсистем за безпечення функціонування системи (електроживлення, охолодження і вентиляції, ліній зв'язку). 2.b.2. Фізичне руйнування системи або виведення з ладу найбільш важливих її компонентів 2.b.3. Відмови програмного та апаратного забезпечення 2.b.4. Порушення роботи (випадкове або навмисне) системи чи її частин 2.b.5. Електромагнітне випромінювання 2.b.6. Вхід в інформаційну систему в обхід засобів захисту (завантаження сторонньої операційної системи із змінних носіїв інформації тощо) 2.b.7. Відключення або виведення з ладу підсистем за безпечення інформаційної безпеки автоматизованих систем 2.b.8. Впровадження апаратних і програмних закладок та вірусів, що дозволяють подолати систему захисту, приховано і незаконно здійснити доступ до IP 2.b.9. Незаконне отримання паролів та інших реквізитів розмежування доступу з подальшим маскуванням під законного користувача 2.b.10. Злам шифрів криптографічного захисту інформації 2.b.11. Відмови в обслуговуванні 2.b.12. Порушення доступу до системи чи її функціональних елементів 2.b.13. Алгоритмічні помилки при проектуванні 2.b.14. Неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки.	2.1. Інформаційно-аналітичні системи 2.2. Вимірювальні інформаційні системи 2.3. Автоматизовані системи управління 2.4. Системи підтримки прийняття рішень 2.5. Експертні системи	2.B.1. Законодавчі засади 2.B.2. Нормативно-методологічні засади 2.B.3. Наукові засади: технічні (апаратний, фізичний рівень); програмні засоби: 2.B.3.1. Здійснення за допомогою спеціалізованих надавачів автоматизованої процедури виявлення та протидії атакам 2.B.3.2. Стикування із зовнішніми кор.-поративними та комерційними інфраструктурами відкритих ключів, побудованими за стандартами відкритих систем 2.B.3.3. Контроль та обмеження доступу 2.B.3.4. Захист від НСД 2.B.3.5. Установка джерел безперебійного живлення 2.B.3.6. Використання власних аварійних електрогенераторів або резервних ліній електроживлення 2.B.3.7. Захист від стихійних лих 2.B.3.8. Використання обладнання ІТ з малим рівнем випромінювання 2.B.3.9. Резервне копіювання даних 2.B.3.10. Забезпечення плану не перервності бізнесу

Структура КСБІТ, які використовуються для задач управління проблемними ситуаціями, дозволяє реалізувати адекватний вибір елементів захисту рівнів – ІР, ІС, ІП, ІМ(К), У відповідно до моделей загроз, що і забезпечує цілісність.

Розроблено методологію комплексної системи безпеки ІТ для задач управління проблемними ситуаціями, яка має властивості цілісності та емерджентності: стан підсистем безпеки ІР, ІС, ІП, М(К), У, кожна з яких характеризується множиною параметрів захисту даних, та функціональна взаємодія, взаємозв'язок, взаємовідносини між ними визначають сутність КСБІТ у цілому, для якої характерна нова множина параметрів захисту.

Застосування цієї методології на практиці дозволить забезпечити інформаційну безпеку ІТ на рівні "витік – модифікація – знищення" в рамках ФБ на рівні "невизначеність – відмова – аварія", що дає підстави для реалізації уніфікованих методів і засобів захисту даних з метою забезпечення захищеності автоматизованих систем контролю технічного стану об'єктів.

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. – Київ : 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. *Микитин Г.В.* До проблеми побудови інформаційних технологій / Г.В. Микитин // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України. – 2012. – № 63. – С. 142–157.

4. Про Національну програму інформатизації : Закон України від 4 лютого 1998 року № 74/98-ВР [Електронний ресурс]. – Режим доступу : http : // zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

5. *Згуровський М.З.* Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К. : Видавнича група BHV, 2007. – 498 с.

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

7. *Сербін В.Г.* Визначення і формалізація основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу для їх оцінки і прогнозування / В.Г. Сербін, А.І. Сухомлин // Математичні машини і системи. – 2012. – № 4. – С. 182–189.

8. *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.

9. *Хенли Э.Дж.* Надежностное проектирование технических систем и оценка риска / Э.Дж. Хенли, Х. Кумамото ; пер. с англ., под ред. Ю.Г. Заренина. – К. : Вища шк. : Головное изд-во, 1987. – 544 с.

10. *Мельников В.В.* Безопасность информации в автоматизированных системах : монография / В.В. Мельников. – М. : Финансы и статистика, 2003. – 367 с.

11. *Бахмач Е.С.* Отказобезопасные информационно-управляющие системы на программируемой логике / 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.

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

13. *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.

14. *Скляр В.В.* Оцінка програмного забезпечення інформаційних та управляючих систем АЕС при експертизі ядерної й радіаційної безпеки / В.В. Скляр, М.А. Ястребенецький, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2008. – № 6(33). – С. 180–184.

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

16. *Микитин Г.В.* Системна, нормативна та комплексна моделі захисту інформаційних технологій / Г.В. Микитин // Вісник Національного університету "Львівська політехніка", Автоматика, вимірювання та керування. – 2011. – № 695. – С. 126–132.

Отримано 18.12.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.